Lab-8 Report

Akhilesh Gowda Mandya Ramesh

***Abstract*—The Lab-8 introduced us to the webgoat excercise related to Broken Authentication which includes Authentication Bypasses, JWT tokens and password reset.**

I. Introduction

THE insecure application that provides functionalities to observe the vulnerabilities of applications, such as WebGoat can be used to learn and get exposure to different types of vulnerabilities in the area of injection and authentication and broken Authentication such as Authentication Bypass, JWT tokens and password reset. For the first tassk i intercepted the request and changed the secQuestions to secQuestions00 and secQuestion1 to secQuestion01 and the task was completed

II. Authentication Bypasses

Authentication Bypasses can occur in many ways but they usually take advantage of some flaws that is present in he configuration or the logic. They involve tampering to achieve the right conditions. They make use of hidden inputs which relies on simple inputs that is in the Web page or DOM. If the attacker does not know the correct value of the parameter, they will be able to remove the parameter altogether to experiment and check what is about to happen. Suppose the area of the site is unprotected by the configuration then the attacker can take advantage of the vulnerabilities by accessing that area of the website using Brute Force methods.

III. JWT tokens

This section introduced JSON Web Tokens (JWT) which can be used for authentication. It introduced how to securely implement the usage and validation of the tokens. The structure of a JWT token consists of three parts header, claims and signature. both the header and claims are represented by JSON Object. The header describes the cryptographic operations applied to he JWT and optionally, additional properties of JWT. The claims represent a JSON object whose members are the claims conveyed by the JWT. For the task-3 i used the decoder to decode the token and found that the username is user.

IV. Password Reset

This section introduced materials related to the password reset functionality, which is the most overlooked part of the application leading to many interesting logic flaws. The goal here is to securely implement reset functionality within the application. Every website has its own way of implementing he password reset functionality, some differences include using a link to reset the password whereas some others use security questions to reset the password. We looked into some of the most common implementations. the task -1 of password reset was to reset the password. I Used webwolf o reset the password. For forgot password i yped my email amandyar@webgoat.org and the password was received in the web wolf mailbox, which was then used o complete the assignment. During password reset we will receive messages such as whether the email exists or not, This information can be used by the attacker as part of phishing. The attacker will send a link to the user as he will know it is a valid account, this way he can get the password back while the user enters it in the link. The next task was to guess the username and favorite color o login. I tried different usernames and at the end Tom was the correct username. I did the same for the color as well tried different color in he end purple was the answer. The next task was to guess he right security question and in the end i found out that the right answer is What is your favorite animal?.

Advisor: Luyi Xing, Jiale Guan.

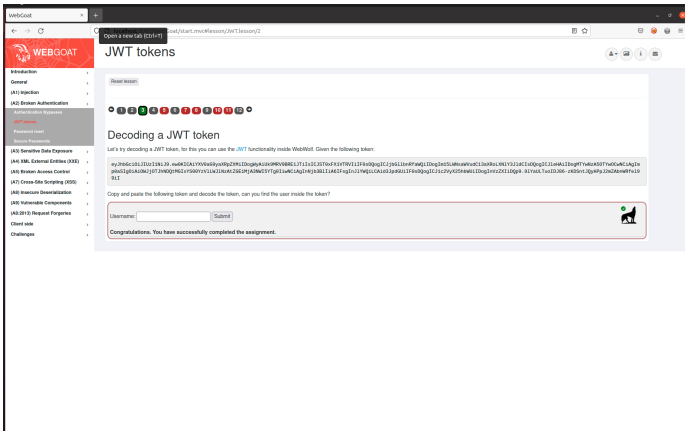

Fig. 1. JWT token task -3

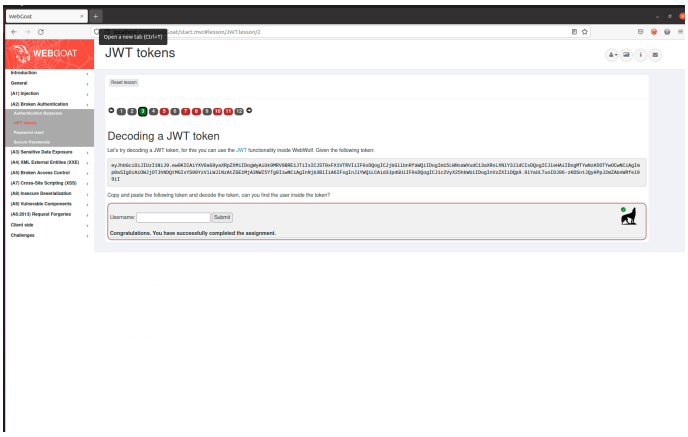

Fig. 2. JWT token task - 6 and 7 completion

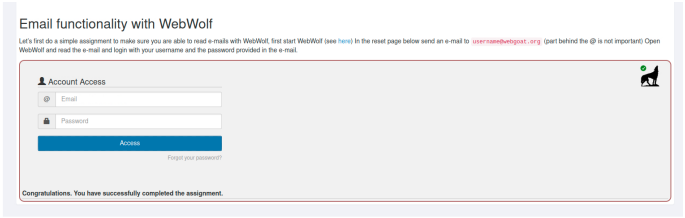

Fig. 3. password reset task -1

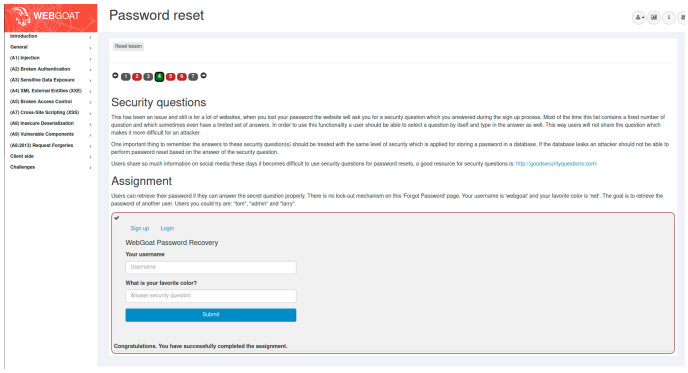

Fig. 4. password reset task -4

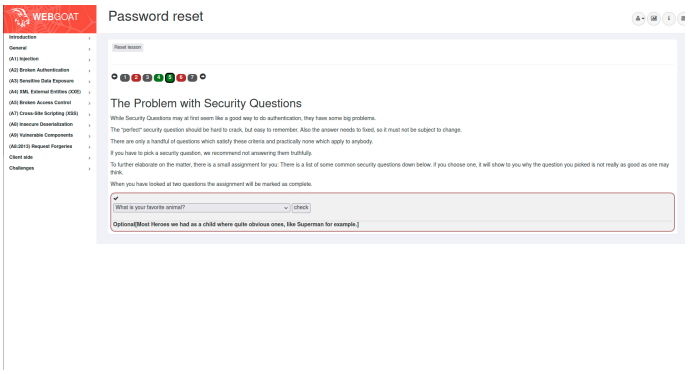

Fig. 5. password reset task -5

V. Conclusion

In Summary as WebGoats vulnerabilities can be exploited to study and bolster the attacks, We can also use it to study and mitigate the attacks such caused by SQL injection as the CIA Triads can be compromised by performing SQL Injection. This lab we studied Broken Authentication includes Authentication Bypasses, JWT tokens and password reset. This was we can decide to try and develop a website that are less vulnerable to all of these. This way we can try to develop websites that do not compromise a CIA triads.Authentication Bypasses can occur in many ways but they usually take advantage of some flaws that is present in he configuration or the logic. They involve tampering to achieve the right conditions. They make use of hidden inputs which relies on simple inputs that is in the Web page or DOM. Authentication is one of the most fundamental thing to be implemented in the website. We need to make sure that there is no flaw or vulnerability that the attacker can use to attack the website. We need to make sure that the websites are not vulnerable to phishing.

References

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