Lab - 2

Venkata Diwakar Reddy Kashireddy

***Abstract*—This report discusses the HTTP basics, HTTP Proxy, Development/Security Testing tools - ZAP and Browser developer tools, and Security monitoring - Crypto Basics.**

I. Introduction

In this lab, we completed two tasks as well as an additional task for bonus points. We finished HTTP Basics, HTTP Proxies, Developer Tools, CIA Triad, and Crypto basics (steps 1 - 4 and bonus step 8) of WebGoat.

II. Tools

• KVM (Kernel-based Virtual Machine): It is a full virtualization solution for Linux. [1]
• WebGoat: A deliberately insecure web application maintained by OWASP designed for teaching web application security concepts. [2]
• Overleaf: It is a collaborative cloud-based LaTeX editor that helps to create documents easily by providing standard formats. [3]
• GitHub: GitHub is an Internet hosting service for software development and version control using Git. [4]
• Red: – IU Research Desktop (RED) is a virtual desktop service for users with accounts on the Carbonate research supercomputer at IU. [5]
• ZAP: OWASP ZAP (Zed Attack Proxy) is an open-source web application security scanner. It is used by those new to application security and professional penetration testers. [6]
• Firefox DevTools: Firefox Developer Tools is a set of web developer tools built into Firefox. It can be accessed to inspect the webpage. [7]

III. HTTP Basics

This lab covered the basics of HTTP and an insight into how the web actually works. The topics that were covered are HTTP/Web, HTTP methods (GET, POST), HTTP Sessions, Cookies, and HTTP Headers.
GET: The method is used to request data from a specific source (e.g.: Servers). The URL parameters in a GET request are available in web access logs.
POST: This method is used to send data to a server to create/ update a resource.

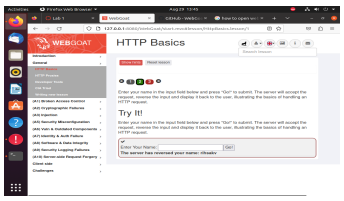

Fig. 1: POST request sent to server.

Fig. 2: POST request information from web access log.

IV. HTTP Proxies

A proxy is an intermediary server that acts as a gateway between a client and a destination server. The application is used for routing, testing an application, and getting access to the internet when there is no direct connection to the internet. ZAP - It is an open-source web application scanner used to record or inspect traffic and modify requests and responses from and to your browser on the vulnerabilities. In this lab, we installed ZAP, used filters to filter traffic, used breakpoint to interrupt a POST request and modified it, and forwarded the modified request.

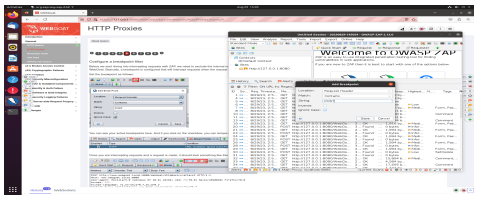

Fig. 3: Break Point filter in ZAP.

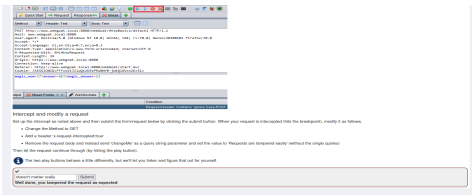

Fig. 4: Successfully tampered with web request using ZAP and forwarded the edited request.

V. DEVELOPER TOOLS

Developer tools in web browsers are a set of built-in utilities that allow web developers to inspect and debug web pages. They provide insights into a website's structure, performance, and behavior, helping developers identify and fix issues during the development process. They also enable security experts to analyze network traffic, uncover vulnerabilities, and assess the security posture of web applications, contributing to enhanced cybersecurity practices.

Fig. 5: Using developer tool-console tab to inspect the code.

Fig. 6: Using developer tool-network tab to inspect a specific HTTP request.

VI. THE CIA TRIAD

It refers to a fundamental framework that helps organizations and security professionals understand and address the core principles of information security. In the lab, we completed a quiz based on the CIA TRIAD.

1. Confidentiality ensures restricted access to sensitive data through measures like encryption and access controls. It ensures that information is only accessible to those who have the proper authorization or permission to view it.

2. Integrity safeguards data accuracy and trustworthiness, preventing corruption during storage, processing, or transmission using techniques like hashing and digital signatures.

3. Availability guarantees data and system accessibility, preventing downtime through strategies such as redundancy and disaster recovery planning. It ensures that information and resources are accessible and usable by authorized users when needed.

VII. CRYPTO BASICS

In the lab, we learned about different cryptography techniques used in web applications to protect information.

1. Encoding: The base64 encoding technique is used by most web applications for basic authentication.

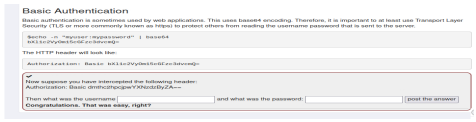

Fig. 7: Successfully decoded a base64 header.

2. XOR Encoding: XOR encoding can be used as a basic form of data obfuscation or encryption, but it is not a strong defense mechanism on its own and should not be relied upon as the sole means of protecting sensitive information. IBM recommends to protect access to these files and to replace the default XOR encoding by your own custom encryption.

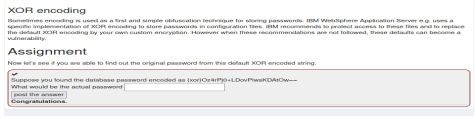

Fig. 8: Successfully decoded an XOR encoded text.

3. Hashing: Hashing is a type of cryptography that is mostly used to detect if the original data has been changed. A hash is generated from the original data.

Fig. 9: Decoded the password for given hash values.

A. Bonus: Step-8 Default Configurations

When you get access to host an application from the hosting server, the configurations are on default settings. So, one of the first things to do is you cannot ssh as a root user and you cannot ssh using a username/password., but only with a valid and strong ssh key, else the application will be open to continuous brute force attempts to login to the server.

Fig. 10: Retrieved the secret from docker image container.

VIII. CONCLUSION

In conclusion, we learned about HTTP basics, proxies, developer tools, CIA triad, and Crypto basics. We used developer tools, ZAP to perform some operations to identify potential openings for vulnerabilities and to interrupt requests. Also, learned about CIA principles and crypto basics and how to decode for different encoding techniques.

REFERENCES

[1] KVM
https://www.linux-kvm.org/page/MainPage..
[2] WebGoat
https://owasp.org/www-project-webgoat/..
[3] OverLeaf
https://www.overleaf.com/.
[4] Github
https://en.wikipedia.org/wiki/GitHub.
[5] RED
https://kb.iu.edu/d/apum.
[6] OWASP ZAP
https://www.zaproxy.org/
[7] Firefox DevTools
https://firefox-source-docs.mozilla.org/devtools-user/