

**VULNERABILITY ASSESSMENT AND PENETRATION
TESTING ON API
INSTITUTION TRAINING – MINOR PROJECT**

(22SSP539)

Submitted By
DHARSHAN P
22MSS009

Under the Guidance of

Dr.V.Usharani, M.C.A., M.Phil., Ph.D.,

Associate Professor

Department of Software Systems

In Partial Fulfillment of the Requirements for the Award of the Degree of

MASTER OF SCIENCE IN SOFTWARE SYSTEMS

(Five-Years Integrated Course)



DEPARTMENT OF SOFTWARE SYSTEMS

PSG COLLEGE OF ARTS & SCIENCE

An Autonomous College - Affiliated to Bharathiar University

Accredited with 'A++' Grade by NAAC (4th Cycle)

College with Potential for Excellence (Status Awarded by the UGC)

Star College Status Awarded by DBT - MST

An ISO 9001:2015 Certified Institution

Coimbatore - 641 014

October 2024

DEPARTMENT OF SOFTWARE SYSTEMS

PSG COLLEGE OF ARTS & SCIENCE

An Autonomous College - Affiliated to Bharathiar University

Accredited with 'A++' Grade by NAAC (4th Cycle)

College with Potential for Excellence

(Status Awarded by the UGC)

Star College Status Awarded by DBT - MST

An ISO 9001:2015 Certified Institution

Coimbatore - 641 014

CERTIFICATE

This is to certify that this project work entitled **“VULNERABILITY ASSESSMENT AND PENETRATION TESTING ON API ”** is a bonafide record of work done by **DHARSHAN P 22MSS009** in partial fulfillment of the requirements for the award of Degree of **Master of Science in Software Systems** (Five Years Integrated Course) of Bharathiar University.

Faculty Guide

Head of the Department

Submitted for Viva-Voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I, **DHARSHAN P 22MSS009**, hereby declare that this project work entitled **“VULNERABILITY ASSESSMENT AND PENETRATION TESTING ON API”** is submitted to PSG College of Arts & Science, Coimbatore in partial fulfillment of the requirements for the award of the degree of Master of Science in Software Systems, is a record of original work done by me under the supervision and guidance of **Dr.V.Usharani, M.C.A., M.Phil., Ph.D.,** Associate Professor, Department of Software Systems, PSG College of Arts & Science, Coimbatore.

This report has not been submitted by me for the award of any other Degree / Diploma / Associateship / Fellowship or any other similar degree to any other university.

Place : Coimbatore

Dharshan P

Date : 15.10.2024

(22MSS009)

ACKNOWLEDGEMENT

My venture stands imperfect without dedicating my gratitude to a few people who have contributed a lot towards the victorious completion for my project work.

I would like to thank **Thiru L. Gopalakrishnan, Managing Trustee, PSG & Sons Charities**, for providing me a prospect and surroundings that made the work possible.

I take this opportunity to express my deep sense of gratitude to **Dr. T. Kannaian, Secretary** of PSG College of Arts & Science, Coimbatore for permitting and doing the needful towards the successful completion of this project.

I express my deep sense of gratitude and sincere thanks to our Principal **Dr. D. Brindha** for her valuable advice and concern on students. I am very thankful to **Dr. M Umarani, Vice Principal** for her support towards my project.

I sincerely thank **Dr. K. V. Rukmani** Head of the Department, Department of Software Systems for her whole hearted help to complete this project successfully by giving valuable suggestions.

I convey my heartiest and passionate sense of thankfulness to my project guide **Dr.V.Usharani** Associate Professor, Department of Software Systems, for her timely suggestion which had enable me in completing the project successfully.

This note of acknowledgement will be incomplete without paying my heartfelt devotion to my parents, my friends and other people, for their blessings, encouragement, financial support and the patience, without which it would have been impossible for me to complete the job.

Dharshan P

(22MSS009)

SYNOPSIS

The project entitled “**Vulnerability Assessment and Penetration Testing on API**” is the most comprehensive audit and penetration service. Vulnerability analysis is performed to test the security posture of information systems. Penetration testing is an attempt to break into a system using methods and devices that real hackers use. The main purpose of penetration testing is to discover as many existing vulnerabilities as possible and develop viable solutions to fix the problems and improve the overall security of the system.

Penetration testing and vulnerability assessment perform two different tasks within the same scope, but often with different results. Each organization confirms that its security measures are working properly through vulnerability analysis and penetration testing. Methodologies include discovery, enumeration and vulnerability identification, vulnerability assessment, attack exploitation and initiation, reporting, external penetration testing, Internal penetration testing, before starting. Depending on the vulnerability, manual penetration testing or automated penetration testing can be performed. The main aim of the project is to perform the pen test on the API with the given credentials and generate the necessary reports accordingly.

TABLE OF CONTENTS

S.No	CONTENTS	PAGE NO
1	INTRODUCTION	
	1.1 Project Overview	2
	1.2 Module Description	3
2	TESTING ANALYSIS	
	2.1 Existing Testing	5
	2.2 Proposed Testing	5
3	SYSTEM CONFIGURATION	
	3.1 Hardware Specification	6
	3.2 Software Specification	6
4	SOFTWARE DESCRIPTION	
	4.1 Automated Testing Tools	7
	4.2 Semi-Automated Testing Tools	8
5	SYSTEM DESIGN	
	5.1 System Flow Diagram	9
	5.2 Input	11
	5.3 Output	12
6	SYSTEM IMPLEMENTATION & TESTING	13
7	CONCLUSION	14
8	SCOPE FOR FUTURE ENHANCEMENT	15
9	BIBLIOGRAPHY	16
10	APPENDIX	
	A. Screenshot	17
	B. Sample Coding	23

CHAPTER - 1

INTRODUCTION

1.1 PROJECT OVERVIEW

The cyber threat landscape is constantly evolving. So, it's not an IT system that was delivered correctly yesterday, certainly today. A threat is an event that exploits a vulnerability to damage an organization's assets. To prevent this, Organizations identify new vulnerabilities and fix or mitigate the acceptable level of risk.

Vulnerability Assessment and Penetration Testing (VAPT) describes a wide range of security assessment services. Designed to identify and remediate cybersecurity risks across an organization's IT inventory.

Understanding them is important to ensure that you choose the right type of assessment for your organization's needs of different types of VAPT services and their differences. This understanding is important to ensure testing as depth, breadth, scope and price can vary significantly offers the best value for money.

Vulnerability assessment is a rapid, automated scan of network devices, servers, and systems to identify keys. Vulnerabilities and configuration issues that attackers can exploit. We basically carry out within a network of internal devices and with a small footprint, it can be run daily. Penetration testing is a thorough, expert-led activity focused on identifying various possible routes to an attacker. It can infiltrate your network. In addition to vulnerabilities, it also identifies potential damage and harm. Another internal compromise that an attacker can perform through your perimeter.

In this project, an API penetration test will be performed to identify vulnerabilities, and penetration testing will be conducted to raise awareness of the security flaws in the application, allowing the organization to patch them and protect itself in the modern internet era.

1.2 MODULE DESCRIPTION

This module comprises a set of source files and build settings tailored for API penetration testing. It allows you to customize your project into various operational units, with the possibility of having multiple modules, where one module can depend on another.

1.2.1 INFORMATION GATHERING

Information gathering is a critical initial phase in API penetration testing. The more comprehensive the information collected about the API, the better equipped you will be to identify vulnerabilities and potential exploits.

- **Postman**
- **Burp Suite**

POSTMAN

Postman is used to send API requests, analyze responses, explore endpoints, validate authentication mechanisms, and identify potential vulnerabilities and data exposure.

BURP SUITE

Burp Suite is employed to inspect the API endpoints, helping to uncover valuable information about the API's functionality and potential vulnerabilities.

1.2.2 VULNERABILITY ASSESSMENT

A vulnerability assessment evaluates the security weaknesses across the API and estimates the likelihood of an attack by malicious actors. This process generates detailed reports and outlines mitigation strategies.

- **Zaproxy**
- **Report Generation**

ZAPROXY

Conduct a scan of the API using its IP address to provide results regarding vulnerability assessments.

REPORT GENERATION

Create a comprehensive vulnerability assessment report detailing findings and recommendations.

1.2.3 PENETRATION TESTING

This module involves executing various attacks to gain access to the API and simulate real-world scenarios that could compromise sensitive data. These tests help identify vulnerabilities and discover potential exploits within the API.

- **Exploitation**

EXPLOITATION

Attempt to exploit the API to identify any backdoors or security flaws present.

1.2.4 REPORT GENERATION

In this module, the report generation in API penetration testing involves summarizing findings, assessing vulnerabilities, providing recommendations, and documenting testing scope and methodology to communicate security risks effectively to stakeholders.

CHAPTER-2

TESTING ANALYSIS

2.1 EXISTING TESTING

Existing testing was done by manual inspection rather than the human review that typically tests the security impact of people, policies, and processes. Manual inspection may also include inspection of engineering decisions such as architectural design. Existing tests are also run using the old checklist which is only intended to check fewer topics.

DRAWBACKS

- Consumes longer period of time.
- Support material is not always available.
- Traditional checklist with few test cases.

2.2 PROPOSED TESTING

Automated and semi-automated testing has become a popular technique to help system designers think about possible security threats to their systems and applications. Automated testing can therefore be viewed as an application risk assessment. This allows designers to formulate strategies to mitigate potential vulnerabilities and focus their naturally limited resources and attention on the parts of the system that need it most.

FEATURES

- A real attacker's view of the system.
- New checklist with more test cases.
- Backdoors can be found easily.

CHAPTER – 3

SYSTEM CONFIGURATION

3.1 HARDWARE SPECIFICATION

- **PROCESSOR** : Intel Core i5
- **RAM** : 8 GB
- **CPU CLOCK SPEED** : 2.93 GHz and above
- **HARD DISK DRIVE** : 320 GB and above
- **HARDWARE** : Mouse & Keyboard

3.2 SOFTWARE SPECIFICATION

- **OPERATING SYSTEM** : Windows 11, Kali Linux (VMware)
- **WORKSTATION** : VMware
- **AUTOMATED TESTING TOOLS** : Burpsuite, Postman
- **SEMI-AUTOMATED TOOLS** : OWASP ZAP, JWT_Tool

CHAPTER – 4

SOFTWARE DESCRIPTION

4.1 AUTOMATED TESTING TOOLS

4.1.1 BURPSUITE

Burp Suite is an incorporated platform/graphical device for acting safely trying out of net applications. Its various tools work seamlessly together to support the entire testing process, from initial application attack surface mapping and analysis to security vulnerability discovery and exploitation. Burp Suite is installed on Kali Linux by default.

It aims to provide a comprehensive solution for security auditing of web applications. Besides basic features such as proxy server, scanner and intruder, this tool also includes advanced options such as spider, repeater, decoder, comparator, extender and sequencer.

4.1.2 POSTMAN

Postman is an integrated platform designed for API development and testing. Its diverse tools work together seamlessly to support the entire API lifecycle, from building and testing to documentation and monitoring. Postman can be installed on various operating systems, including Windows, macOS, and Linux.

The tool aims to provide a comprehensive solution for developers and testers working with APIs. In addition to basic features like sending requests and analyzing responses, Postman offers advanced functionalities such as environment management, automated testing with collections, and mock servers for simulating API responses. It also includes collaboration tools for team sharing and API documentation generation, making it an essential resource for efficient API development and security auditing.

4.2 SEMI-AUTOMATED TESTING TOOLS

4.2.1 OWASP ZAP

OWASP ZAP (Zed Attack Proxy) is an integrated platform designed for security testing of web applications. Its various tools work together seamlessly to support the entire testing process, from initial reconnaissance and scanning to vulnerability discovery and exploitation. ZAP is open-source and can be run on multiple platforms, including Windows, macOS, and Linux.

ZAP aims to provide a comprehensive solution for identifying security vulnerabilities in web applications. Alongside basic features like a proxy server and automated scanners, it includes advanced options such as active scanning, fuzzing, and a built-in scripting engine. ZAP also offers tools for session management, reporting, and integrations with CI/CD pipelines, making it an invaluable resource for security professionals and developers focused on improving application security.

4.2.2 JWT_TOOL

JWT Tool is a specialized platform designed for the creation, decoding, and verification of JSON Web Tokens (JWTs). Its user-friendly interface facilitates the entire process of working with JWTs, from generating tokens to inspecting their payloads and signatures. JWT Tool is web-based, making it easily accessible from any browser.

The tool aims to provide a comprehensive solution for developers and security professionals working with JWTs in authentication and authorization processes. In addition to basic features like token creation and decoding, JWT Tool offers advanced functionalities such as signature verification, algorithm selection, and expiration checks. It also includes options for visualizing token structure and payload data, making it an essential resource for ensuring secure and effective implementation of JWTs in applications.

CHAPTER - 5

SYSTEM DESIGN

System design is the process of defining properties, product structure, modules, links, and system data to meet specific needs. System design can be seen as the application of system theory to product development.

5.1 SYSTEM FLOW DIAGRAM

A system flow diagram is a graphical representation of data flow within a system in software development. This diagram consists of several steps that identify where inputs enter the system and where outputs exit the system. With the help of diagrams, you can control the event determination of your system and the flow of data into your system. A system flow diagram is therefore essentially a visual representation of the data flow, excluding the smaller parts and including the major parts of the system in order.

Like other types of flowcharts, system flowcharts consist of start/end terminals, processes, and decisions, all connected by arrows to show the flow and movement of data within the flow.

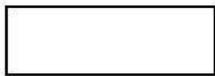
5.1.1 SYMBOLS



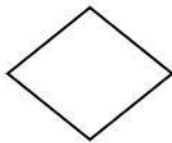
- The oval represents the start and endpoint.



- The arrow represents graphical flow into or out of process.



- The rectangle represents the process.



- The diamond represents the decision or the branching point.



- It represents the documents or reports.

SYSTEM FLOW DIAGRAM

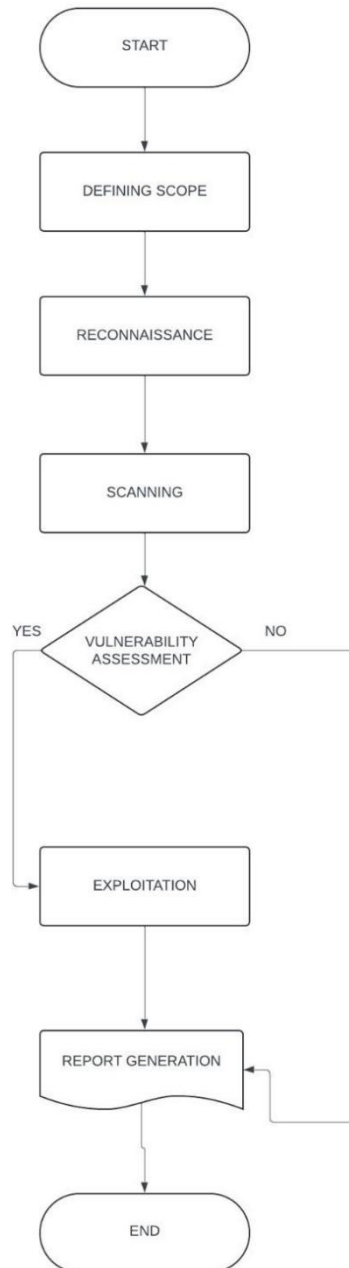


Figure 5.1 System Flow Diagram for the VAPT

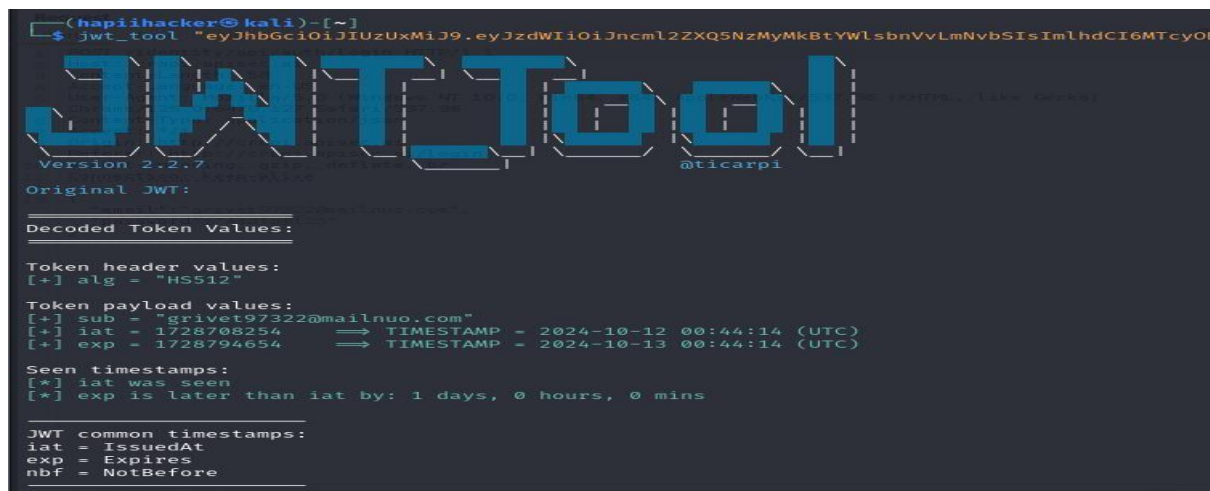
The flow starts from defining the scope of the testing (either black box, white box or greybox testing) as well as the URL and other details. Then the initial testing phase begins with the reconnaissance and scanning of the web URL provided. After that vulnerability assessment will be performed which is important stage before providing to the pen testing

and there is condition whether to perform penetration testing or perform only vulnerability assessment which depends upon the scope of the project. In the penetration testing stage, intense testing will be done to find more vulnerabilities of different severity and try to exploit the web application to gain the domain access in the exploitation stage. In analysis, overall analysis will be done for the test performed. Finally, the report will be generated with the necessary details of the vulnerabilities and a issue tracker will be created with all the test cases performed.

5.2 INPUT

Input design encompasses advanced specifications and data processing procedures necessary for transforming raw data into a usable format that can be accessed by computer systems. This process may involve reading data from written or printed text, keystrokes, or direct input into the system. The focus of input design is on managing the required volume of input, controlling errors, minimizing delays, reducing unnecessary steps, and simplifying the process. Additionally, the input is structured to ensure security and facilitate the maintenance of confidentiality.

FIGURE 5.2



```
(hapiihacker@kali)~$ jwt_tool "eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJncml2ZXQ5NzMyMkYlbnVvLmNvbSI6ImIldCI6MTcyODQ"
Version 2.2.7 @ticarpi
Original JWT:
Decoded Token Values:
Token header values:
[+] alg = "HS512"
Token payload values:
[+] sub = "grivet97322@mailnuo.com"
[+] iat = 1728798254    => TIMESTAMP = 2024-10-12 00:44:14 (UTC)
[+] exp = 1728794654    => TIMESTAMP = 2024-10-13 00:44:14 (UTC)
Seen timestamps:
[*] iat was seen
[*] exp is later than iat by: 1 days, 0 hours, 0 mins
JWT common timestamps:
iat = IssuedAt
exp = Expires
nbf = NotBefore
```

Figure 5.2 represents the jwt_tool to which user give the input of the target and the command to execute.

5.3 OUTPUT

Quality output alone, meets the needs of the end user and presents the information clearly. In any system, the results of the processing are transmitted to users and to another system automatically. In the output, it is determined how the information will be deleted so that it is needed as soon as possible with the release of a hard copy. It is a very important and direct source of information for the user. An efficient and intelligent output enhances system testing to help make user decisions.

FIGURE 5.3

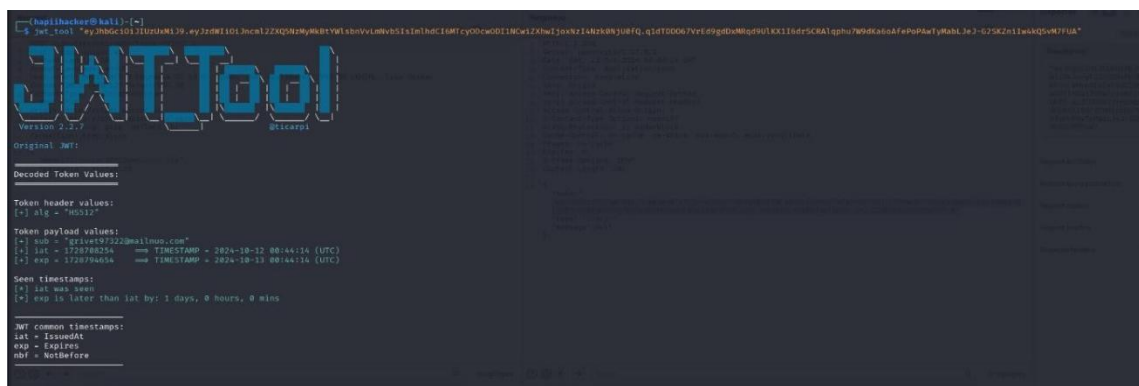


Figure 5.3 represents the api token requests & response using `jwt_tool`.

CHAPTER - 6

SYSTEM IMPLEMENTATION AND TESTING

6.1 SYSTEM TESTING

Evaluation is an important part of the success of this program. System testing makes sense that if all parts of the system are correct, the goal will be achieved successfully. System testing is the implementation phase aimed at ensuring that the system operates accurately and efficiently.

6.1.1 TESTING METHODOLOGY

BLACK BOX TESTING

Black Box Penetration Testing is a penetration testing service aimed at finding and exploiting system vulnerabilities as an outsider. In black box penetration testing, security experts receive no information about the target system prior to testing. Similar to the end user, except for the destination URL and (probably) access. This means that testers do not have access to the application's source code (other than publicly available code), internal data, structure, and design prior to testing. The name "black box" indicates a dark, uninformed starting point for testing.

Here's how to take advantage of the Black Box Pentest:

- Test your application as a hacker.
- Find exposed vulnerabilities in your network and apps.
- Tests your application at runtime, which helps identify implementation and configuration issues.
- Social engineering techniques can be used to detect security issues related to people.
- Detect security issues that arise from interactions with the underlying environment (eg, improper configuration files, unhardened operating systems and applications).
- Detect input/output validation errors, information leaks in error messages, and other issues.
- It can be cheaper to do black box penetration testing compared to other pen testing types such as gray box and white box.

CHAPTER - 7

CONCLUSION

With the number of data breaches on the rise, companies are urgently looking for new ways to protect their data. Internet is overflowing with information about how companies can protect their data. The truth is that businesses of all sizes need to use VAPT's excellent data protection solution. In this blog post, we discussed the importance of the VAPT solution and how it can help protect your business from malicious attacks. The best part is that it is affordable for all businesses.

Penetration testing is very important for any organization that takes cyber security seriously. It's a proactive approach to maintain a high level of security and protection against hackers because if a penetration tester can exploit vulnerabilities and can compromise your network, then a real hacker can. As we have heard about the famous The WannaCry ransomware attack that hit more than 2 million computers worldwide and demanded ransom payments in the form of bitcoins to unlock systems. This attack affected many large organizations. With such massive cyber-attacks happening these days, it is very important to perform penetration testing at regular intervals protect our information system from security breaches. This highlights the importance of conducting vulnerability assessments and penetration testing to prevent attackers from stealing our confidential data. Over with VA we can identify vulnerabilities and then with PT we can fix the vulnerabilities.

CHAPTER - 8

SCOPE FOR FUTURE ENHANCEMENTS

The scope of the VAPT determines which assets to scan and which to keep. The scope is decided in the VAPT planning stage and the whole process runs accordingly. The future of penetration testing lies in using artificial intelligence to refine results and make evaluations more efficient. But it is also important to understand the pen testers still need to use their experience and knowledge to ultimately decide what the best course of action is assessment. The future of penetration testing lies in the use of artificial intelligence to refine results and provide better evaluation effective. However, it is also important to understand that pen testers still need to use their experience and knowledge ultimately decide what is the best course of action to carry out the assessment.

Vulnerability Assessment and Penetration Testing (VAPT) are security services that focus on identifying vulnerabilities in the network, server and system infrastructure. Both services serve a different purpose and are performed to achieve a different one but complementary goals. VAPT is important to meet compliance standards. Protects your business from data loss and unauthorized access. In the future, we will focus on the practical implementation of vulnerability analysis and Penetration testing using tools like NMAP, WIRESHARK, SQLMAP, NESSUS, METASPLOIT and NIKTO.

CHAPTER – 9

BIBLIOGRAPHY

The following books and websites were referred during the analysis and execution phase of the project.

9.1 BOOK REFERENCES

1. “ API Security in Action”, Neil Madden.
2. “The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy”, Book by Patrick Engebretson.
3. “API Testing and Development with Postman”, Dave Westerveld.
4. “API Security: The Definitive Guide”, Neil McDonald.

9.2 WEBSITES

- 1) <https://university.apisec.ai/products/api-penetration-testing>
- 2) <https://github.com/Erdemstar/VulnerableApp4APISecurity/tree/main/Resource/Postman>
- 3) <https://github.com/API-Security/APISandbox>

CHAPTER-10

APPENDIX

A. SCREENSHOTS

1. BURPSUITE

Figure 1.1

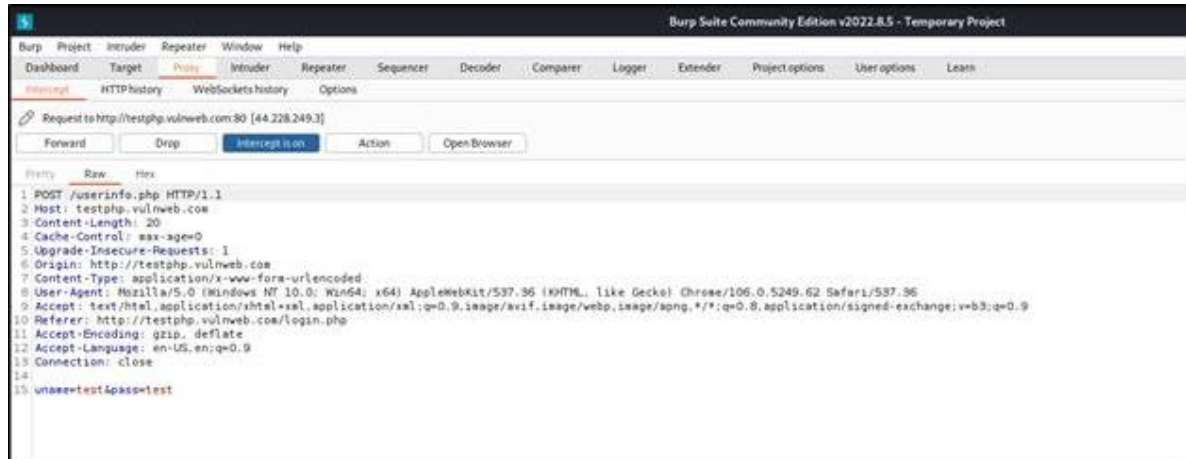


Figure 1.1 represents the Burpsuite intercept performed during the login activity in the API.

2. POSTMAN

Figure 2.1

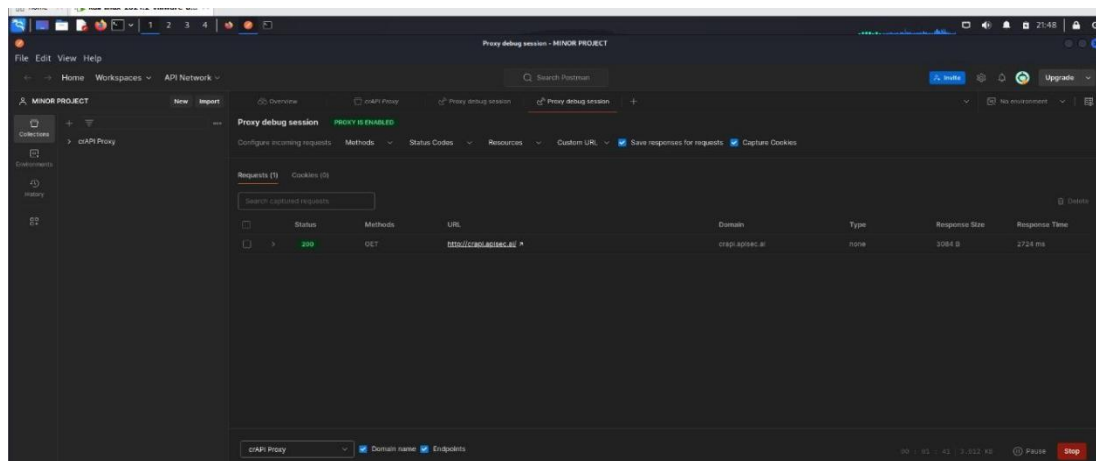


Figure 2.1 represents the Postman request capturing during the various activity in the crAPI.

3. OWASP ZAP(ZAPROXY)

Figure 3.1

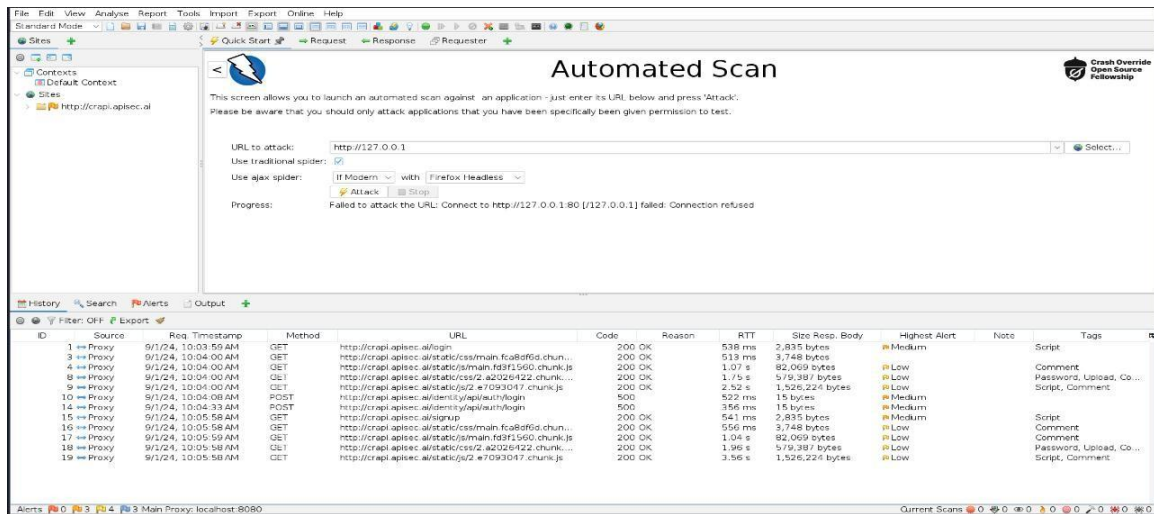


Figure 3.1 represents the Zap proxy Automated Scan the localhost://127.0.0.1:8080 which the thetarget API.

4. SCANNING VULNERABILITIES

4.1 AUTOMATED SCAN

Figure 4.1.1

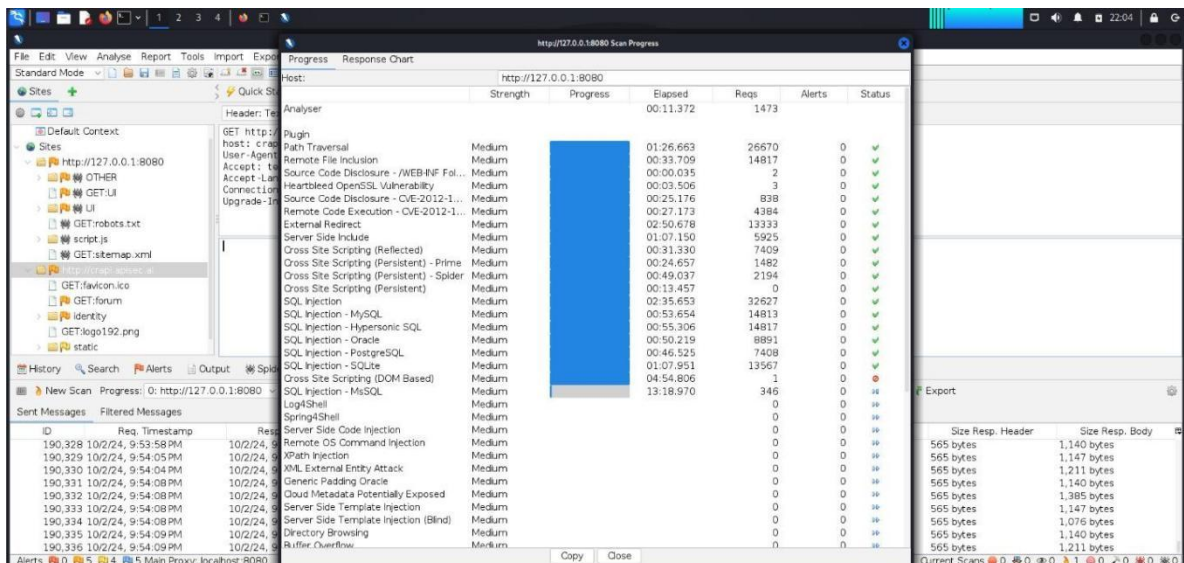


Figure 4.1.1 represents the automated scan for vulnerabilities in the crAPI.

Figure 5.1.1

Figure 5.1.1 represents the authorization attack request sent by various payloads.

Figure 5.1.2

Figure 5.1.2 represents the authorization attack response sent and received by various payloads.

5.2 BROKEN OBJECT LEVEL AUTHORIZATION(BOLA)

Figure 5.2.1



Figure 5.2.1 represents the BOLA attack in which user B credinal token is used to login user A.

Figure 5.2.2

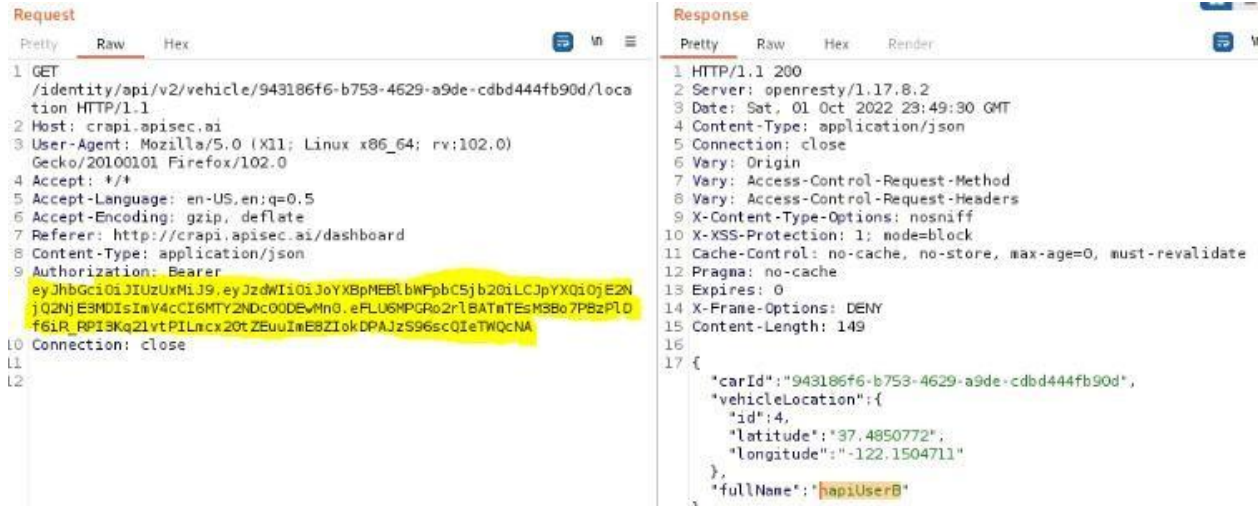


Figure 5.2.2 represents the BOLA attack in which we login user A account using user B's token.

5.3 IMPROPER ASSETS MANAGEMENT

Figure 5.3.1

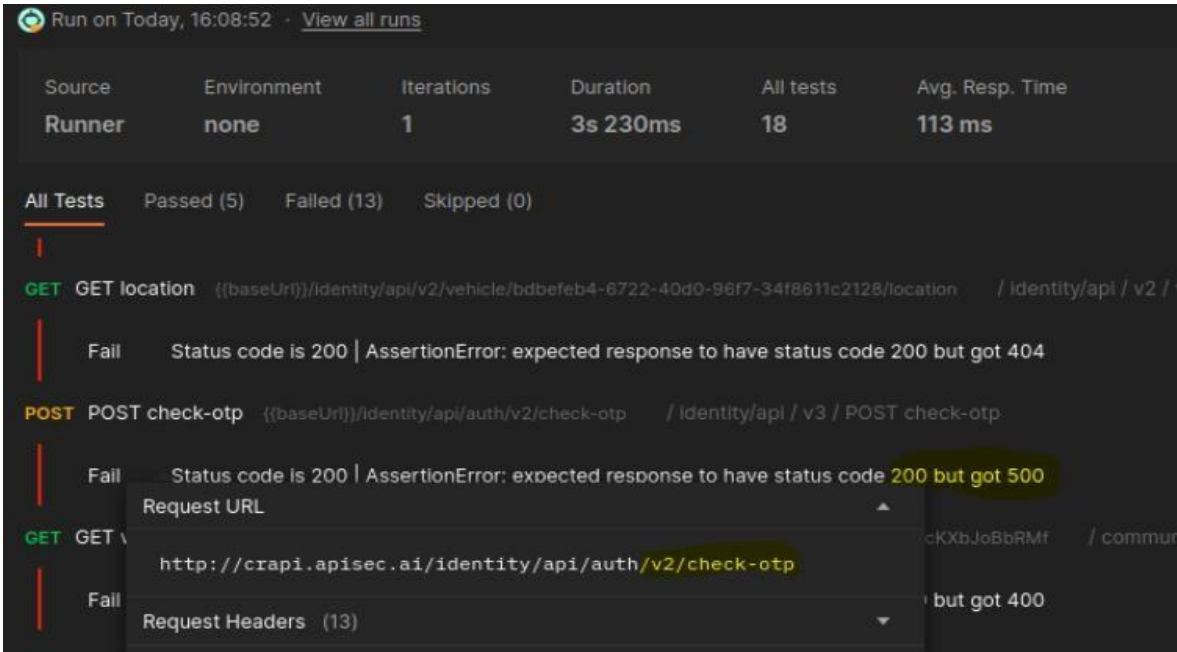


Figure 5.3.1 represents the improper asset management discovery result by analysing the statuscode (eg: 404 not found).

5.3.1 IMPROPER ASSET MANAGEMENT HTTP 500 ERROR

Figure 5.3.2

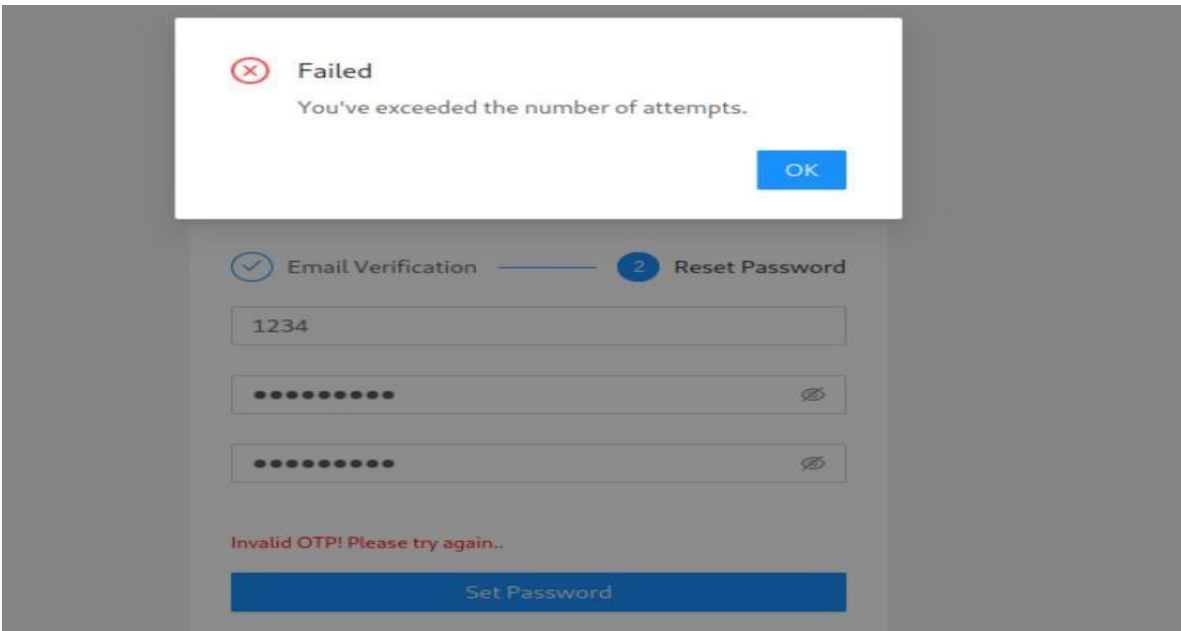


Figure 5.3.2 represents the OTP the application has a control that limits the number of times you can attempt to send the one-time passcode (OTP). Sending too many requests to /v3 will result in a different 500 response.

Figure 5.3.3

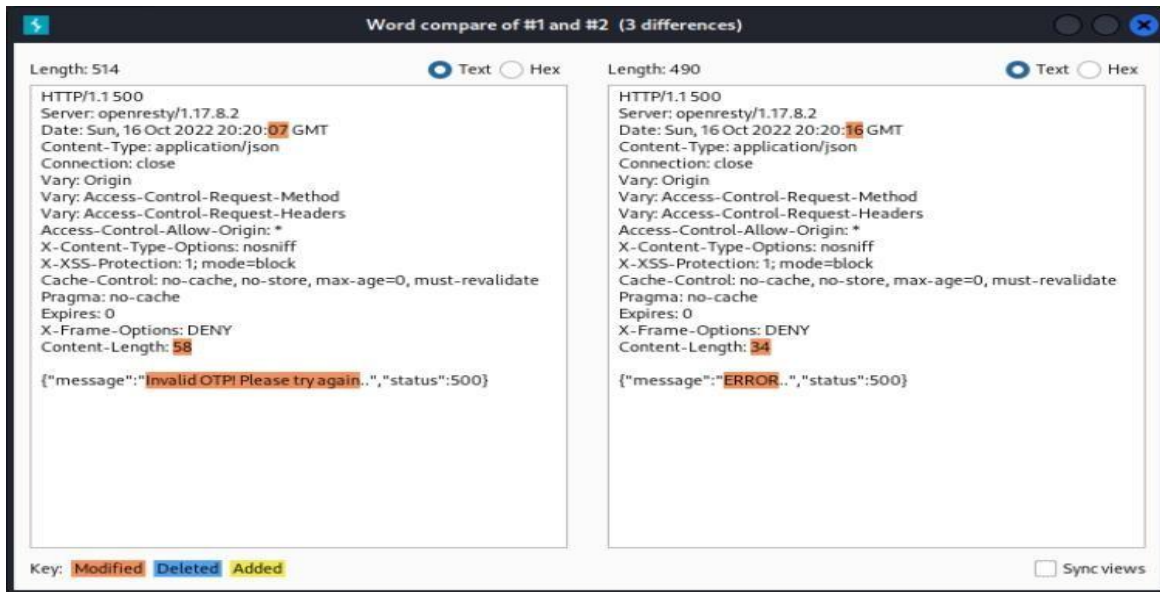


Figure 5.3.3 represents the /v2 password reset request responds with the body (left):
{"message": "Invalid OTP! Please try again..", "status": 500}
The /v3 password reset request responds with the body (right):
{"message": "ERROR..", "status": 500}.

B. SAMPLE CODING

CURL

```
curl -X GET https://api.example.com/endpoint
```

```
curl -X GET "https://api.example.com/endpoint" -H "Authorization: Bearer YOUR_TOKEN"
```

```
curl -X POST "https://api.example.com/endpoint" -H "Content-Type: application/json" -d  
'{"key":"value"}'
```

POSTMAN

```
newman run collection.json
```

BURP SUITE

```
java -jar burpsuite.jar
```

OWASP ZAP

```
zap.sh
```

SYNOPSIS

The project entitled “**Vulnerability Assessment and Penetration Testing on API (Application Programming Interface)**” is the most comprehensive audit and penetration service. Vulnerability analysis is performed to test the security posture of information systems. Penetration testing is an attempt to break into a system using methods and devices that real hackers use. The main purpose of penetration testing is to discover as many existing vulnerabilities as possible and develop viable solutions to fix the problems and improve the overall security of the system.

Penetration testing and vulnerability assessment perform two different tasks within the same scope, but often with different results. Each organization confirms that its security measures are working properly through vulnerability analysis and penetration testing. Methodologies include Discovery, Enumeration and Vulnerability identification, vulnerability assessment, attack exploitation and initiation, reporting, external penetration testing, Internal penetration testing, before starting. Depending on the vulnerability, manual penetration testing or automated penetration testing can be performed. The main aim of the project is to perform the pen test on the API with the given credentials and generate the necessary reports accordingly



DHARSHAN P (22MSS009), III M.Sc Software systems
Batch (2022-2027) in PSG college of Arts & science, Coimbatore.