Burp Suite

What is Burp Suite

Burp Suite is a proxy program that enables us to track, examine, and alter requests made by our browsers before they are forwarded to a distant server. Burp Suite is a prominent web application security solution. It gives us the ability to manually test for vulnerabilities, intercepts HTTP messages, and change a message's body and header.
It is the most widely used tool among experts in online app security and bug bounty hunters. It is a better option than free substitutes like OWASP ZAP because of how simple it is to use.

Why is Burp Suite Used in Cybersecurity

Burp Suite is a comprehensive framework that may be used to carry out several activities, including:

- Web crawling.
- Web application testing, both manually and automatically.
- Analysis of web applications.
- Vulnerability detection

Features in Burp Suite

1. Proxy

The intercepting proxy in BurpSuite enables the user to view and change the contents of requests and answers while they are being sent. Additionally, it eliminates the need for copy-and-paste by allowing the user to pass the request or answer that is being monitored to another pertinent BurpSuite tool. The proxy server can be configured to run on a specific loop-back IP address and port. Additionally, the proxy may be set up to block particular kinds of request-response pairings.

2. Intruder

It is a fuzzer that runs a collection of values across an input point. The results are examined for success/failure and content length after the values have been executed. The response code or response's content length changes as a result of an anomaly most frequently. For its payload slot, BurpSuite supports dictionary files, brute-force attacks, and single values.

3. Repeater

Burp Suite Repeater allows us to craft and/or relay intercepted requests to a target at will. In layman’s terms, it means we can take a request captured in the Proxy, edit it, and send the same request repeatedly as many times as we wish.

4. Sequencer

The sequencer, an entropy checker, verifies the unpredictability of tokens produced by the webserver. These tokens, like cookies and anti-CSRF tokens, are typically used for authentication in sensitive processes. The ideal way to produce these tokens is completely random, which will distribute the likelihood of each potential character appearing at each location
equally. Bitwise and characterwise approaches should be used to accomplish this. This hypothesis' validity is examined with an entropy analyzer.

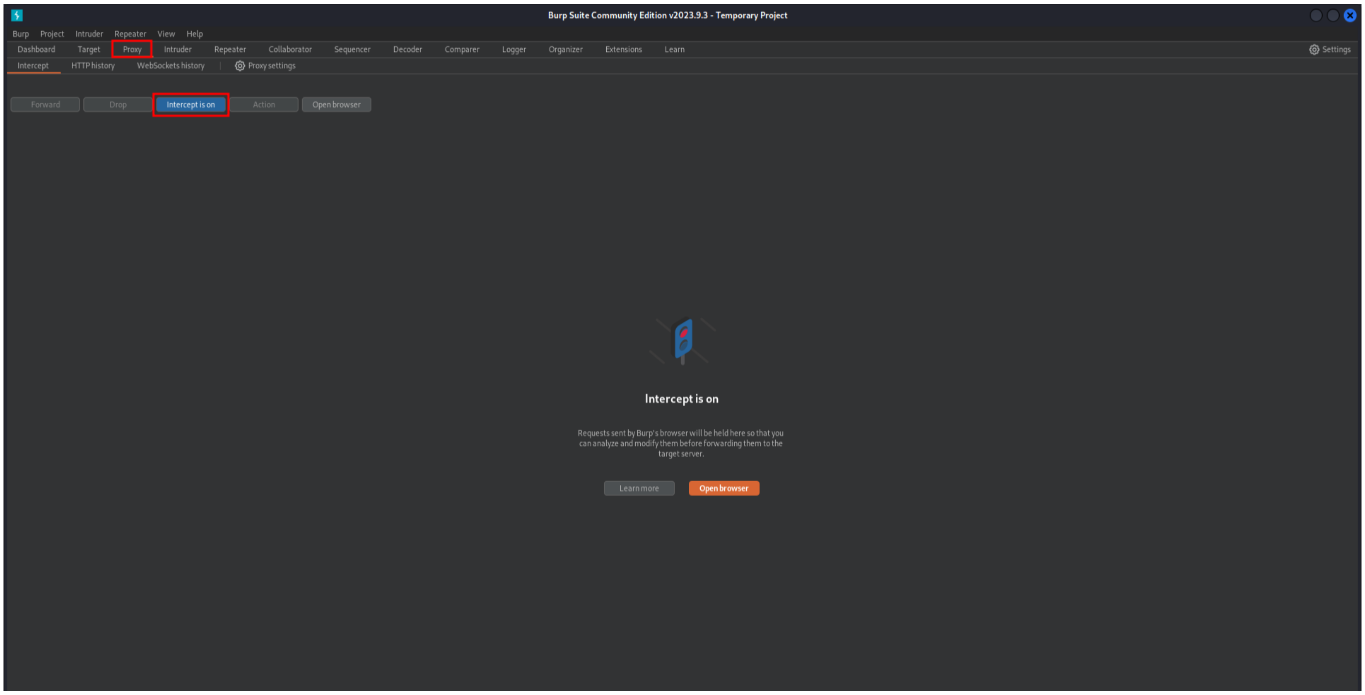
5. Decoder

The decoder provides a list of common encoding techniques such as URL, HTML, Base64, Hex, and so on. When searching for specific data chunks inside the values of parameters or headers, this tool is quite helpful. Additionally, it is employed in the development of payloads for several vulnerability classes. Primary instances of IDOR and session hijacking are also uncovered using it.

Burp Suite on Testfire.net

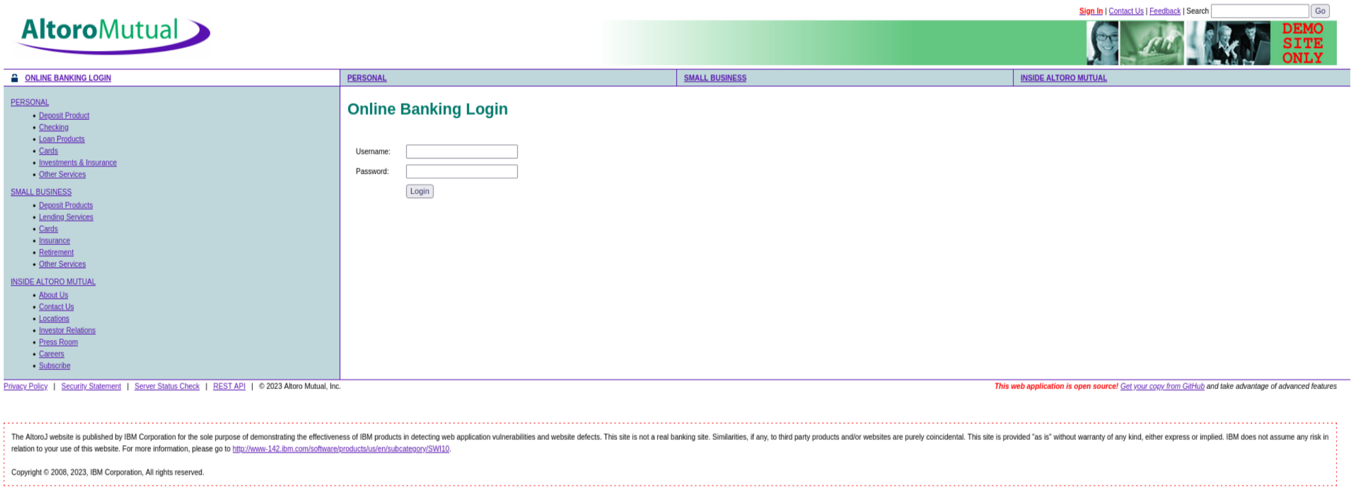
I will be testing the login page on http://testfire.net/.

First we need to set up the proxy on the web browser and turn on the intercept mode.



Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

Now we can head over to the login page and enter our credentials. Press the login button.



Online Banking Login

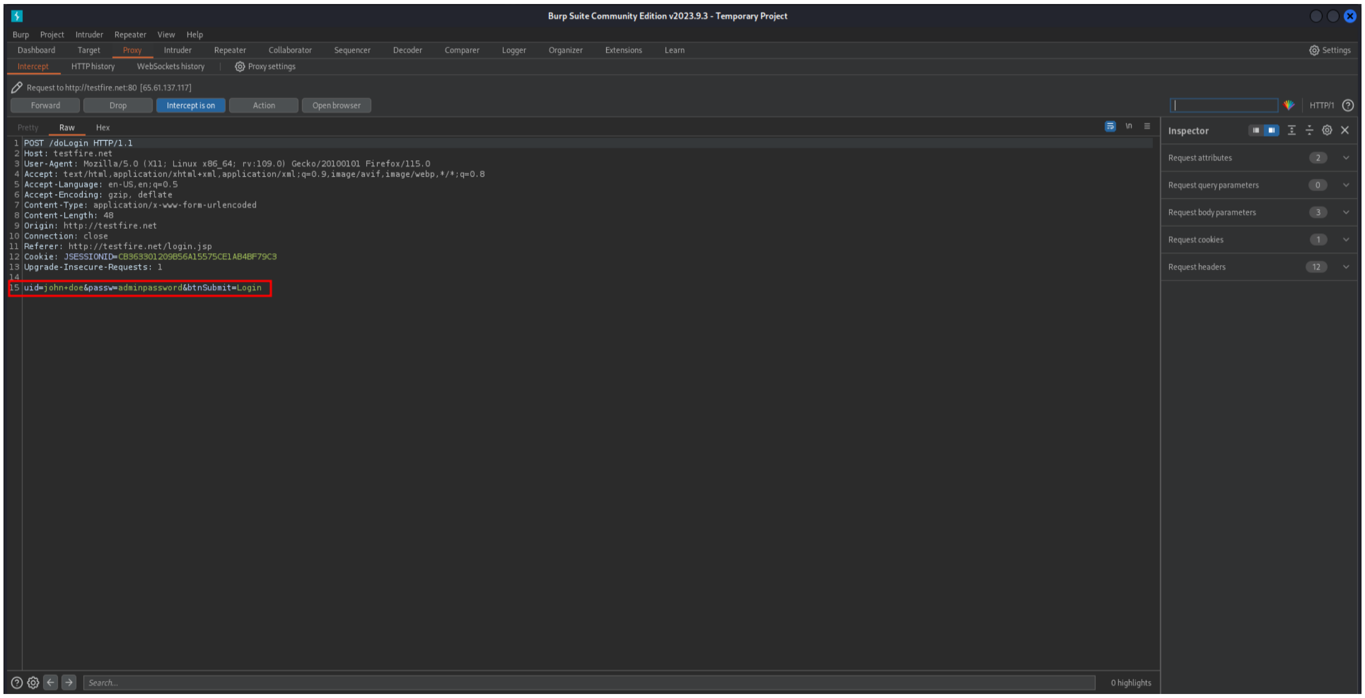
Username:

Password:

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

Burp will intercept the POST request and it allows us to see the data being transmitted. Since the site is not using encryption, we can easily see the username and password in cleartext.


Burp Suite Community Edition v2023.9.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 1
Request headers 12
Search...
0 highlights

Request to http://testfire.net:80 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 48
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=CB363301209B56A15575CE1AB4BF79C3
Upgrade-Insecure-Requests: 1

uid=john+doe&passw=adminpassword&btnSubmit=Login
```