LAB-08

1. Imagine you're a cybersecurity analyst tasked with assessing the security of a newly developed e-commerce website. You would utilize Burp suite and perform following activities to identify and mitigate security flaws in the web application. Start by describing the setup process for Burp Suite, including configuring proxy settings and initiating automated scans to detect common vulnerabilities like SQL Injection.

    i. Manual Testing of SQL Injection

    ii. Proxy Attack with Burp Suite.

i) Manual testing for SQL injection: -

Setting mutillidae app correctly for SQL injection Vulnerability Testing

Go to the target machine(Metaspoiltable 2)—in the terminal type below commands

cd /var/www/mutillidae

sudo nano config.inc

Ensure dbname=owasp10 instead of metasploit

Then save(ctrl+X, Y and enter) and exit.

In the kali linux browser

192.168.62.129

Go to mutillidae and enter the username as ‘ and password field is empty , click on enter It displays errors, which indicates web application is vulnerable

It displays the query in the Diagnotic information.

• Now again click login/Register enter username as **admin**

Password as **blahblah ‘ OR 6=6#**

Then you can observe it is logged in as admin.

• Now trying with username as admin ‘ # and password field must be empty, still you can observe it is logging in as admin.

• In mutillidae page, click on OwaspTOP10->A1 injection -> SQLi Extract Data -> User Info and Enter username=**admin** and password =**adminpass** , click on view account details Then Results for admin. 1 records found would be displayed

Username=admin

Password=adminpass

Signature= Monkey

• **Now for SQLi**

Enter username=**admin** and password= ‘ **OR 1=’1—**

Click on view account details. Then you would observe **Results for admin. 16 records found details…**

ii) Proxy Attack with Burp suite.

• Start both the Kali Linux virtual machine and the Metasploitable 2 virtual machine to ensure they are up and running.

• Navigate to the "Applications" menu in Kali Linux and launch the Burp Suite application. • After Burp Suite has launched, set up the proxy configuration.

• Download the Burp Suite certificate and import it into the relevant certificate store. • Access the proxy settings within Burp Suite and configure a manual proxy setup with the HTTP proxy set to 127.0.0.1 and port number 8080. Confirm the settings by clicking "OK." • Open the Mutillidae application and log in using the credentials: username - "john" and password - "passwd." Before clicking on the login button, activate the intercept feature in Burp Suite. Proceed to click on the login button in Mutillidae.

• Check the Burp Suite application to verify that it captured the login request, including the username and password information.

• Modify the username and password to "admin" and "adminpass" respectively within Burp Suite. Then, click "Forward" to send the modified request.

• Once the modified request is forwarded, observe in the Mutillidae application that the login is successful, indicating that the credentials have been changed to admin/adminpass. • Within the Burp Suite application, navigate to the "Target" tab to review the intercepted information from the target machine.