Sri Lanka Institute of Information Technology

Assignment 02 Report

IE3022

**Penetration testing report based on the lab work performed for the module.**

**Applied Information Security – IE3022**

**B.Sc. (Hons) in Information Technology**

**Student Details**

|  |  |
| --- | --- |
| **Student ID** | **Student Name** |
| IT22560094 | Ranasinghe R.A.D.T.M |

# Overview

In this report, we present the findings and assessments resulting from a comprehensive penetration testing conducted by PentestRus on behalf of Mayo Industries. The test, which includes network and application assessments, was performed by respective teams which are red team, blue team and purple team each with different roles and responsibilities. This report offers insight into the potential vulnerabilities identified, anticipated threats, and recommendations for enhancing Mayo industry's security posture.

# Introduction

Mayo industries, a prominent organization within the sector, recognized the importance of securing its digital infrastructure and enlisted the expertise of PentestRus, which is a powerful digital security company provides Vulnerability Assessment and Penetration Testing (VAPT) services. This report marks a pivotal milestone in the collaboration between PentestRus and Mayo industries, aimed at safeguarding the organization’s digital assets and intellectual properties.

In the preparation of the comprehensive penetration testing, our engagement was initiated with the assumption that a myriad of vulnerabilities may exist within the Mayo Industries network and applications. To ensure an accurate reflection of the potential risks faced by the organization, we selected several vulnerabilities to assess.

Software vulnerabilities like insecure designs, cryptographic failures, buffer overflows, and the unrestricted uploads of dangerous file types. Network vulnerabilities, implementation of weak firewalls, insecure wireless networks, and vulnerabilities related to incoming phishing emails and social engineering tactics withing those mails. Web applications vulnerabilities such as, SQL injections, cross-site scripting, cross-site request forgery, security misconfiguration, broken authentication and path traversals.

It is important to note that while these assumed vulnerabilities are a significant focus of our assessment, the digital landscape is fraught with numerous other potential weaknesses that organizations typically face. This may include misconfigured systems, out-of-date network components, weak password policies, lack of security awareness training, and the possibility of insider threats. Our engagement with Mayo industries aims to holistically assess and identify these aspects as well, although the primary focus remains on the above-mentioned technical vulnerabilities.

By adopting this inclusive approach, we aim to provide a thorough evaluation of Mayo industry's security posture, helping the organization understand and mitigate potential threats beyond the assumed vulnerabilities. Through this comprehensive report, we strive equip mayo industries withing the insights and recommendations required to improve its security measures and safeguard against both known and challenges in the ever-evolving digital landscape.

# Methodology

The red team is prepared to execute a multifaced approach to access potential technical vulnerabilities withing Mayo industries infrastructure. The assumption is that these vulnerabilities might exist, and we aim to simulate real world scenarios to examine the organization's security resilience. The following is the brief overview of the methodologies we assume will be employed,

Software vulnerabilities-we anticipate examining potential software vulnerabilities such as insecure design, cryptographic failure, buffer overflows, and the unrestricted uploads of dangerous file types. Vulnerable and outdated components will be checked for potential exploitation.

Network vulnerabilities-The assessment will extend to network security, withing the focus on the assumption of poor firewall configurations, insecure wireless networks, and security vulnerabilities related to incoming phishing mails and social engineering attacks. We will assume the presence of outdated or unpatched networks and will assess them for weaknesses.

Web application vulnerabilities-In the section of web application security, we assume the presence of vulnerabilities including SQL injections, cross-site scripting, cross-site request forgery, security misconfigurations, broken authentication and path traversals. Each of these vulnerabilities will be assumed for potential exploitations.

# Scope of limitation

The scope of this penetration test process helps to evaluate Mayo industries network and application security, by assuming the potential vulnerabilities exists. No specific zones are deemed off-limits, allowing for a thorough examination of the entire network. However, it's important to note that the focus is on assuming these vulnerabilities rather than risk management reporting at this stage. Additionally, this test is conducted with the following constraints: and limitations in mind.

**Time constraints**- this test is executed withing a specific timeframe.

**Scope limitation**-External factors beyond the network, such as physical security, are not assumed to be assessed in this report.

**Legal and ethical considerations**-all activities are assumed to be carried out within legal and ethical boundaries to ensure no disruption to Mayo industries operations.

These modified sections take into account that the vulnerabilities being addressed are assumptions rather than known issues and provide a clear framework for the rest of the report.

# Red team Findings

The red team assumed a curtail role in conducting a comprehensive assessment of Mayo industries infrastructure, focusing on the identification and analysis of potential vulnerabilities. Red team involves simulating a cyber-attack against an organization’s network, applications, and systems to identify vulnerabilities and potential weaknesses. The goal of cyber red teaming is to objectively assess an organization’s cyber security posture, identify gaps and vulnerabilities, and provide recommendations to improve the organization’s security posture. Red Teaming is a proactive security assessment methodology that helps organizations to identify and mitigate security risks by simulating real-world attacks. In the context of Cyber Security and Ethical Hacking, Red Teaming involves a team of security experts attempting to penetrate an organization's systems and networks using the same tactics, techniques, and procedures (TTPs) as real-world attackers.[1]

Additionally, the red team assessed the severity of each vulnerability, considering the factors such as potential impact and ease of exploitation. They document their findings, providing a detailed description of each vulnerability's location and potential exploitation risks. The red team offered recommendations for remediation, guiding Mayo industries in strengthening their security posture and preventing future exploits. Their realistic threat simulation mirrored the tactics of actual threat actors, collaborating closely with the blue and purple teams to ensure holistic assessment.[2]

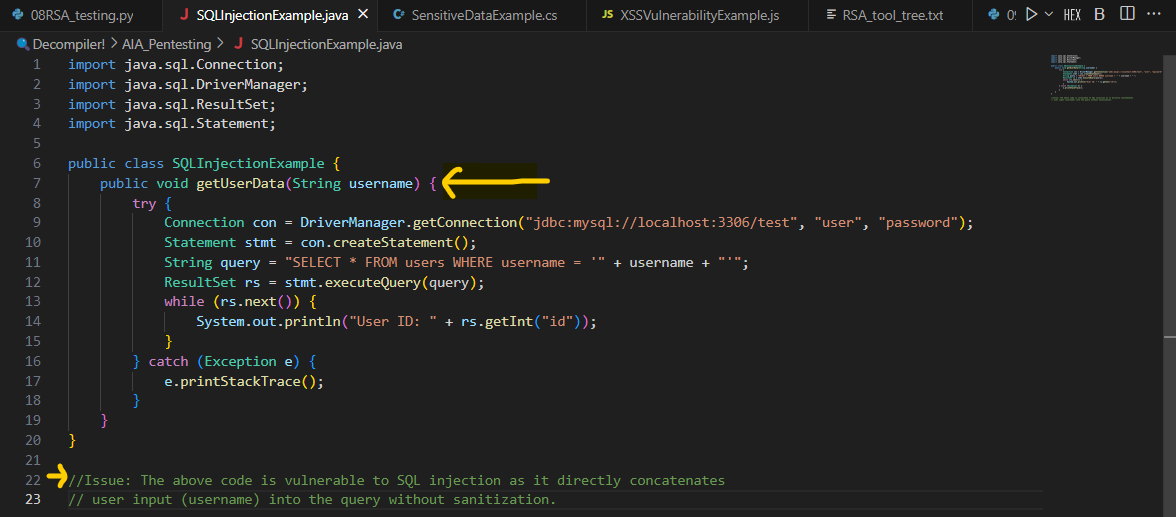
### Findings and Insights

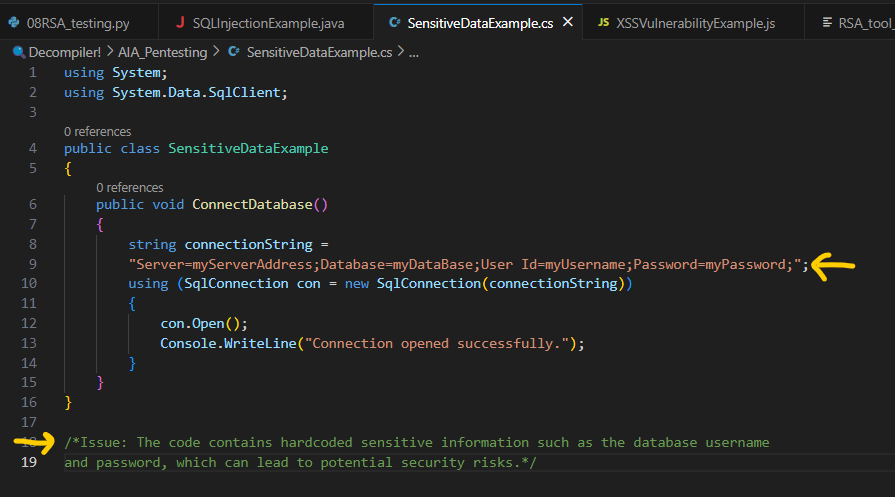
The findings presented in this section reveal the vulnerabilities identified by the red team during their assessment of Mayo industries. These vulnerabilities can be categorized by software, network and web application, which are the main three digital parts of the organization. Each of these vulnerabilities are accompanied by a severity assessment, offering insights on the potential impact of exploitation. The read team’s recommendations for remediation provide actionable steps to bolster the organization’s security measures. These below red team findings will help to understand Mayo industries security strengths and weaknesses, which helps them to navigate ever evolving landscape of potential cyber threats and security challenges.

#### Software Vulnerabilities

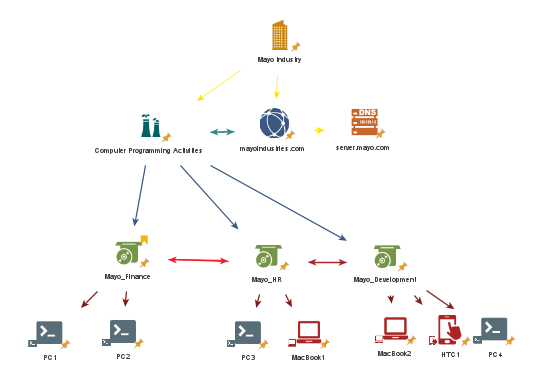
|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability | Description | severity | Detecting tools and techniques |
| Insecure design | Insecure design means weaknesses stemming from flawed software architecture and initial planning.  This vulnerability may occur because of improper access controls, inadequate threat modeling and insufficient security practices during the software design and maintain phases. | High.  Insecure designs can lead to pervasive security issues that are challenging to mitigate once software is developed. | Manual code reviews. (image 01) (image 02)  Secure code review tools like Checkmarx and Fortify.  Maltego tool for information gathering and reconnaissance. (image 03) (image 04)  Recon-ng tool for data discovery and reconnaissance. (image 05)  Dn-spy tool for modify insecure software codes (image 06) |
| Cryptographic failures | Cryptographic failures include issues with encryption and decryption processes.  This can result from using weak encryption algorithms, improper key management, or inadequate protection of cryptographic keys. | High.  Cryptographic failures can expose sensitive data, leading to data breaches and potential regulatory violations. | Nessus. (image 07)  Wireshark for analyzing SSL/TLS traffic. (image 08)  John the ripper for password cracking. (image 09)  Hydra for password cracking including SSH. (image 10) |
| Buffer Overflow | Buffer overflow vulnerabilities occur when a program writes more data to a buffer than it can hold.  That potentially leads to memory corruption or the execution of malicious code. | High.  Exploiting buffer overflows can result in unauthorized code execution and also leads to compromise the software systems. | Valgrind (image 11)  Immunity Debugger (image 12)  Maltego for information gathering and reconnaissance (image 03) |
| Unrestricted Upload of Dangerous File Types | This vulnerability arises when an application allows the unrestricted uploading of files without proper validation.  Attackers can upload malicious files to compromise the system. | Moderate to high.  Depending on the files uploaded, this vulnerability can lead to various levels of compromise. | OWASP ZAP for analyzing file upload vulnerabilities. (image 13)  Burp Suite for intercepting and modifying file uploads (image 14) (image 15) (image 16)  Metasploit for testing file upload vulnerabilities (image 17)  The Harvester for gathering email addresses and information (image 18) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Code Review

(image 01)

(image 02)

Maltego tool



(image 03)

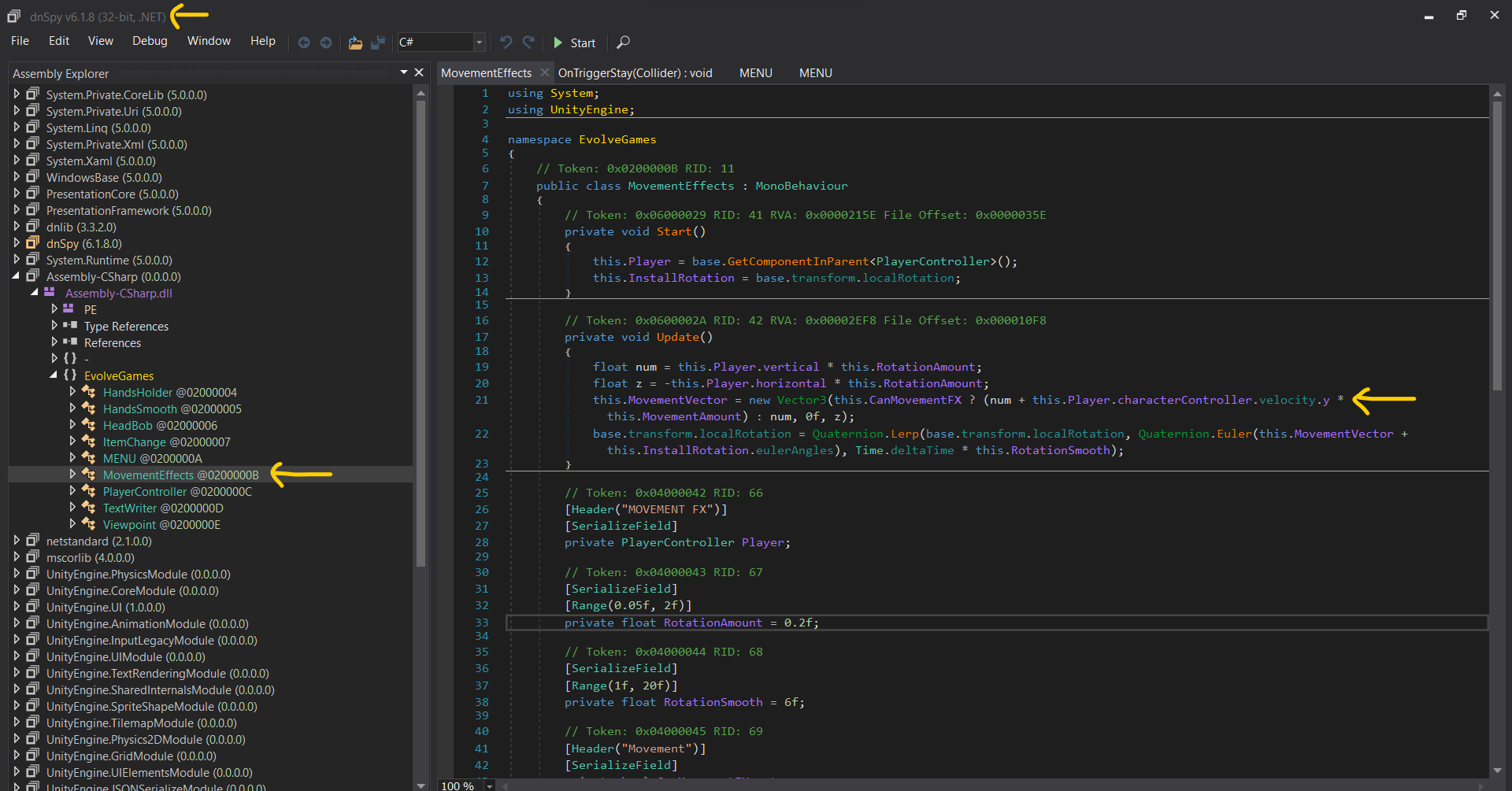
(image 04)

Recon-ng reconnaissance

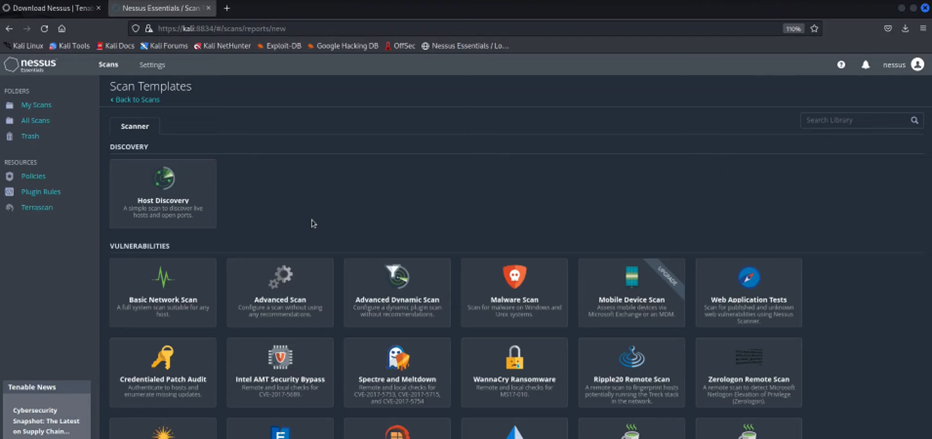


(image 05)

Dn-spy software cracker

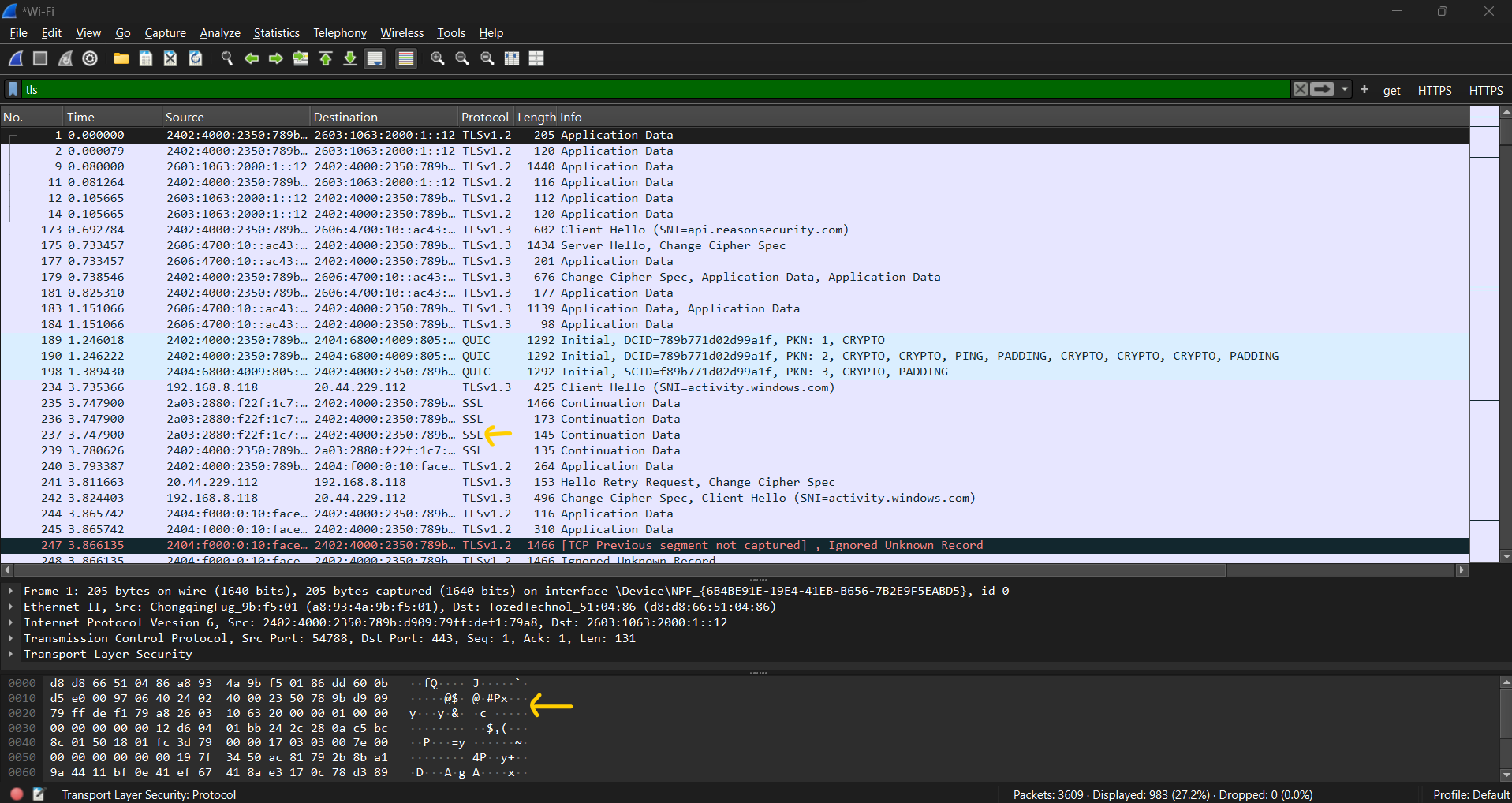
(image 06)

Nessus scanner



(image 06)

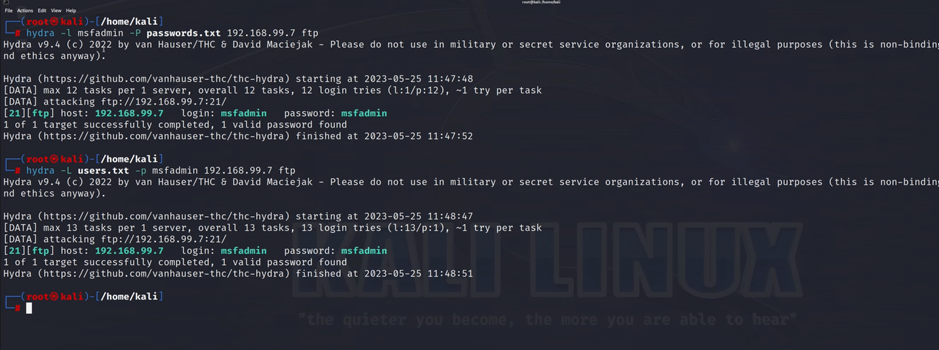
Wireshark

(image 07)

John the ripper

(image 09)

Hydra

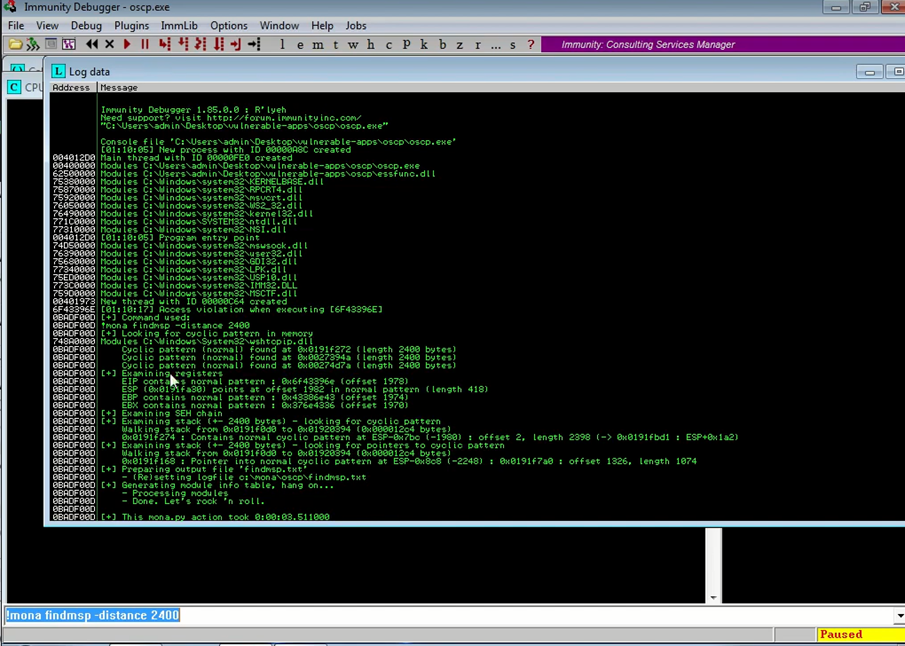


(image 10)

Valgrind

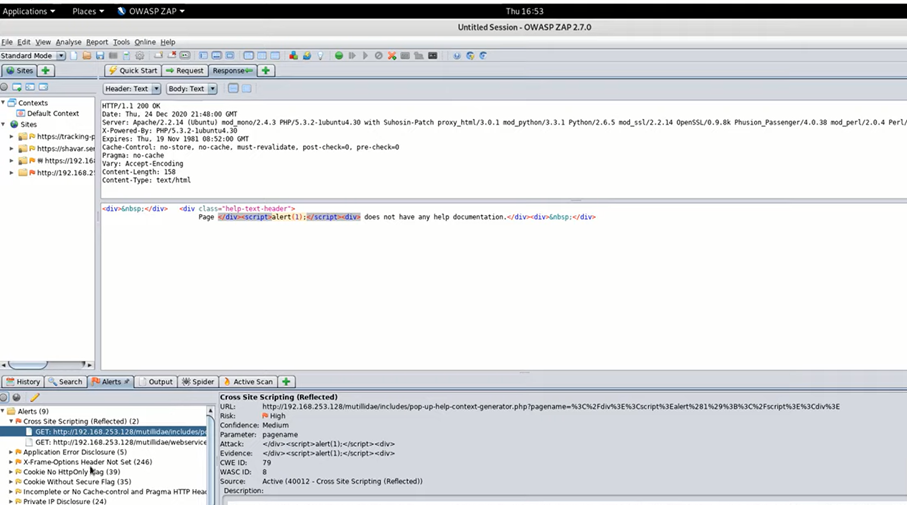
(image 11)

Immunity Debugger



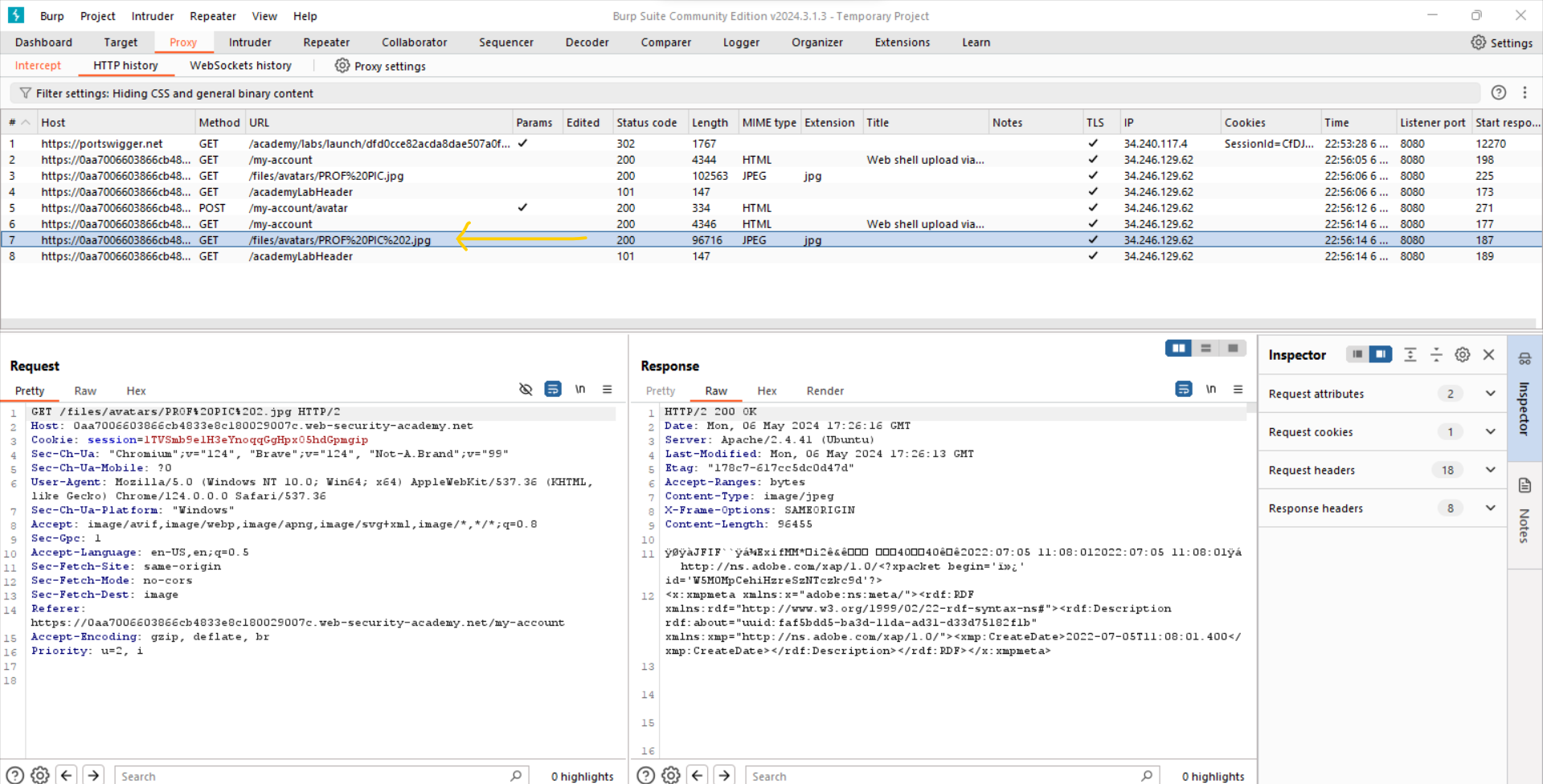
(image 12)

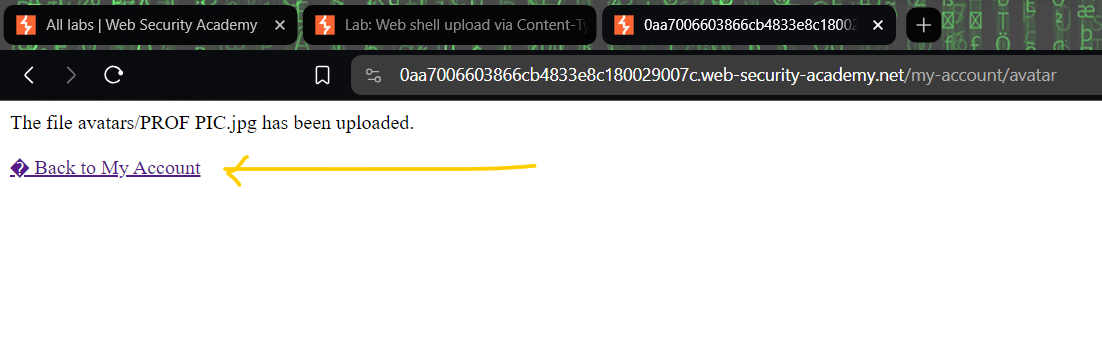
OWASP ZAP



(image 13)

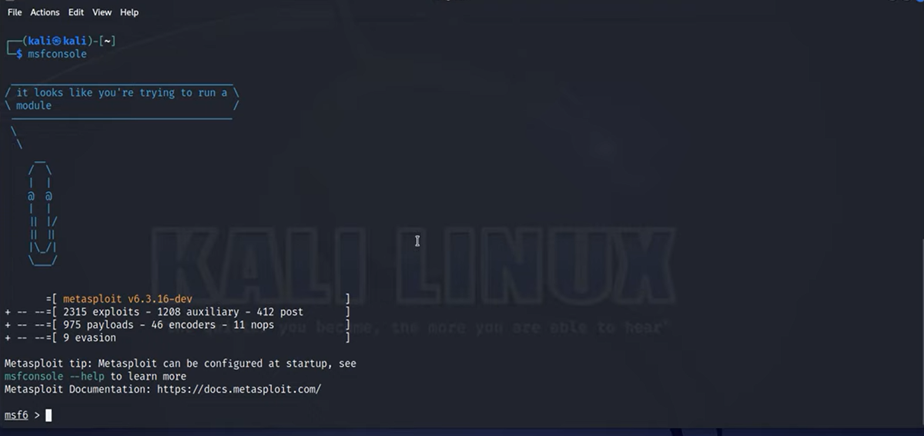
Burp Suite

(image 14)

(image 15)

(image 16)

Metasploit



(image 17)

The Harvester

#### Network Vulnerabilities

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability | Description | severity | Detecting tools and techniques |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

#### Web application vulnerabilities

|  |  |  |  |
| --- | --- | --- | --- |
| Vulnerability | Description | severity | Detecting tools and techniques |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

References

[1] Sarang Tumne, “Practical Red teaming Field-Tested strategies for cyberwarfare”, 2023, [online], Available: [1725939597913 (licdn.com)](https://media.licdn.com/dms/document/media/D4D1FAQFzWikGrFLsIQ/feedshare-document-pdf-analyzed/0/1725939597913?e=1729123200&v=beta&t=yOV7bB4dJXCbZLa5W_IsbFcXbaYCQCPwzUVCNNMlAko)

[2] S. Foster, "Vulnerabilities Definition: Top 10 Software Vulnerabilities," Perforce, July 2020. [Online]. Available: <https://www.perforce.com/blog/kw/common-software-vulnerabilities>.