Burp Suite Web Application Testing Setup and Report

1. Objective

The objective of this project is to set up Burp Suite on Kali Linux, configure it to intercept traffic from the Firefox browser, and demonstrate its capabilities in web application security testing. This includes configuring the proxy, capturing HTTP(S) traffic, and performing basic scanning.

2. Tools Used

- Burp Suite (Community Edition)
- Firefox (Browser)
- Kali Linux (Pentesting Environment)

3. Installation of Burp Suite

Burp Suite is a powerful tool for web application security testing. It can intercept HTTP(S) traffic, perform vulnerability scans, and more.

Steps:

1. Install Burp Suite:

Burp Suite is pre-installed on Kali Linux, but if not, it can be installed via:

```
sudo apt update
sudo apt install burpsuite
```

2. Launch Burp Suite:

In the terminal, run:

```
burpsuite &
```

3. Start a Temporary Project:

Choose Temporary Project and click Start Burp.

4. Configuring Burp Suite to Intercept Traffic

Setting the Proxy in Firefox:

To use Burp Suite to intercept web traffic, configure Firefox to send all HTTP/HTTPS traffic through Burp Suite's proxy server.

1. Open Firefox:

Type about:preferences in the URL bar.

2. Configure Network Settings:

Scroll down to Network Settings -> Click "Settings..."

Select Manual proxy configuration.

Set the following:

- HTTP Proxy: 127.0.0.1
- Port: 8080
- Check "Use this proxy for all protocols".

Click OK to save the changes.

5. Installing Burp Suite's SSL Certificate

To intercept HTTPS traffic, Burp Suite needs to decrypt SSL/TLS connections. This requires installing Burp's CA (Certificate Authority) certificate.

1. Access Burp's Certificate:

Open Firefox and navigate to http://burp.

Download the CA certificate.

2. Install the Certificate in Firefox:

Go to Preferences -> Certificates -> View Certificates.

Import the downloaded certificate and trust this CA to identify websites.

6. Intercepting Web Traffic

Enable Intercept Mode:

1. Burp Suite: Go to Proxy -> Intercept.

2. Turn ON intercept (button should be green).

3. Open a browser tab and visit a website, such as http://testphp.vulnweb.com.

4. Burp will catch the HTTP request made by the browser. You can:

   - Modify the request

   - Forward the request

   - Drop the request

7. Capturing and Testing HTTP Traffic

Testing with Vulnerable Website:

- Visit a vulnerable website (e.g., http://testphp.vulnweb.com) in Firefox.

- Burp Suite will show the captured HTTP request in the Intercept tab.

- You can analyze, modify, and send the request to other Burp tools such as Repeater or Intruder for further testing.

8. Conclusion

Burp Suite has been successfully set up on Kali Linux and configured to intercept and analyze web traffic from Firefox. The following was achieved:

- Set up Burp as an HTTP(S) proxy.
- Installed Burp's SSL certificate to handle HTTPS traffic.
- Tested the intercept feature by analyzing web requests to a vulnerable site.

This project demonstrates the capabilities of Burp Suite in performing web application security assessments.

9. Future Improvements:

- Automated Scanning: Explore Burp Suite's Pro version for automated vulnerability scanning.
- Using Intruder: Test for common vulnerabilities like SQL injection and XSS using Burp's Intruder tool.
- Advanced Configurations: Learn to configure Burp Suite for mobile app traffic interception or use with external proxies.

10. References

- Burp Suite Documentation: https://portswigger.net/burp/documentation
- OWASP ZAP vs. Burp Suite: https://www.acunetix.com/blog/owasp-zap-vs-burp-suite/