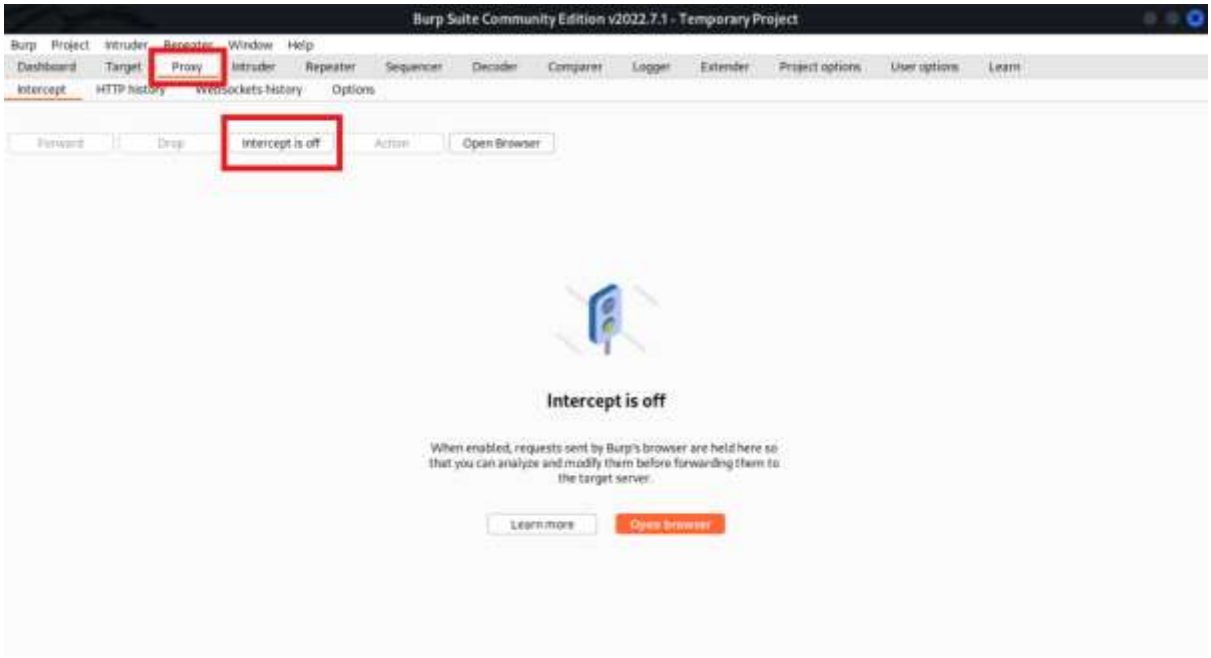
Burp Suite: HTTP Intercepting

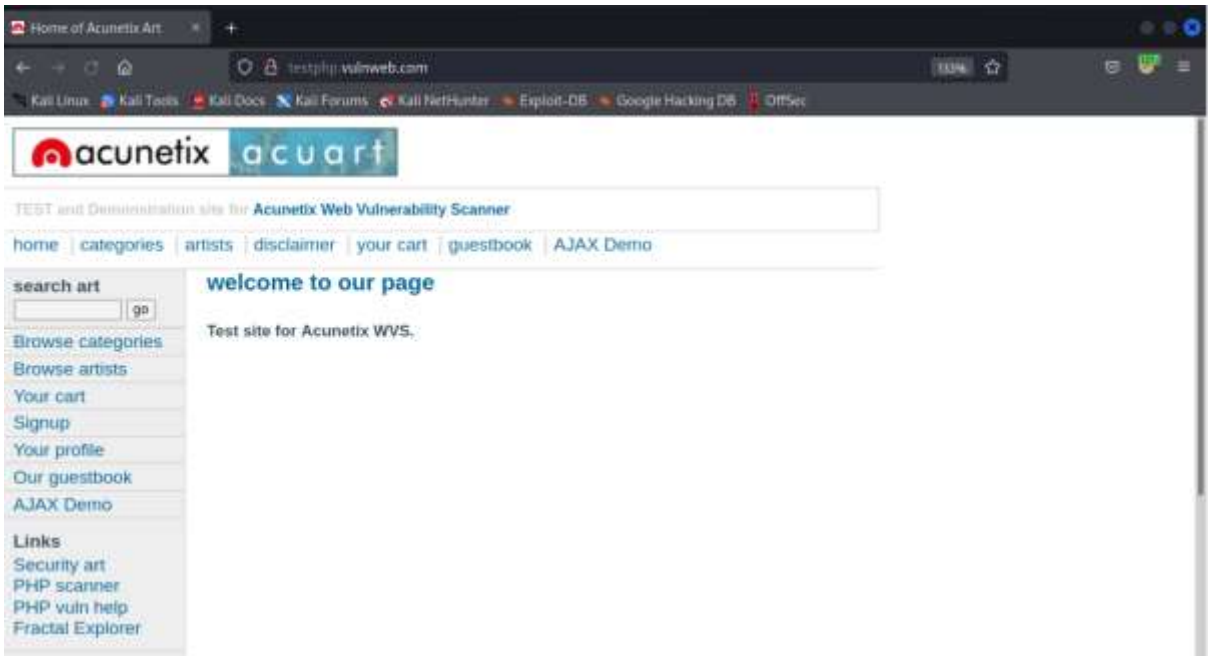
HTTP intercepting in Burp Suite offers significant advantages for web application security testing. It enables detailed traffic analysis by allowing testers to thoroughly inspect both requests and responses, uncovering hidden parameters and headers that might be missed otherwise. This real-time inspection is crucial for understanding the full content exchanged between the client and server, including HTML, JavaScript, JSON, and more. Additionally, intercepting traffic allows testers to manually modify requests and responses on-the-fly, facilitating the testing of input validation, parameter tampering, and the bypassing of client-side controls. This capability is essential for identifying security vulnerabilities such as injection attacks, by inserting malicious payloads into requests, and session management issues, by manipulating session tokens and cookies. Furthermore, it aids in evaluating authentication mechanisms by intercepting and altering authentication requests, thereby revealing potential weaknesses like session fixation and improper session handling. Overall, HTTP intercepting in Burp Suite is a powerful feature that provides deep insight and control, essential for effective security testing.

Examples: -

1. Firstly. Open your burp suite and go to the Proxy tab in order to turn on Intercept option.

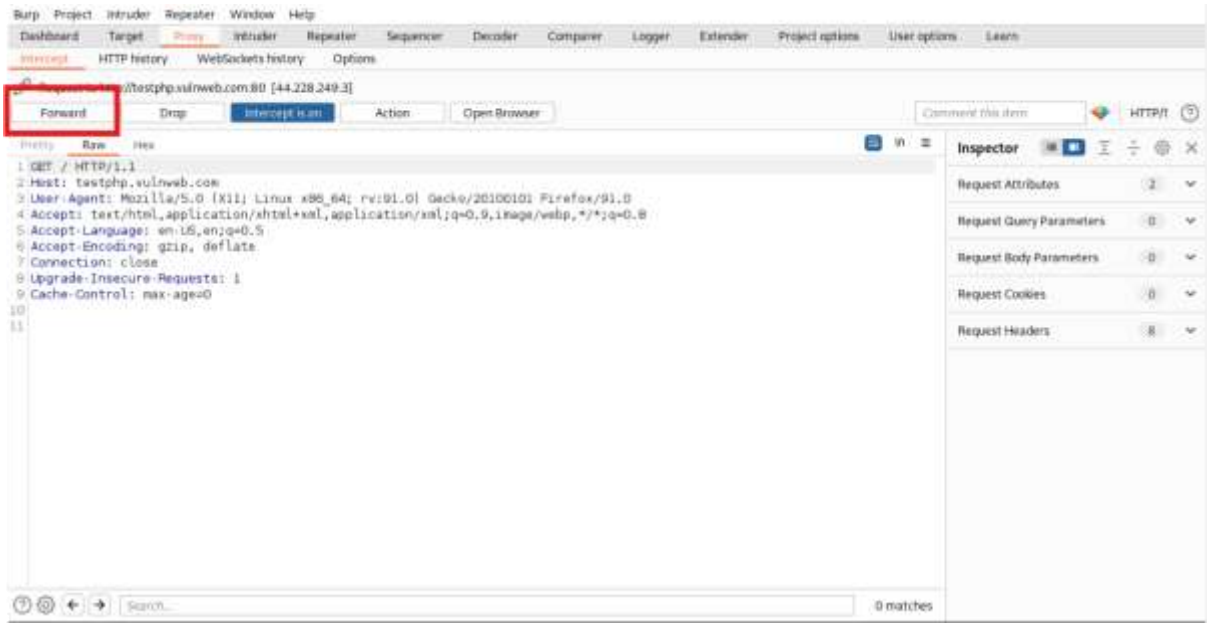


2. Now after turning it on go to the browser to make a get request. Make sure to turn on the browser's proxy before making a web qurry.



3. When you hit the enter button inside the browser the burp will start capturing the request. You can see the result in the proxy tab.

4. Now in order to make multiple requests hit on the forward button.



5. Now to look for the all http request history click on the HTTP History tab.

6. Now to have a detailed insight of each request you can hit on the particular request. This contains information like Request and Response header.