**Logo

Description automatically generated**

**SCHOOL OF INFOCOMM TECHNOLOGY**

**Assignment Report on HRCMS**

Web Application & Pen-Testing

Semester 4 (2021/2022)

Deadline: 30 Jan 2021, 23:59hrs (Sunday)

|  |  |
| --- | --- |
| Student | Student ID |
| Neo Rei Siang Edward | S10204829E |
| Ow Kai Jie, Clarence | S10208659H |
| Mabel Choi JingYi | S10205986F |

**Sign Off Page**

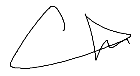
A picture containing hanger

Description automatically generated

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: Neo Rei Siang Edward

Date: 30/01/2022



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: Ow Kai Jie Clarence

Date: 30/01/2022

Letter

Description automatically generated with low confidence

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: Mabel Choi JingYi

Date: 30/01/2022

# **Executive Summary**

Mr Erwin has engaged Team NOC to perform pen-testing on the hrcms-admin web application and assess the current state of its security. After conducting the pen-test exercise, several vulnerabilities have been found and need to be addressed.

**Unauthorised Access to Administrative Pages**

This is a vulnerability where employee accounts have the ability to gain unauthorised access to administrative pages. This vulnerability can be exploited through the use of the URL. This vulnerability can be very dangerous for the web application because employees can act as administrators and perform administrative actions which can result in the destruction of the web application. This vulnerability can be mitigated through the use of proper role-based access control.

**Secure Socket Layer Stripping (SSL Stripping)**

The possibility of SSL stripping occuring has been identified in the web application. This vulnerability is a type of protocol downgrade attack, allowing attackers to become the middleman, intercepting the connection between a client and a server that would usually be confidential. SSL stripping strips away the “S” from “HTTPS” to “HTTP”, thus, allowing the data transmitted to be in a clear text format. This vulnerability could be mitigated by enforcing “Strict-Transport-Security”.

**Stored Cross-Site Scripting (XSS)**

Stored XSS vulnerabilities have been identified in the web application. This vulnerability entry point is an input field that is located in a form and can be exploited through the use of scripts entered by an attacker. This script injected by the attacker remains on the web application and is stored in the database. This allows for opportunities for attackers to impersonate other accounts and perform actions that cannot be linked back to them. This makes it hard to identify the attacks and allows for attackers to be more bold in their attacks. This is an attack that can be mitigated through the use of proper input validation and input sanitization

**Authentication Brute Force Vulnerability**

Authentication brute force vulnerability has been identified for the web application. Authentication brute force refers to exhaustive search and it is a form of an attack that can be carried out with a simple tool or script. This is only possible if a web application does not have a limit to the amount of attempts a user can input for account login. Additionally, with no password policy in place, this brute force attack might also be easier for accounts with weaker passwords, as humans usually would set a password that is easy to remember for themselves. This is an attack that can be mitigated with an enforcement of password policy and a login attempt limit.

**Verbose Errors**

Verbose errors refers to improper error handling which can show the name of an unhandled error or the file path of the web application or even information that attackers can take advantage of. This is a crucial error as it might make the web application more susceptible to attacks as attackers can then make use of these unhandled errors to carry out their attacks on specific places.

**Directory Traversal Attack**

A directory traversal attack has been identified in the web application. A directory traversal attack means that an attack can be conducted from the URL of the webpage. This attack only affects a particular webpage and does not affect the rest of the website but it still allows attackers to delete entries made. This attack can be mitigated through having proper permissions on the folders.

**Exposed Directories**

Exposed directories have been identified on the web application. Attackers can travel to these directories using the url. In these directories, sensitive information can be leaked. Sensitive information such as codes used for the webpage can be analyzed by attackers to identify the website’s architecture and to gain a greater understanding of the features and functions of the web application.

**Insufficient Logging & Monitoring**

Insufficient Logging & Monitoring has been discovered on the web application. Although the logs capture the date and time of whoever performed an action, it does not log the public ip address. Hence, even if in the log it says that a particular person performed this action, we won't be able to tell if it's the legitimate person or if there are multiple people using that account. Incorrect logging was also found. When a user edits the entry and tries to save it, even if the user encounters any issues while saving the edited entry, resulting in it not being saved, the log would capture that the entry has been modified when in actual fact the entry was not modified at all. Failed and successful login attempts are also not logged. This is important as it can tell if anybody tried to brute force into an account.

**Weak Password Requirements**

Minimum password requirements on the website have been identified to be very weak. A simple password such as “123” is able to be used and these types of password should be unacceptable. Without having proper passwords, attackers are able to brute force account credentials which can then lead to account impersonations and identity theft.

**Missing Security Headers**

There are security headers that are missing from the website. These security headers are bonus features that do help and protect the websites. They have the ability to prevent certain types of attacks such as cross-site scripting and clickjacking. They enhance the overall safety of the website and act as another layer of protection. If possible, it would be best to install these security headers to ensure the website is secure and hardened.

[**Executive Summary**](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_k2de387tr60u) **3**

[**1.0 Introduction**](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_pn02lqijcxwt) **9**

[**2.0 Client Information**](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_4zdy7widjnq) **10**

[**3.0 Pen-Test Schedule**](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_l90v0jfxnspa) **10**

[**4.0 Information Gathering Summary Findings**](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_dvqxa7asgez) **11**

[4.1 Passive Reconnaissance](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_gi2v21ooq0cq) 11

[4.1.1 Ping](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_1jaa9ntsglpb) 11

[4.1.2 Nmap](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_glu5ae6zl060) 12

[4.1.3 WhatWeb](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_dzswy5xj3n6z) 12

[4.1.4 Netcraft](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_7os1n2aii306) 12

[4.1.5 HTTP Methods](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_e7updix8db7j) 12

[4.1.6 nslookup](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_8ucsbezaatg3) 13

[4.1.6.1 NSLookUp using kali terminal](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_ywp8i1rdcies) 13

[4.1.6.2 NSLookUp using nslookup.io](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_5qf0pfrrkpwg) 13

[4.1.7 dnsenum](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_g8as7tc8129x) 13

[4.1.8 What CMS](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_nj9ukwc1pnh5) 13

[1.1.9 Security Headers](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_8l5uru7el8h5) 14

[1.1.10 Business Site Map](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_ba9jkkb90tw6) 14

[1.1.10.1 Employer Account](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_je49033le3gc) 14

[1.1.10.2 Employee Account](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_4r2eoez622jg) 15

[4.2 Active Reconnaissance](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_svt6tue6ygn7) 15

[4.2.1 DirBuster](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_llnfd4ymh4j4) 15

[4.2.2 Dirb](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_yqd09d4lvnxd) 15

[4.2.3 Wfuzz](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_nfi2dfm3fuwh) 16

[4.2.4 SQL MAP](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_noc1hep9nntp) 16

[4.2.5 SSL Labs](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_v7jfmqowwkz3) 16

[4.2.6 Network Diagram](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_421tcj82vgy4) 17

[4.2.7 Website Architecture Diagram](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_2tntt3x96yvk) 17

[4.2.8 Domain Site Map](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_g0nqz8fni3ej) 18

[4.2.8.1 Employer Account](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_gjvoj4ne9oo0) 18

[4.2.8.2 Employee Account](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_xgfseh7wa6eg) 19

[4.3 Vulnerability Scanning](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_2kgdb5x59u1q) 19

[4.3.1 OWASP ZAP](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_o2g2elwybvnm) 19

[4.3.1.1 OWASP ZAP - Employer Account](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_r5vgbzn7kfox) 19

[4.3.1.2 OWASP ZAP - Employee Account](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_5rahltaa9wl8) 20

[4.3.2 Nessus](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_il01l6y0eshu) 20

[4.3.3 Nexpose](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_l9lkp1nvyzi0) 21

[4.3.4 Skipfish](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_ryb2fmqr7d4d) 21

[4.4 XSS Scanning](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_2aotux2kpnvs) 21

[4.4.1 XssSniper](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_5maxv5on1tnp) 21

[4.4.2 Xsser](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_sm0ekbv6lwpz) 22

[4.4.3 Wapiti](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_7pg839mhk7bg) 22

[4.4.4 ZAP Fuzzing](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_t980z5vk8rd3) 22

[**5.0 Vulnerabilities Summary Findings**](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_ytkg6kbrw9mk) **23**

[5.1 Vulnerability Findings Matrix Table](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_q6wk31lf9ma1) 23

[5.2 Missing Security Headers](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_iivd2wtoaoc3) 25

[5.2.1 Proof of Vulnerability](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_x3tl968689k5) 25

[5.2.2 Summary of Findings](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_44vxaj76hpx8) 26

[5.3 Weak Password Requirements](file:///D:\NP_Year_2.2\WAPT\ASG\WAPT%20Report%20(Mr%20Erwin).docx#_aawcedbl6fxk) 26

# 1.0 Introduction

Mr Tan Hock Guan (NP’s Squad NOC in charge) had engaged Team Squad NOC to perform a security assessment penetration testing on the HRCMS (staging site) web application.

Team Squad NOC was engaged by Mr Erwin Tris Sanjaya from Tri-Niche Pte Ltd to perform a grey-box penetration testing on the HRCMS web application from 23 December 2021 to 30 January 2022.

This report will discuss the details of the penetration testing results that were conducted by team Squad NOC, as well as recommendations to improve on the security aspect of the HRCMS web application.

This report only covers the security of the web application assessed during the above mentioned time period. The security standards of the HRCMS web application may have changed since the assessment was completed.

# 2.0 Client Information

Tri-Niche is a company that operates in both Indonesia and Singapore, offering many IT solutions for mobile apps, websites, IT support and more.

Tri-Niche also mainly provides 2 different products, SCALLA and HRCMS. SCALLA is a Cloud ERP Software that is used for Manufacturing, Distribution and Services for Small & Medium Enterprises, while HRCMS is an all-in-one cloud based software, catering to all human resource needs from attendance taking and tracking to welfare management.

# 3.0 Pen-Test Schedule

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Date | Activity | Time Start | Time End | Name of student | Your home’s Public IP Address | Name of ISP |
| 26/12/2021-  27/12/2021 | Scanning the website (DirbBuster) | 4.00PM | 12.00AM | Neo Rei Siang Edward | 116.88.97.224 | Starhub |
| 27/12/2021 | Scanning the website  (Wfuzz) | 1.00PM | 1.20PM | Neo Rei Siang Edward | 116.88.97.224 | Starhub |
| 27/12/2021 | Scanning the Website  (Skipfish) | 1.30PM | 1.45PM | Neo Rei Siang Edward | 116.88.97.224 | Starhub |
| 27/12/2021 | Scanning the Website  (XSSSniper) | 2.00PM | 2.05 PM | Neo Rei Siang Edward | 116.88.97.224 | Starhub |
| 27/12/2021 | Scanning the Website (Wapiti) | 2.10PM | 2.15 PM | Neo Rei Siang Edward | 116.88.97.224 | Starhub |
| 01/01/2022 | Scanning the website | 12.56PM | 3.43PM | Mabel Choi JingYi | 42.60.38.20 | Singtel |
| 01/01/2022 to 02/01/2022 | Scanning the website | 11.23PM | 12.56AM | Mabel Choi JingYi | 42.60.38.20 | Singtel |
| 08/01/2022 | Scanning the website | 8.00PM | 10.00PM | Mabel Choi JingYi | 116.87.130.19 | Starhub |
| 18/01/2022 | Scanning the website | 11.42AM | 1.14PM | Mabel Choi JingYi | 116.87.130.19 | Starhub |
| 18/1/2022 | Scanning the website | 2.00PM | 2.30PM | Ow Kai Jie Clarence | 42.60.238.38 | Singtel |
| 20/1/2022 | Scanning the Website | 9.00AM | 12.00PM | Ow Kai Jie Clarence | 42.60.238.38 | Singtel |
| 23/1/2022 | Scanning the Website | 3.00PM | 3.10PM | Ow Kai Jie Clarence | 42.60.238.38 | Singtel |
| 10/1/2022  -  23/1/2021 | Manual Testing | 12.00AM | 11:59PM | Neo Rei Siang Edward | 116.88.97.224 | Starhub |
| 13/01/2022 - 31/01/2022 | Manual Testing | 12.00AM | 5.00PM | Mabel Choi JingYi | 116.87.130.19 | Starhub |
| 8/1/2022  -  29/1/2022 | Manual Testing | 12.00AM | 11:59PM | Ow Kai Jie Clarence | 42.60.238.38 | Singtel |

# 4.0 Information Gathering Summary Findings

## 4.1 Passive Reconnaissance

### 4.1.1 Ping

Ping is used to query a computer or server on a network to see if there is a connection to it. With ping, we are also able to find out the IP address of the hostname of the web application, which is, “198.54.115.179”.

Please refer to appendix section 9.6 for the image of the code used and the results attained.

### 4.1.2 Nmap

NMap refers to a network mapper that is used to find live hosts on a network, perform port scanning, ping sweeps, and detect the operating system or a version of a server.

The “-O” is used to detect and guess the operating system that is used by the server, while the “-O --osscan-guess” is used to guess the operating system that is used by the server more aggressively, and the “-O -sV” is used to guess the version of the service that is provided by the server.

Please refer to appendix section 9.7 for the image of the code used and the results attained.

### 4.1.3 WhatWeb

Whatweb was used to find out more information about the website. From this command we can guarantee the ip address of the targeted website is 198.54.115.179 as comparing the result of this tool and “ping” gives the same address. We can also see that this website is hosted in the United States. We can also identify the technologies hrcms-admin is using which are HTMLS, HTTPServer, LiteSpeed, and x-turbo-charged-by HTTP headers.

Please refer to appendix section 9.8 for the image of the code used and the results attained.

### 4.1.4 Netcraft

Netcraft is an internet services company that is based in the United Kingdom providing internet security services, including cybercrime disruption, application security testing and automated vulnerability scanning. With Netcraft, we are able to get more information about the web application that we are pen testing while allowing us to know more about the technology used by the web application as well.

Please refer to appendix section 9.9 for the image of the code used and the results attained.

### 4.1.5 HTTP Methods

We tried to see the list of HTTP methods that can be done on the website. In order to do so, we used the curl -X OPTIONS command. ‘Curl’ is a command line tool that developers use to transfer data to and from a server. It allows the user to communicate with the server through different HTTP methods. However, no HTTP methods could be identified.

Please refer to appendix section 9.10 for the image of the code used and the results obtained.

### 4.1.6 nslookup

NSLookUp, also known as, name server lookup, is a utility program that displays the IP address of a hostname of the hostname of an IP address by querying the domain name system server.

#### 4.1.6.1 NSLookUp using kali terminal

With the terminal in kali, we were able to find the public IP address of the web application that we are pen-testing, which is, 192.54.115.179.

Additionally, we were also able to find the name of the web application hosting platform that HRCMS is using to host its website, which is, “namecheaphosting”.

Please refer to appendix section 9.11.1 to see the results obtained from the tool.

#### 4.1.6.2 NSLookUp using nslookup.io

NsLookup.io is an online tool that is used to find DNS records for a domain name. We entered the URL of the web application, “hrcms-admin.tri-niche.com”, and were able to find out that the web application hosting platform, “namecheaphosting”, used by HRCMS is located in America.

Please refer to appendix section 9.11.2 to see the results obtained from the website.

### 4.1.7 dnsenum

Dnsenum is a tool that uses a multithreaded perl script to enumerate DNS information of a domain. It also discovers non-contiguous ip blocks. The main purpose of using Dnsenum is to gather as much information as possible about a domain. In this case, we can see that hrcms-admin has blocked the dnsenum script, preventing us from gaining information about the name servers available in the domains.

Please refer to appendix section 9.12 to see the results obtained from the tool.

### 4.1.8 What CMS

What CMS is a tool that is used to detect the Content Management System of a website. It helps to find out the name of the software of web framework, programming language and web server used by hrcms-admin. In this case, we can see that hrcms-admin uses codeigniter as the web framework, PHP as the programming language used and Litespeed as the web server. This allows us to find out more about these software and the possible known security vulnerabilities they have.

Please refer to appendix section 9.13 to see the results obtained from the tool.

### 1.1.9 Security Headers

Security headers are directives that are used by web applications to configure security defenses in web browsers. There are many different types of security header, with each helping the website in a different way.

Please refer to appendix section 9.14 to see the results obtained from the tool.

### 1.1.10 Business Site Map

#### 1.1.10.1 Employer Account

Diagram

Description automatically generated

#### 1.1.10.2 Employee Account

Diagram

Description automatically generated

## 4.2 Active Reconnaissance

### 4.2.1 DirBuster

We tried using the tool, “DirBuster” in Kali Linux. This is a tool that brute forces the website and tries to search for available directories. We used the medium word list for this tool and this tool would use each word in the text file to see if a directory can be found. However, each of the words in the medium word list gave a header response of 301.

Please refer to appendix section 9.15 to see the interface settings and results obtained from the tool.

### 4.2.2 Dirb

Although it is almost the same as dirbuster, Dirb uses a different word list for directory brute forcing. Hence, this tool can be used to add on to dirbuster and possibly cross reference to make sure the results are reliable as Dirbuster is also known to provide quite a lot of false-positive results.

Please refer to appendix section 9.16 to see the results obtained from the tool.

### 4.2.3 Wfuzz

We decided to use Wfuzz instead for directory brute forcing and decided to use the common word list for the tool. This word list consists of words that are commonly used for directories. Most of the words gave a response of 404 which means that there is no directory. However, there were a few words that gave a header response of 200, which means a successful connection was made to that directory.

Please refer to the images in the appendix at 9.17 to see the pages returned by these directories.

### 4.2.4 SQL MAP

SQLmap is a tool that is used in penetration testing to detect and exploit SQL injection flaws. It also automates the process of detecting and exploiting SQL injection. SQL injection can take advantage of any database that makes use of and utilities SQL, as SQL injection can affect any websites or web applications that might have SQL databases linked to it. Some examples are MySQL, SQL Server, Oracle and many more.

Based on the result, we can conclude that all the requests that we had made to the web server were not successful as the web application firewall has blocked the connection.

Please refer to appendix section 9.18 to see the results obtained from the tool.

### 4.2.5 SSL Labs

SSL Labs is a collection of documents, tools and thoughts related to SSL. This serves as a great attempt to understand how SSL is deployed, and an attempt to make it better. In this case, we can use SSL Labs to find out if the SSL certificate has expired or has any weaknesses.

Please refer to appendix section 9.19 to see the results obtained from the tool.

### 4.2.6 Network Diagram

Diagram

Description automatically generated

### 4.2.7 Website Architecture Diagram

Diagram

Description automatically generated

### 4.2.8 Domain Site Map

#### 4.2.8.1 Employer Account

Chart, waterfall chart

Description automatically generated

#### 4.2.8.2 Employee Account

Chart, waterfall chart

Description automatically generated

## 4.3 Vulnerability Scanning

### 4.3.1 OWASP ZAP

OWASP ZAP is an open-source web application security vulnerability scanner, intended for users new to application security as well as professional penetration testers. It is also a dynamic application security testing tool for finding vulnerabilities that exist in web applications.

Please refer to appendix section 9.20 to see the results obtained from the tool.

### 4.3.1.1 OWASP ZAP - Employer Account

Based on the results, there are not many security vulnerabilities that we need to be concerned about as with some security configuration, we would be able to lower the risk level identified.

**Table

Description automatically generated**

Please refer to appendix section 9.20.1 to see the detailed steps taken.

### 4.3.1.2 OWASP ZAP - Employee Account

Based on the results, there are not many security vulnerabilities that we need to be concerned about as with some basic security configuration, we would be able to mitigate away the risk level.

Graphical user interface, table

Description automatically generated

Please refer to appendix section 9.20.2 to see the detailed steps taken.

### 4.3.2 Nessus

Nessus is a proprietary vulnerability scanner, which scans for network security vulnerabilities, misconfigurations, denial of services vulnerabilities, and even default or absent passwords that could be tied to a user account. We ran a scan on the HRCMS web application, “hrcms-admin.tri-niche.com” and there are some concerns that we should take note of, specifically those with the Critical and High Vulnerability alerts.

Please refer to appendix section 9.21 to see the results obtained from the tool.

### 4.3.3 Nexpose

Nexpose is a vulnerability scanner which aims to support the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting and mitigation. It also integrates with Rapid7’s Metasploit for vulnerability exploitation.

Please refer to appendix section 9.22 to see the results obtained from the tool.

### 4.3.4 Skipfish

Skipfish is an automated tool that can be used to scan for and identify vulnerabilities that can be found on the hrcms-admin website. The command we use for the skipfish tool is “skipfish -d 16 -M -E -U -o skipfish\_results5 <https://hrcms-admin.tri-niche.com/>”.

The results we gained from the skipfish scan showed that there were a few vulnerabilities with the most critical stating that there is a shell injection vector. However, most of these vulnerabilities that were flagged by the tool were related to the recaptcha page and thus are not accurate vulnerabilities. For example, for the shell injection vector, skipfish said that we can submit ‘false’ and it will give us a successful header response with code 200. However, the page that was redirected was a captcha page, and thus it did not perform a proper shell injection.

Please refer to appendix section 9.23 to see the code used, results attained and an example of a HTTP trace from Skipfish.

## 4.4 XSS Scanning

### 4.4.1 XssSniper

We tried to find XSS vulnerabilities on the hrcms-admin website through the use of automated tools. We first used XSS Sniper which is a XSS discovery tool that has mass discovering functionalities. We used the command, “python xsssniper.py -u <https://hrcms-admin.tri-niche.com> --crawl --form”. However, the results from XSSSniper showed that it found zero possible XSS points.

Please refer to appendix section 9.24 to see the code used and results obtained from “XssSniper” tool.

### 4.4.2 Xsser

Xsser is an automatic tool that is used to detect, exploit, and report on XSS vulnerabilities in web-based applications. However, Xsser was unable to find any possible XSS vulnerabilities on the hrcms-admin website.

Please refer to appendix section 9.25 to see the results obtained from the “Xsser” tool.

### 4.4.3 Wapiti

Next, we tried to use wapiti to detect vulnerabilities. Wapiti is an open source tool that scans web applications for multiple vulnerabilities such as database injections, file disclosures, XSS and command execution attacks. The command used was “sudo wapiti -u <https://hrcms-admin.tri-niche.com/> -o /home/kali/Desktop”.

From the results of the wapiti scan, it stated there were five vulnerabilities. The first is related to Content Security Policy Configuration where the Content Security Policy is not set. The rest of the four vulnerabilities are related to HTTP Secure Headers. The second vulnerability is that X-Frame Options are not set. The third vulnerability is that X-Content-Type-Options is not set. The fourth is that X-XSS-Protection is not set. The last vulnerability is that the Strict-Transport-Security is not set.

Image of the code used and proof of these vulnerabilities can be found at appendix section 9.26

### 4.4.4 ZAP Fuzzing

Fuzzing is a technique that submits a lot of invalid or unexpected data to a target. It also is an automated software testing technique that involves providing invalid, unexpected or random data as inputs to an input field or entry point. It can be used for XSS scanning as there is a built-in library of XSS scripts in ZAP that can be used on a defined field.

From the results, we can see a lot of false positives, which indicates to us that the field that we had fuzzed is not cross site scriptable.

Graphical user interface, text, application

Description automatically generated

Please refer to appendix section 9.27 to see the results obtained

# 5.0 Vulnerabilities Summary Findings

## 5.1 Vulnerability Findings Matrix Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| #No | Vulnerability Finding | Severity Classification | OWASP Number & Name | CVW & CWE Details |
| 1 | Unauthorised Access to Administrative Pages (POC) | Critical | 5 - Broken Access Control | CWE-285: Improper Access Control (Authorization) |
| 2 | SSL Stripping | Critical | 3- Sensitive Data Exposure | CWE-200: Exposure of Sensitive Information to an Unauthorized Actor |
| 3 | Stored Cross-Site Scripting Vulnerability  (POC) | High | 7 - Cross-Site Scripting | CWE-79: Failure to Preserve Web Page Structure ('Cross-site Scripting') |
| 4 | Authentication Brute Force Vulnerability (POC) | High | 2 - Broken Authentication | CWE-307: Improper Restriction of Excessive Authentication Attempts |
| 5 | Verbose Errors  (POC) | High | 6 - Security Misconfiguration | CWE-209:Information Exposure Through an Error Message |
| 6 | Directory Traversal Attack (POC) | Medium | 5 - Broken Access Control | CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| 7 | Exposed Directories  (POC) | Medium | 6 - Security Misconfiguration | CWE-548: Information Leak Through Directory Listing |
| 8 | Insufficient Logging & Monitoring (POC) | Medium | 10 - Insufficient Logging & Monitoring | CWE-778: Insufficient Logging |
| 9 | Weak Password Requirements | Medium | N.A. | CWE-521: Weak Password Requirements |
| 10 | Missing Security Headers | Low | N.A. | N.A. |

**\* All descriptions of the vulnerability entries with Proof-Of-Concept (POC) can be found in Section 6.0. \***

**\*The HRCMS web application had no XXE and Insecure Deserialization vulnerabilities\***

## 5.2 Missing Security Headers

### 5.2.1 Proof of Vulnerability

Graphical user interface, website

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

### 5.2.2 Summary of Findings

Using the tools, “Security Headers” and “Wapiti”, we managed to identify a total of seven security headers that were reported to have been missing. These headers are, “Strict-Transport-Security”, “Content-Security-Policy”, “X-Frame Options”, “X-Content-Type-Options”, “Referrer-Policy”, “Permissions Policy” and “X-XSS-Protection”.

These missing security headers are classified as “Low” risk because a website can still be relatively secure without the use of these headers. These headers definitely do help and protect the websites but they usually serve as additional protection. It enhances the overall security of the website and can reduce the potential vulnerabilities faced by the websites. However, there are other more important security features that can be prioritised over the security headers. Furthermore, if there already are proper implementations of other security features, the website should be safe from vulnerabilities and do not necessarily need these security headers. Thus, we feel that the implementation of security headers acts as another layer of protection and is not an immediate need to have.

## 5.3 Weak Password Requirements

5.3.1 Proof of Vulnerability

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

5.3.2 Summary of Findings

As we can see from the image above, the password in which we have tried to set for an account is “123”. When we click on Save changes, the old password managed to update and we were able to log in to the account. “123” is a very weak password because it fails several strong password requirements.

This vulnerability is part of the “Medium” risk category because attacks can abuse weak passwords to gain unauthorised access to the website. Attackers are able to conduct brute force attacks on users accounts so as to gain unauthorised access to these accounts. This can be an even greater threat for the website if the attacker is able to get hold of an employer account as the attacker will be able to have administrative privileges and can disrupt the entire website.