# Lab-2 Report

Akhilesh Gowda Mandya Ramesh

***Abstract*—The Lab-2 introduced tools such as ZAP to observe the Vulnerabilities in WebGoat.**

## I. Introduction

THE insecure application that provides functionalities to observe the vulnerabilities of applications, such as WebGoat can be used to observe and clearly understand the core functionalities such as HTTP/Web, The methods that HTTP offers such as get and post, HTTP session and cookies and HTTP headers can be made use of using a tool called ZAP which provides functionalities for users to intercept the traffic and can even manipulate it for their use.

## II. HTTP

An application-layer protocol called Hypertext Transfer Protocol (HTTP) is used to send hypermedia documents. Although it was created for web browser and web server communication, there are other uses for it as well. In the traditional client-server architecture used by HTTP, a client first establishes a connection, sends a request, and then waits for a response. Because HTTP is a stateless protocol, the server does not save any information (state) between requests. This HTTP interaction between the client and the server requests have header and a body. GET method of HTTP can be used to request the services of a server from client. POST method is used by the server to send back an appropriate response back to the client. The Lab challenge was to send an HTTP request through ZAP and modifying the request which will be revealed in the response window of ZAP.

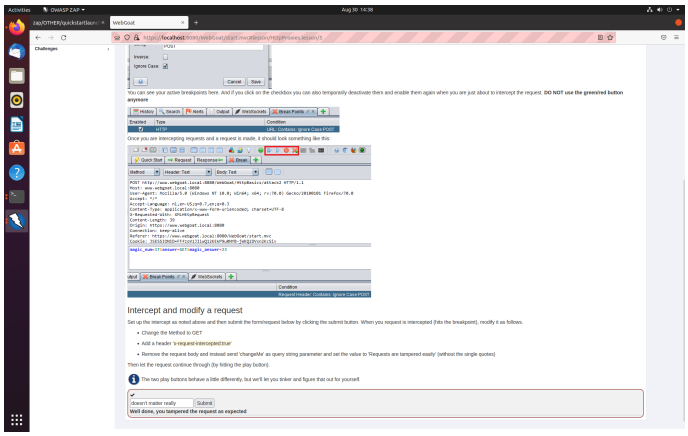


Fig. 1. entering the intercepted message via ZAP to complete the task

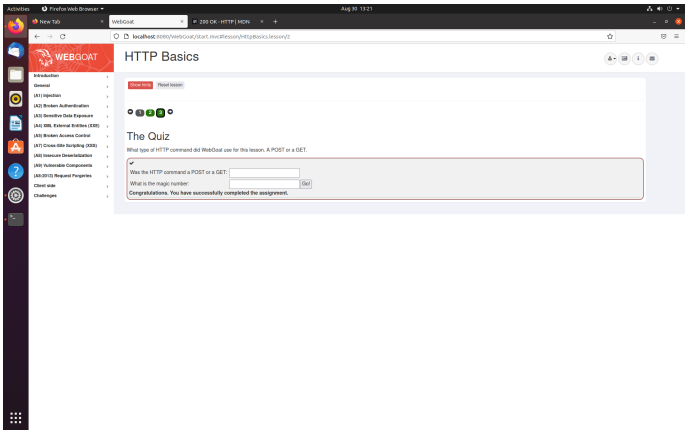


Fig. 2. HTTP Basics Quiz completion

## III. Developer Tools

Web browsers comes along with developer tools, Which can be used to inspect the Web page. There are several options in the developer tools such as inspect which is used to view the HTML, CSS and layout/structure of the page, Console which is used for logging and running the JavaScript Code, Source helps in viewing and editing the files, Network which is used to inspect or track network activity, Performance is used to analyze and evaluate the run time performance and many more features that can be exploited by the users. The lab task was to check the console to retrieve the number from the function webgoat.customjs.phoneHome(). The following tasks was to use the network functionality from the developer tool which contains the network traffic to get the number generated upon clicking the the go button to make a request. The number retrieved then has to be entered in the box and needs to be checked if it is the right number.

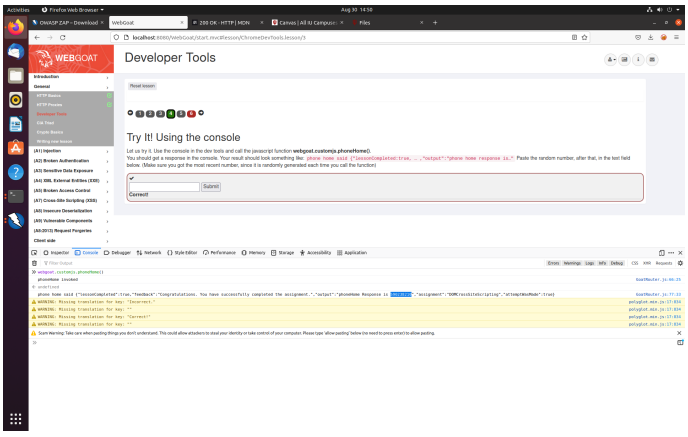


Fig. 3. Running the function in the console and entering the number

Advisor: Luyi Xing, Jiale Guan .

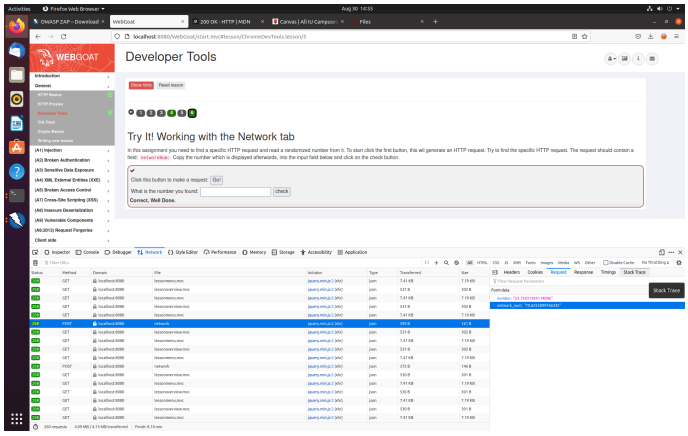


Fig. 4. Using Network to get the Number after making a request

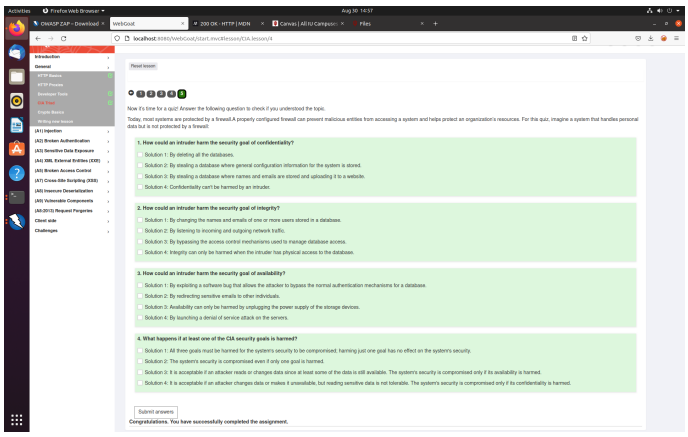


Fig. 5. CIA Quiz completion

## IV. CIA Triad

Confidentiality, Integrity and Availability are the triad that forms the fundamentals of security. Its a challenge to make sure none of these triads fail as they cannot be compromised. Confidentiality means that users who are unauthorized must not be able to access the resources. Integrity refers to maintaining the correct and valid information where the information cannot be changed during propagation. Availability refers to having the resources available for users to access the data.

## V. Crypto

Data being transferred needs to be encrypted making it hard for attackers to retrieve the data if it were to be compromised. There are several encoding/decoding algorithms which can be made use of to mask the data. In the Lab Base64 technique was used to transform the data within a specific range which is primarily used for email encryption. The other technique that was introduced was the XOR encoding which uses XOR logical operator to encode the data.

## VI. Conclusion

In Summary WebGoats vulnerabilities can be exploited to study and bolster the attacks. ZAP can be used to intercept

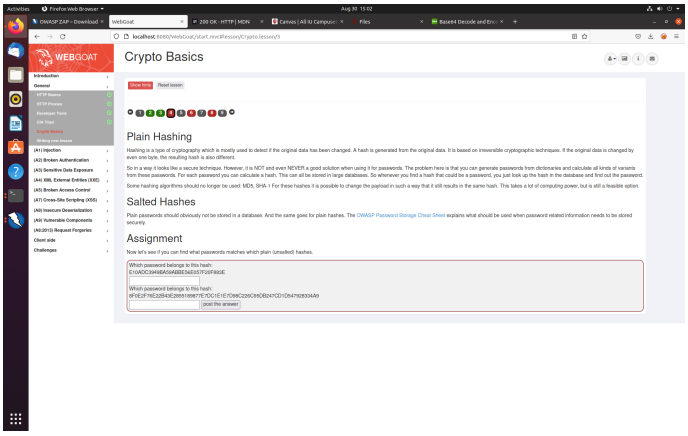


Fig. 6. All Tasks completed screenshot

HTTP requests, and the traffic can be changed using proxies. The CIA triad cannot be compromised in any applications as they are the basic pillars. The developer tools can be used to take advantage of the wide range of functionalities that it has got to offer. To make sure of Confidentiality, Integrity and Availability the data can be encrypted using techniques such as XOR, Base64

## References

[1] https://github.com/WebGoat/WebGoat
[2] https://owasp.org/
[3] https://www.zaproxy.org