Lab 2: Security Tools and HTTP Basics

Thangamuthu Balaji

I. Introduction

Lab 2 focused on foundational concepts of the HTTP protocol and the use of various security and development tools. Key objectives included understanding HTTP basics, installing and configuring security tools such as ZAP, and testing them through real-world web application security scenarios. This report details the steps undertaken during the lab, the tools used, and the knowledge gained.

II. HTTP Basics

1. In this part, I looked into the fundamental concepts of HTTP, such as its methods (GET, POST), sessions, and headers. By using the "HTTP Basics" section of WebGoat, I examined form data, intercepted HTTP requests, and found vulnerabilities like incorrectly set HTTP methods. I utilized browser developer tools and ZAP to check HTTP request headers and adjust traffic to reveal security flaws..

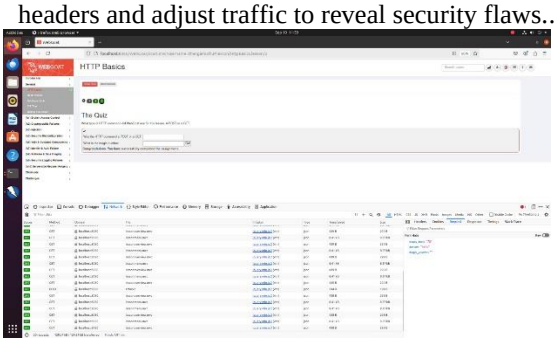

Fig. 1. HTTP Basics

III. HTTP Proxies

1. I used the ZAP tool to catch HTTP requests, showing how proxies can grab and change web traffic. I tried out different HTTP methods and headers, which is really important for figuring out how hackers can take advantage of security weaknesses. This activity showed me how important proxies are for mimicking real-life situations, where attackers tweak requests to get around security protections.

IV. Developer Tools

1. Browser developer tools are super important for seeing how web apps work. I checked out the network tab to look at how data moves around and ran some JavaScript functions to figure out what the web app is doing. This was really helpful for finding hidden values in network requests and understanding how data travels between the client and the server.

2. The CIA Triad—Confidentiality, Integrity, and Availability—is key to information

Fig. 2. HTTP Proxy

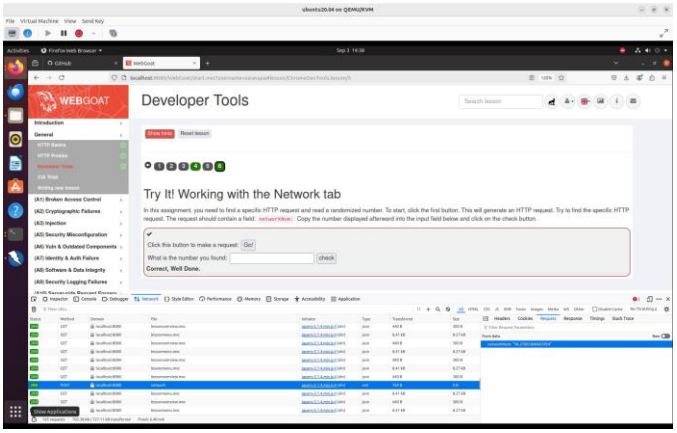

Fig. 3. Developer Tools

V. CIA Triad

security. In this lab, I looked at how these ideas relate to web applications. The activities helped me see how each part helps protect data shared over HTTP connections. However, there was no question at the end.

VI. Crypto Basics

In this section, I worked with basic cryptographic techniques, including encoding methods like base64 and XOR encryption. Using online decoders, I successfully decoded encoded messages, highlighting the importance of proper encryption to ensure secure communication. This task demonstrated how weak cryptographic implementations can be exploited by attackers.

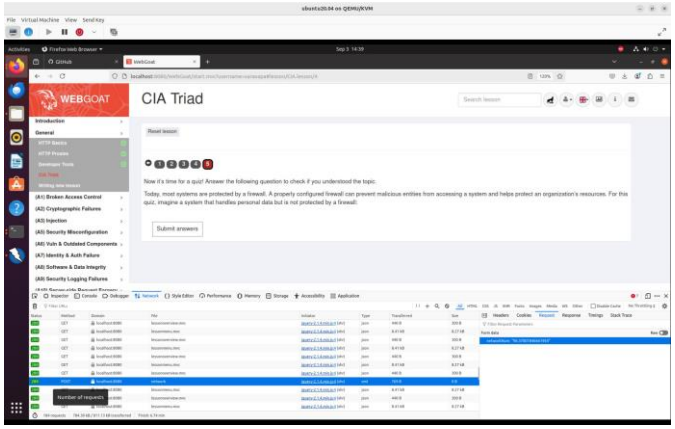

Fig. 4. CIA Triad

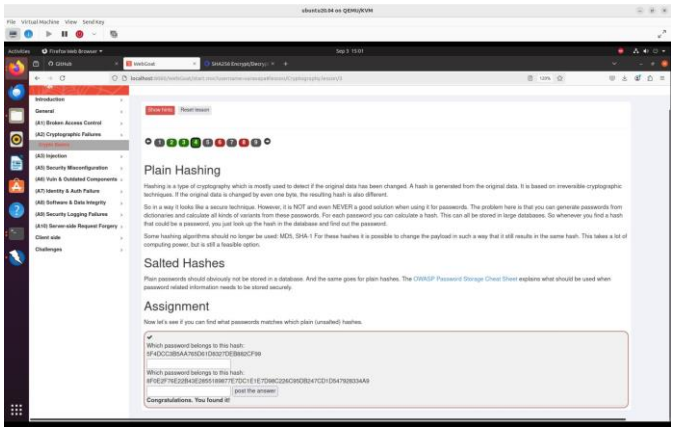

Fig. 5. Crypto Basics

VII. ZAP Installation

ZAP was installed and configured as a man-in-the-middle proxy to intercept and manipulate HTTP requests. I used ZAP to modify request parameters and observe how web applications respond to altered inputs. This exercise provided valuable insights into how attackers could exploit vulnerabilities by intercepting and modifying web traffic, reinforcing the importance of secure web application development.

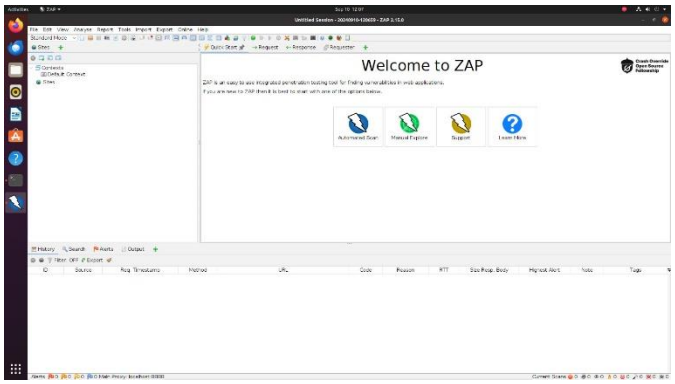

Fig. 6. ZAP Installation

IX. Conclusion

Lab 2 gave us a detailed look at HTTP protocols, the basics of cryptography, and how to use security tools like ZAP. The hands-on activities highlighted how important it is to understand web traffic and the weaknesses that can be found in security. Learning to use tools like ZAP and inotify-tools is really important for both school projects and real-world situations in cybersecurity, especially when it comes to spotting and fixing security problems in web applications.

References

[1] HTTP:https://developer.mozilla.org/enUS/docs/Learn/Getting_started_with_the_web/How_the_Web_works
[2] URL Encoding: https://www.w3schools.com/tags/ref urlencode. ASP
[3] Inotify-tools - https://github.com/rvoicilas/inotify-tools/wiki
[4] ZAP Installation: https://github.com/zaproxy/zaproxy/releases/download/v2.13.0/ZAP_2_1_3_0_unix.sh
[5] FoxyProxy: https: //addons.mozilla.org/en-US/firefox/addon/ foxyproxy-standard