Name :- M Om Nivas Reg No :- 21BCE9706

E-mail :- omnivas.21bce9706@vitapstudent.ac.in

Using of Burp Suite

Weekly

Assignment – 4

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 was created by a business with the alias Portswigger, whose creator Dafydd Stuttard also works there. BurpSuite is designed to be an all-in-one toolkit, and BApps are add-ons that may be installed to expand its functionality.

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. The community edition of Burp Suite is accessible for free, whereas the professional edition and the enterprise edition need payment.

Why burp suite?

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

Burpsuite also has the advantage of being built into the Chrome browser.

What are the features of burp suite?

1. Spider

A web crawler or spider is employed to map the target web application. The mapping's goal is to compile a list of endpoints so that their capabilities may be examined and possible vulnerabilities can be discovered. Spidering is carried out for the straightforward reason that more attack surfaces are available during real testing if you collect more endpoints during recon.

2. 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.

3. 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. The invader is employed for:

- Brute-force assaults against password forms, pin forms, and other forms of this nature.
- Dictionary attacks on password fields on forms are thought to make them susceptible to XSS or SQL injection.
- Rate limitation on the web app is being tested and attacked.

4. Repeater

A user can submit requests repeatedly with manual adjustments using a repeater. It's employed for:

- Examining if the user-provided values are being examined.
- How successfully is the verification of user-supplied values being carried out?
- What values are expected by the server for an input parameter or request header?
- What happens when the server receives unexpected values?
- Is the server using input sanitization?
- How thoroughly the user-supplied inputs are sanitized by the server?
- What kind of cleanliness practices does the server employ?
- Which cookie is the real session cookie out of the ones that are already there?
- If there is a means to get around CSRF protection and how is it put into practice?

5. 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.

This is how it works: first, it is thought that the tokens are random. The tokens are then put to the test using specific criteria for certain traits. The definition of a "**significance level**" is a minimal value of probability that a token will demonstrate for a characteristic, such that the token's randomness hypothesis will be rejected if the token's characteristic probability is below the significance level. This utility may be used to discover weak tokens and show how they are made.

6. 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.

7. Extender

BurpSuite enables the integration of extra components into the toolkit to expand its functionality. These external components are referred to as BApps. These perform the same tasks as browser extensions... The Extender window allows you to **examine, modify, install, and remove them**. Some of them are supported by the free community version, while others need the professional version, which is a paid upgrade.

8. Scanner

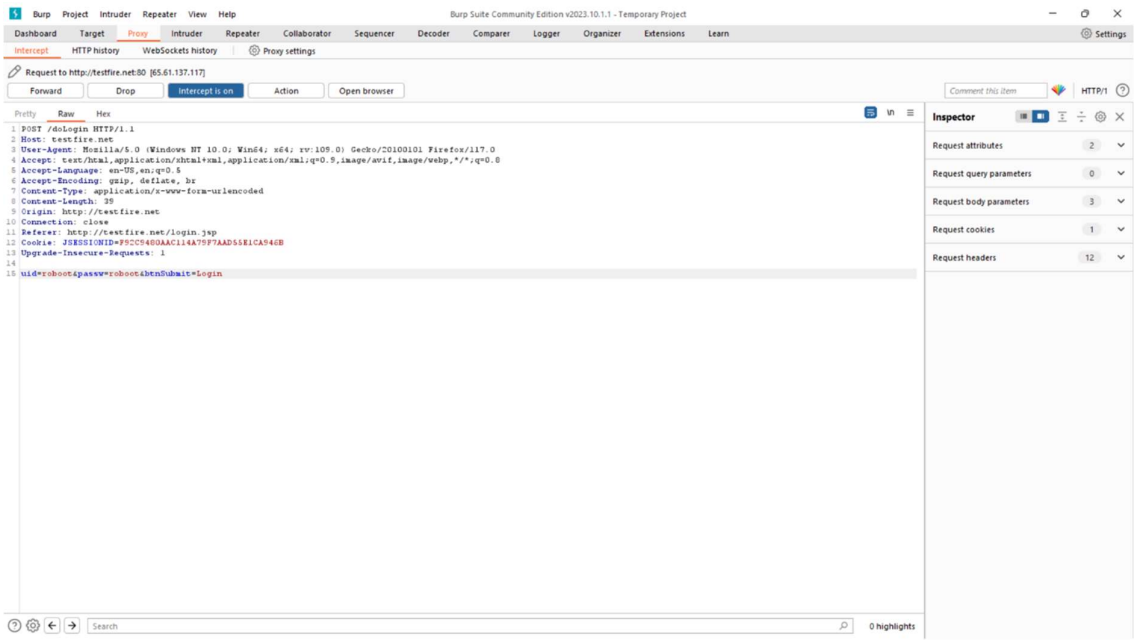
The community edition does not have a scanner. It automatically analyses the website for a variety of common vulnerabilities and provides them together with details on the reliability of each discovery and the difficulty of exploiting them. It is routinely updated to add brand-new, and lesser-known vulnerabilities.

Test the vulnerabilities of testfire.net

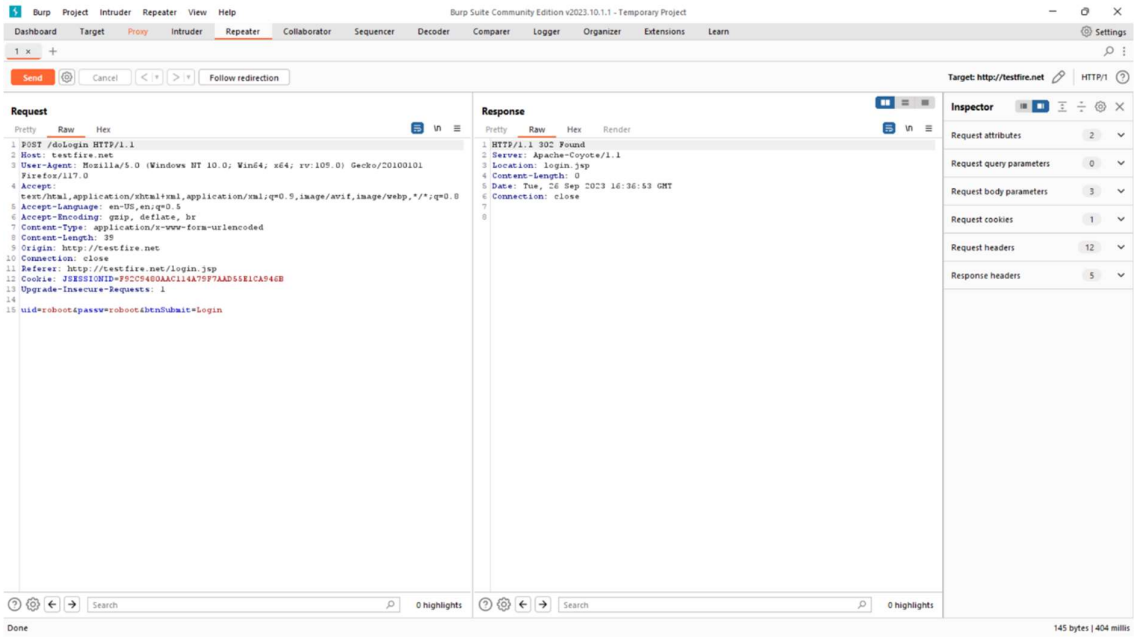
www.http://testfire.net

Proxy and Intercept :-

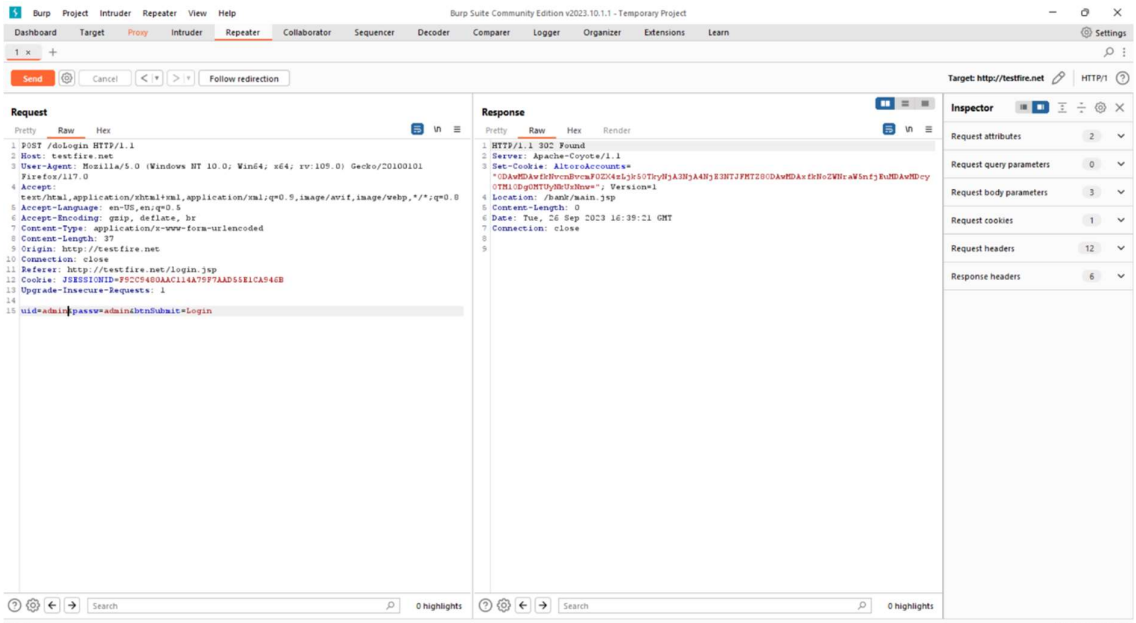
Monitoring the http requests and sending it to Repeater and Intruder.

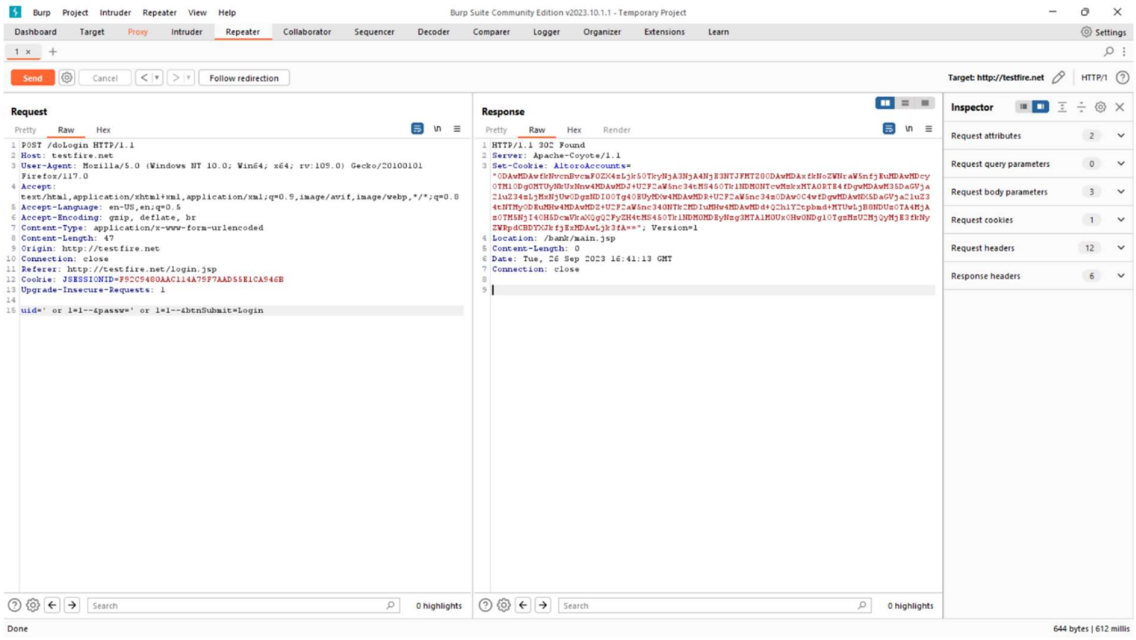


Repeater :- viewing the Response in this we can view single response

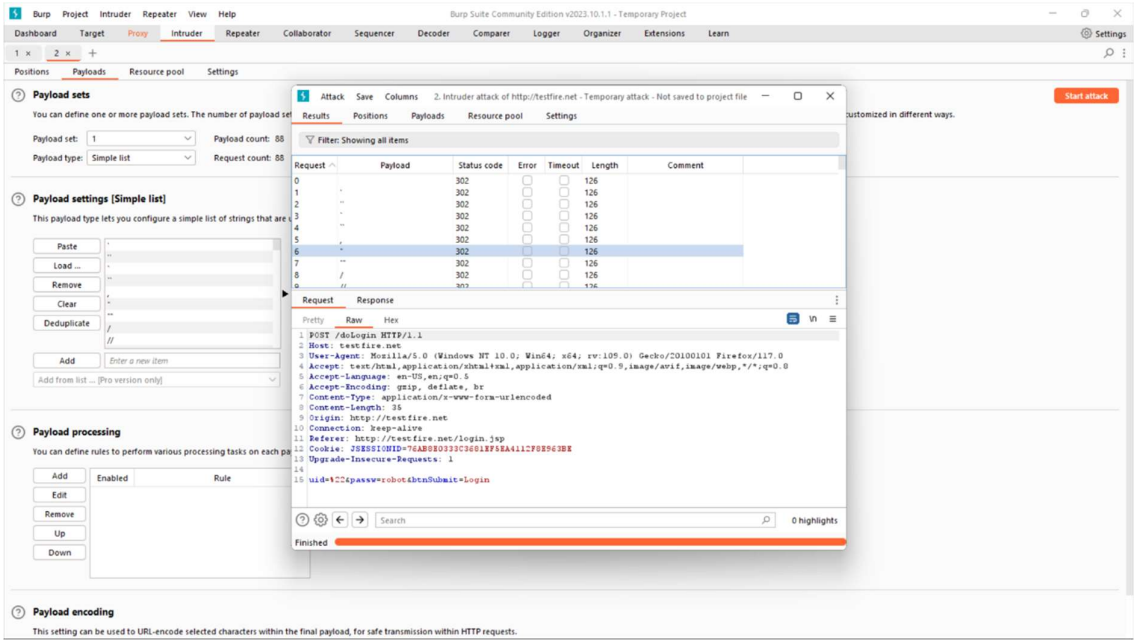


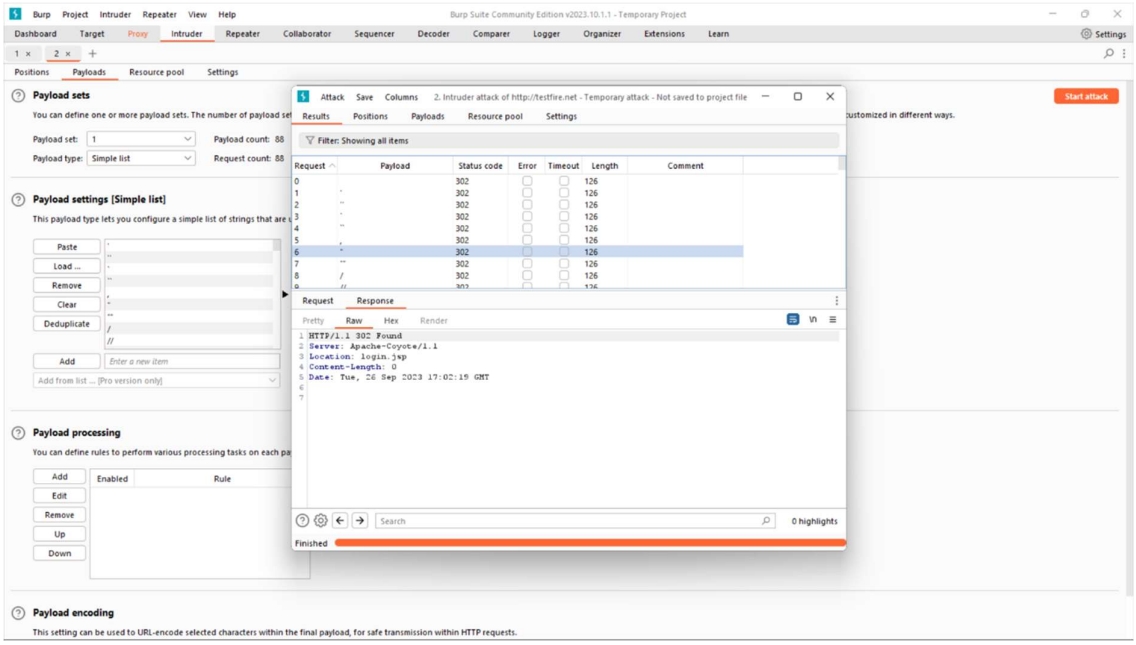
Modifying the UID and PASWD



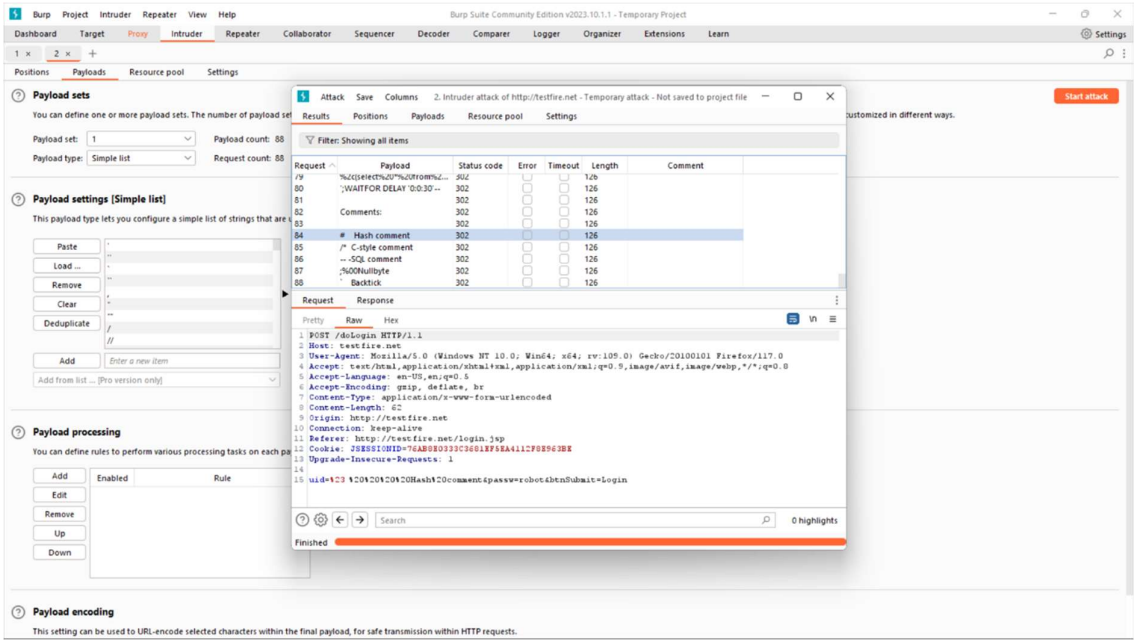


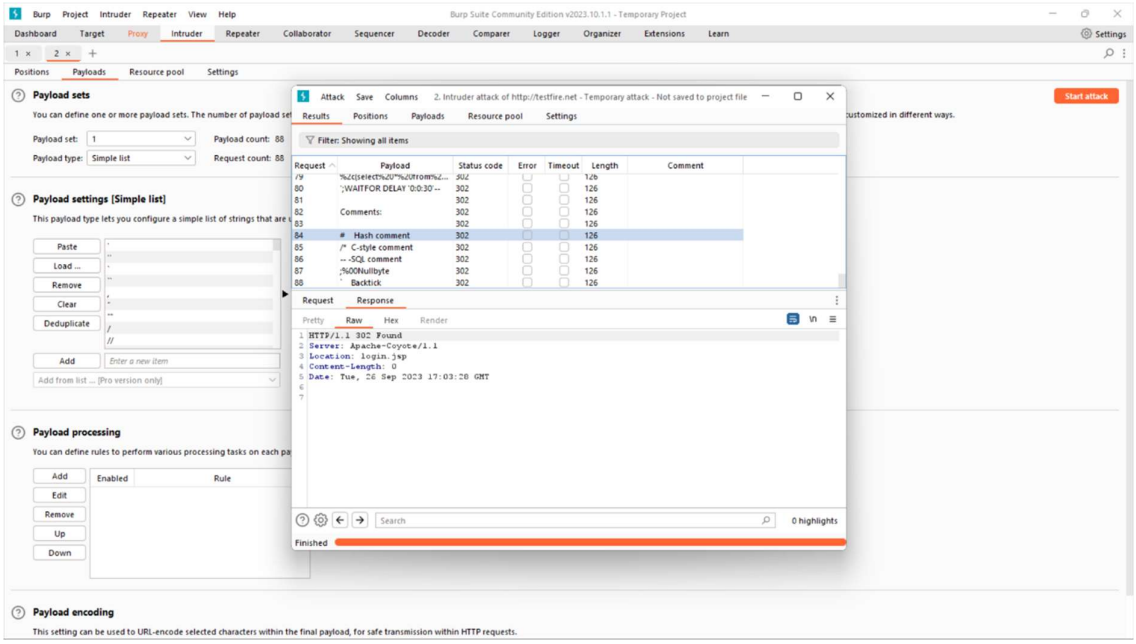
Intruder :- In this we Can Upload a Payload and Search for multiple UID and PASWD at the same time by just pasting





Checking different payload uid and paswd





END