Made by Moeez Javed

Burp Suite – Professional Guide

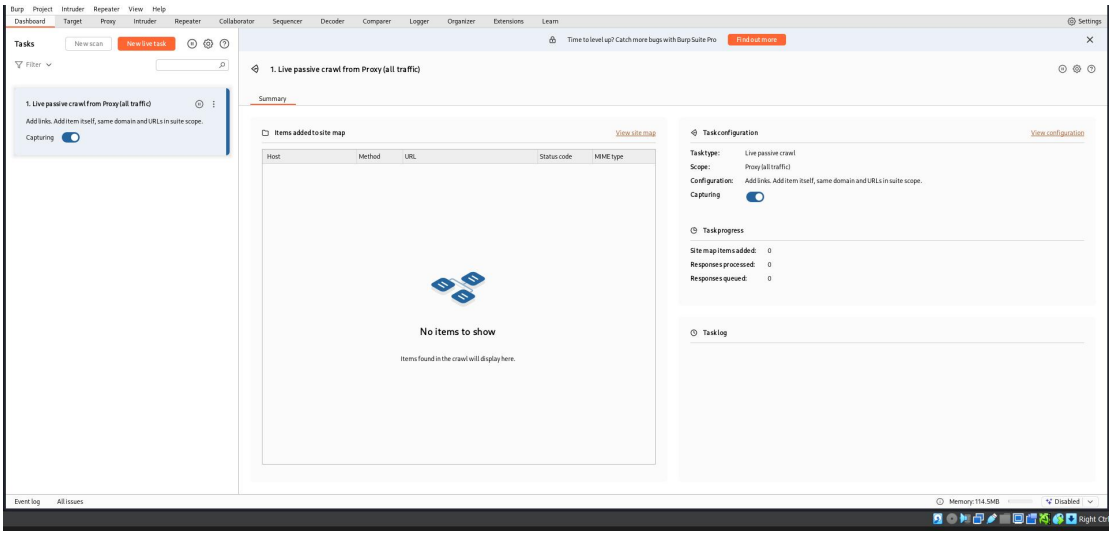
Prepared for Cybersecurity Students

Burp suite:

Burp Suite is a powerful web application security testing tool developed by PortSwigger. It is widely used by penetration testers, bug bounty hunters, and security researchers to identify and exploit vulnerabilities in web applications.

Step 1:

Open burpsuite



What is Interception in Burp Suite?

Definition:
Interception allows Burp Suite to pause (intercept) HTTP(S) requests and responses before they reach their destination (server or browser), giving you a chance to view, modify, or drop them.

Why It's Important

- You can analyze requests and responses in real-time.
- Allows you to manipulate data (e.g., parameters, cookies, headers, form values) before the server processes it.
- Critical for testing injections, parameter tampering, and authentication bypasses.

How It Works

1. You turn intercept ON (in the Proxy tab).
2. When you perform an action in the browser (like submitting a form), Burp catches the request.
3. You can edit anything in the request.
4. You then click Forward to send it to the server.

What Does the Forward Button Do?

Definition:
The Forward button in Burp Suite is used to send the intercepted request or response to its next destination.

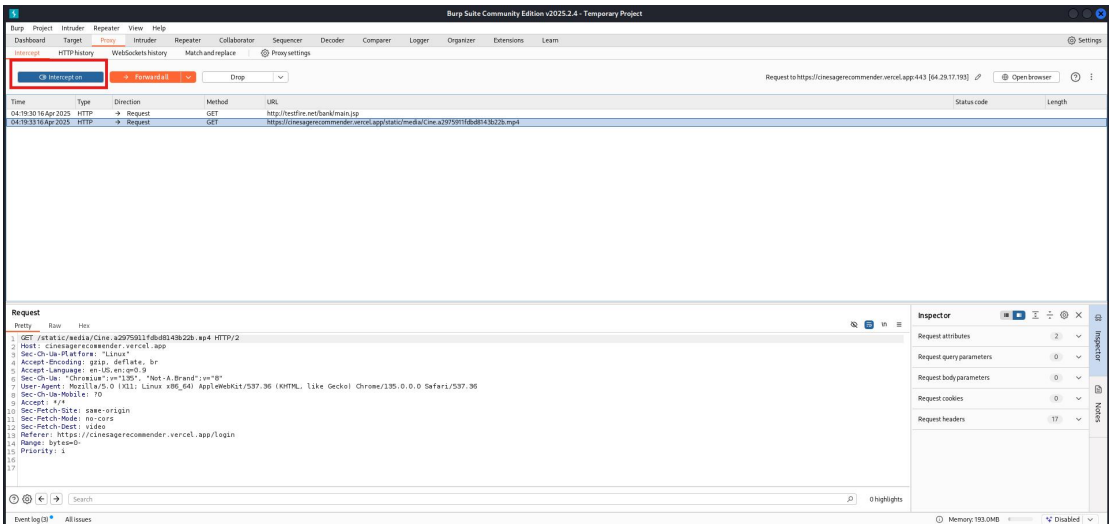
Use Cases

- After modifying a login request, click Forward to test if login works with a different password.
- Intercept a form submission, change parameters, and use Forward to send the modified data.
- Intercept a server response and analyze or change it before it reaches the browser.

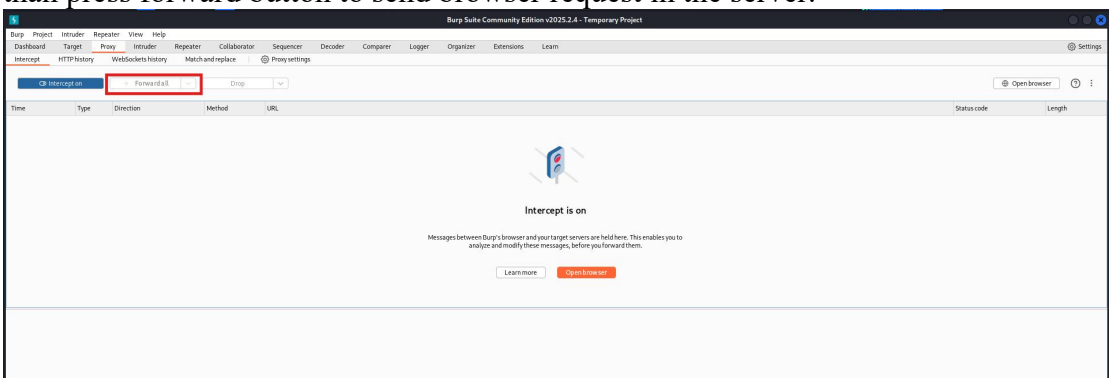
Made by Moeez Javed

In Simple Words

Feature	Purpose
Interception	Stops the request/response so you can view or edit it.
Forward	Sends the request or response to the next step (server or browser).



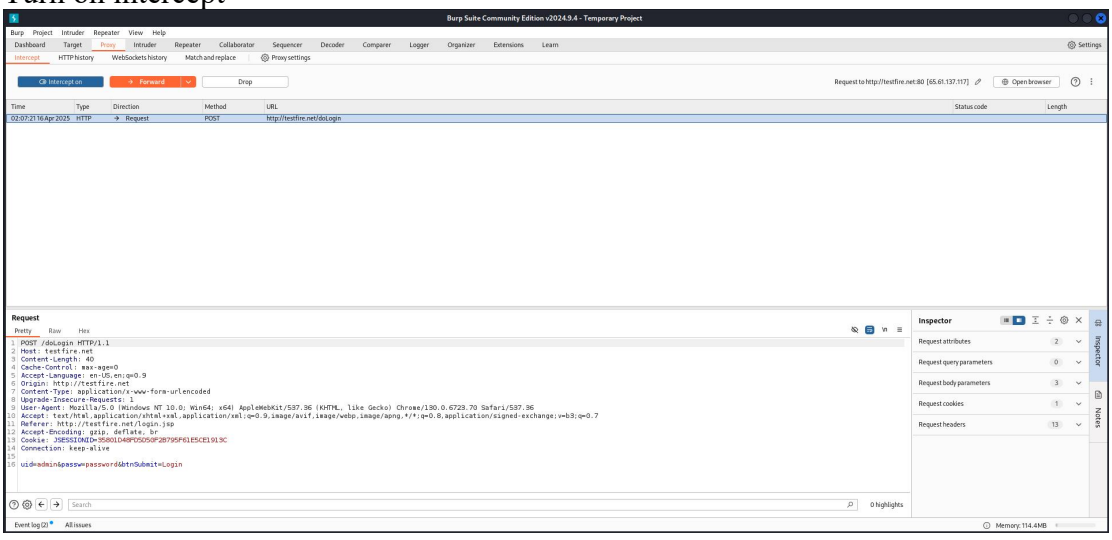
than press forward button to send browser request in the server.



Forward Button is Pressed and it send to the server.

Step 2:

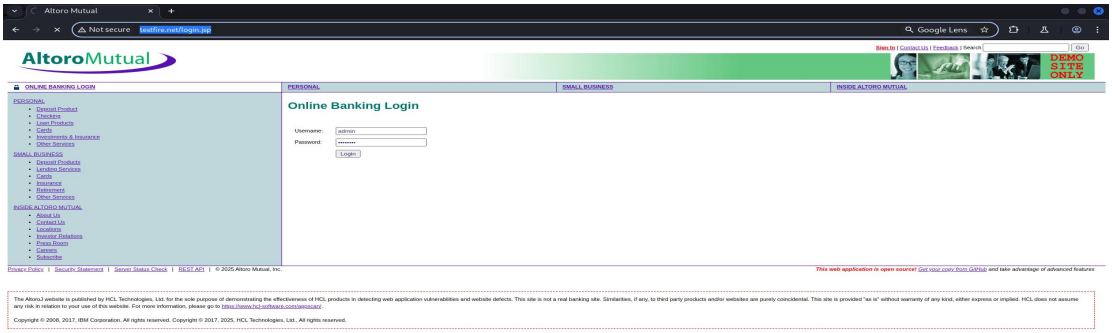
Turn on intercept



Made by Moeez Javed

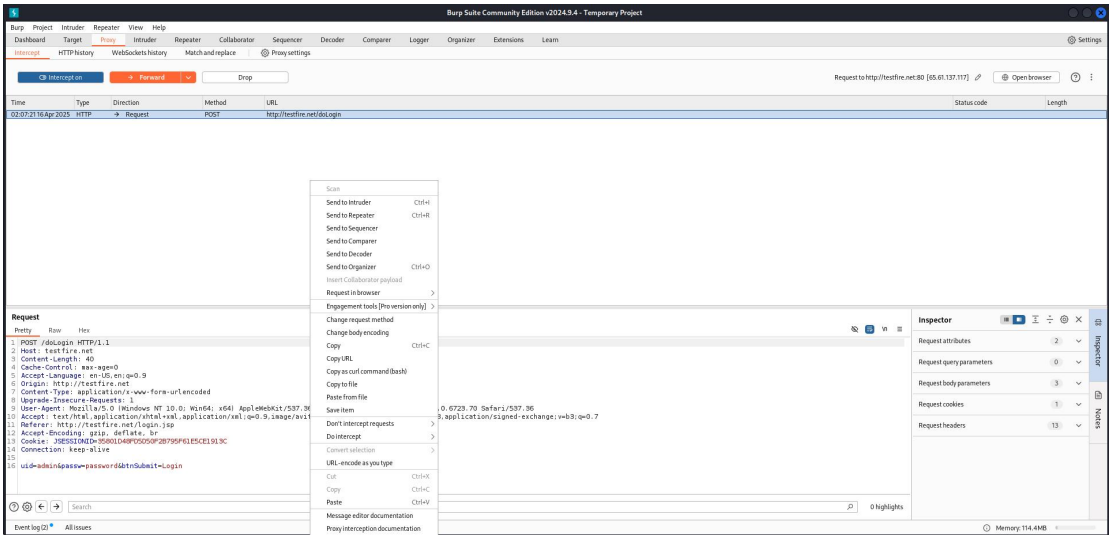
Step 3:

http://testfire.net/ go to the this website,
write username and password by your wish



step 4:

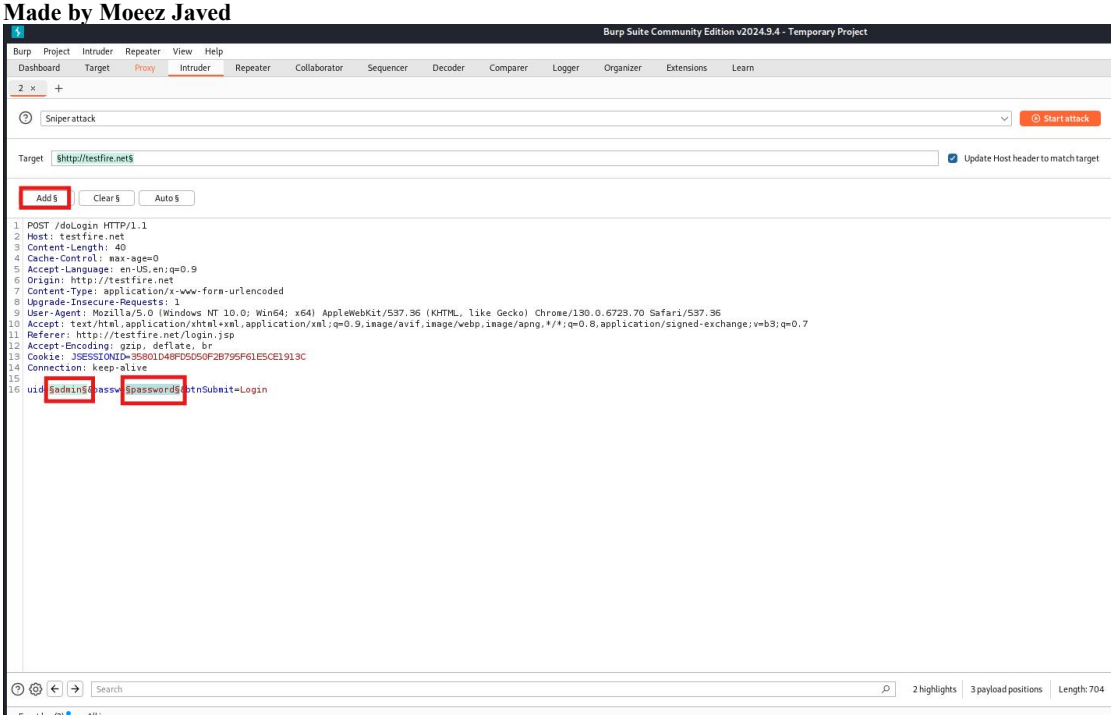
Click on the sent to the intruder.



Step 5:

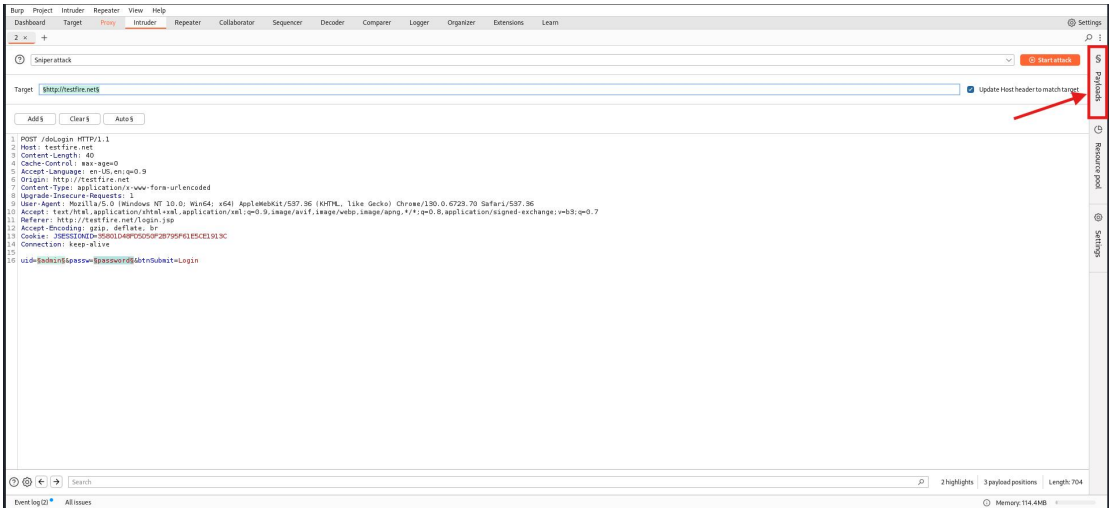
Select password and press add button than also select admin, and press add button

Made by Moeez Javed



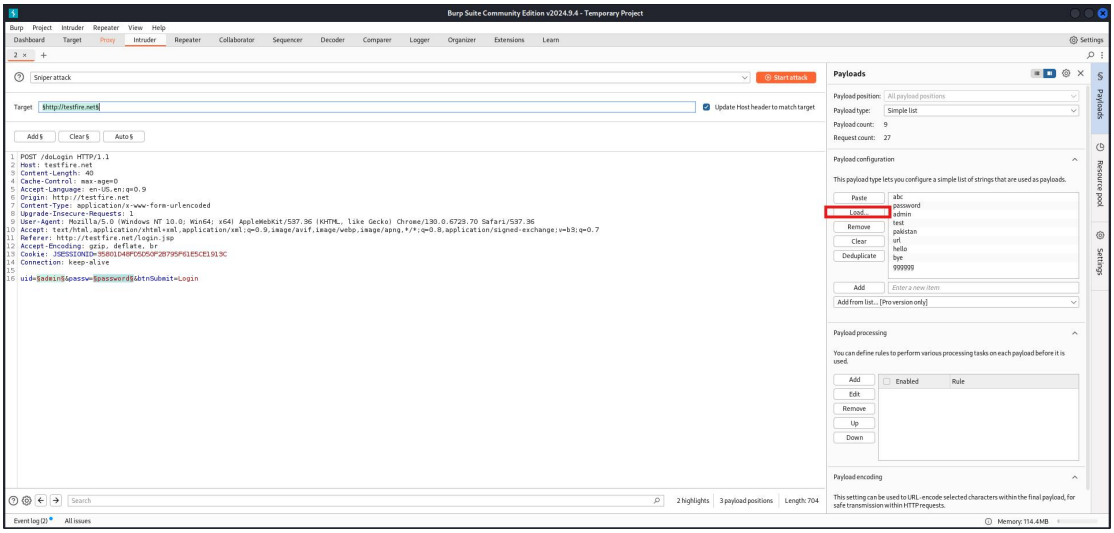
Step 6:

Click on the payload and it will display the payload.



Step 7:

Click on the load than import the password.txt file.

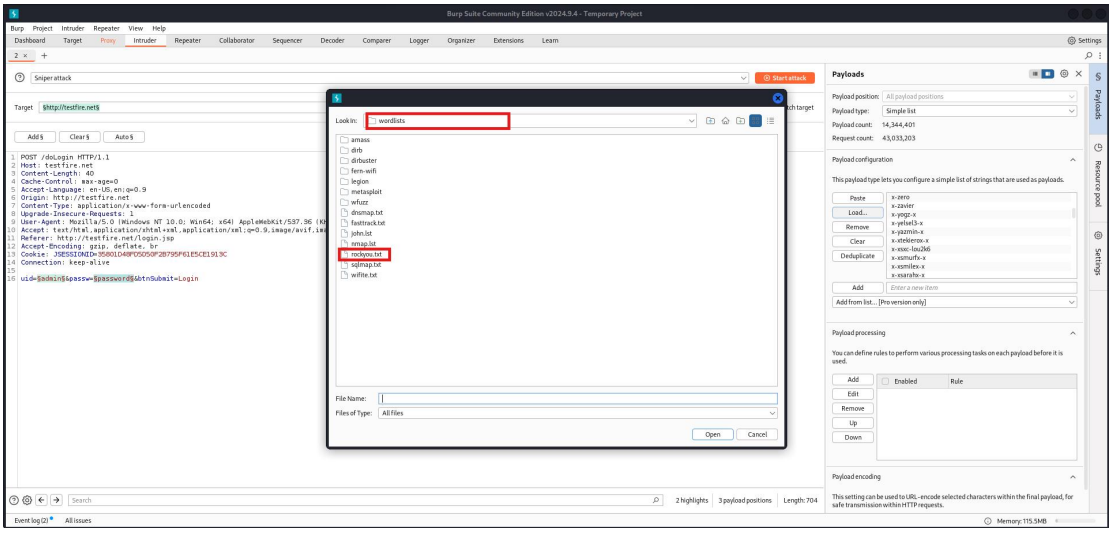


Made by Moeez Javed

Step 8:

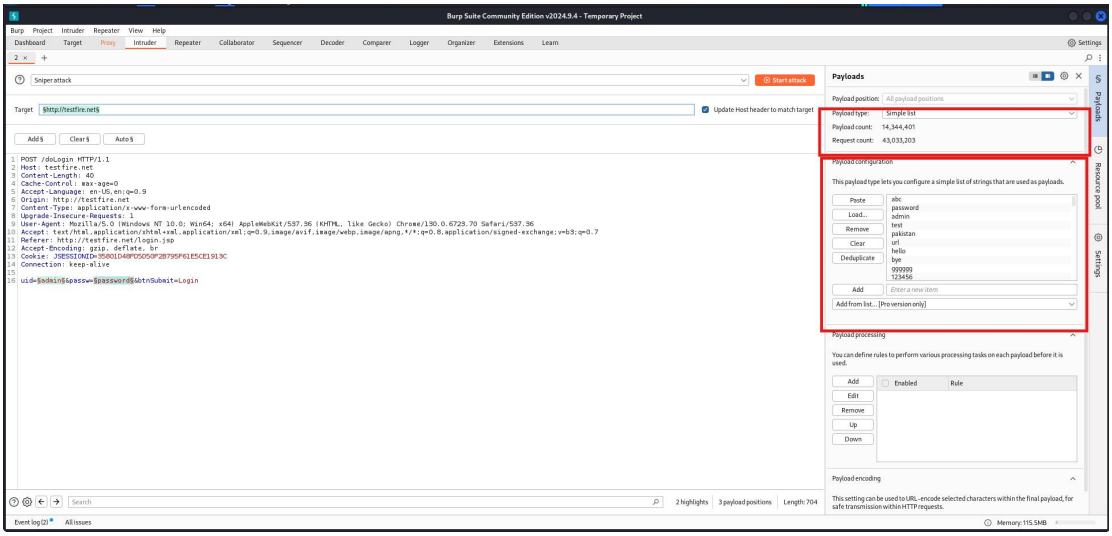
First run this command on terminal
ls -lh **/usr/share/wordlists/**

than follow this link **/usr/share/wordlists/** in the search of



Step 9:

All the passwords will be show in the image.



Step 10:

Sniper Attack
Definition:
The Sniper attack targets one input parameter at a time.
You provide a default username (e.g., Admin)
Burp replaces only the password field using the wordlist.
It's mainly used when you want to test one variable (like passwords) while keeping the others fixed.
Use Case: Brute-forcing passwords for a known user.
Battering Ram Attack
Definition:
The Battering Ram attack uses the same payload in all defined positions at the same time.

If you define both username and password positions, Burp will insert the same word from the wordlist into both fields.
Use Case: When username and password are likely to be the same, like admin:admin or test:test.

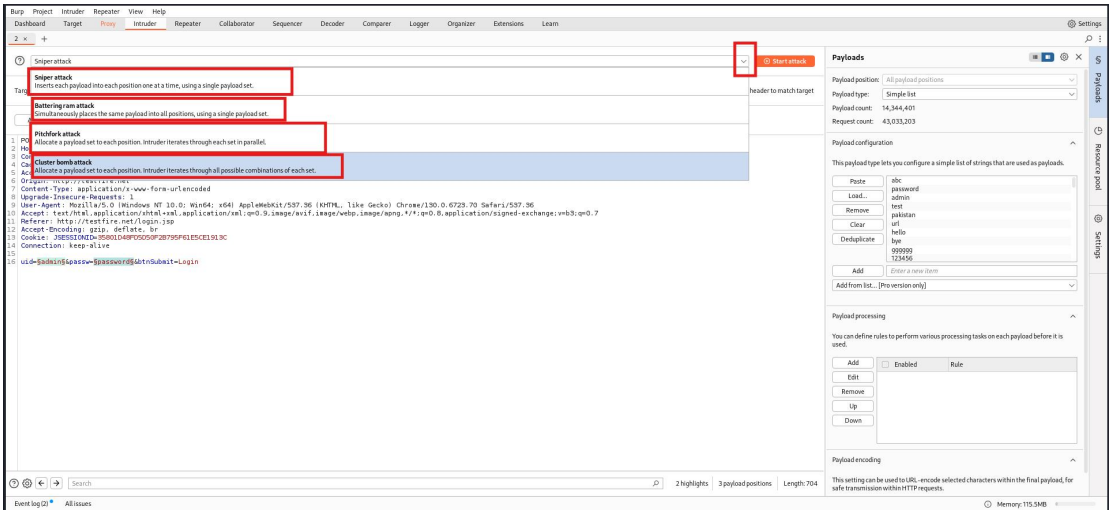
Pitchfork Attack

Definition:
The Pitchfork attack uses multiple payload positions, each with its own separate wordlist.

It runs through the wordlists in parallel, matching one line per list per request.
Example:
Username wordlist: admin, user1, root
Password wordlist: 123, password, root123
It will test admin:123, user1:password, root:root123
Use Case: When you want to test corresponding pairs of usernames and passwords.

Cluster Bomb Attack

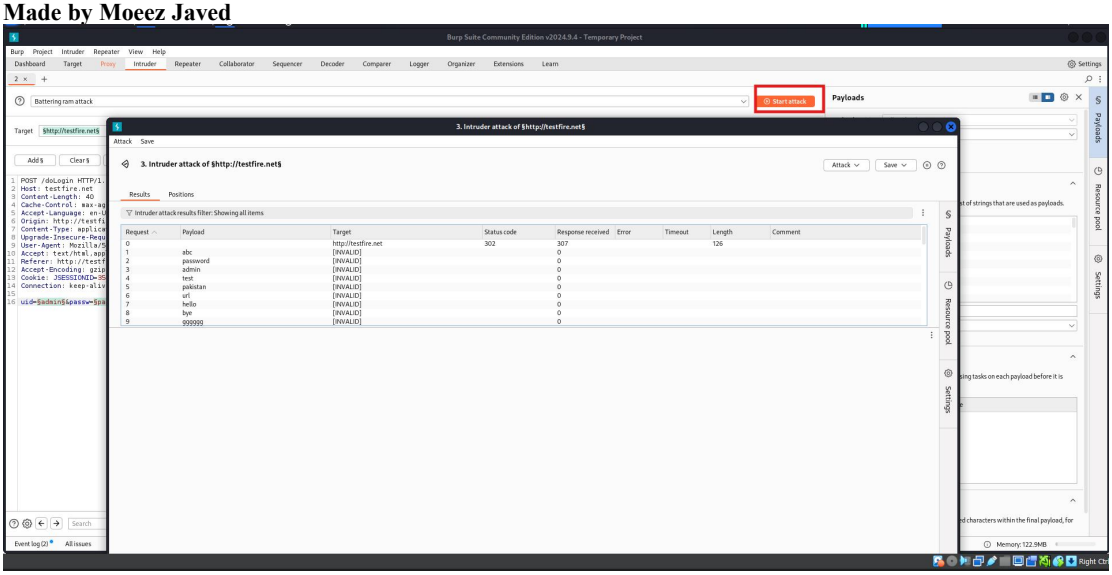
Definition:
The Cluster Bomb attack tests all possible combinations of multiple payloads.
Each position uses its own wordlist, and Burp tries every combination.
Example:
Usernames: admin, user1
Passwords: 123, password
Burp will test: admin:123, admin:password, user1:123, user1:password
Use Case: When you want to brute-force every possible combination of usernames and passwords.



Step11:

Than select Sniper or battering ram attack, and than start attack.

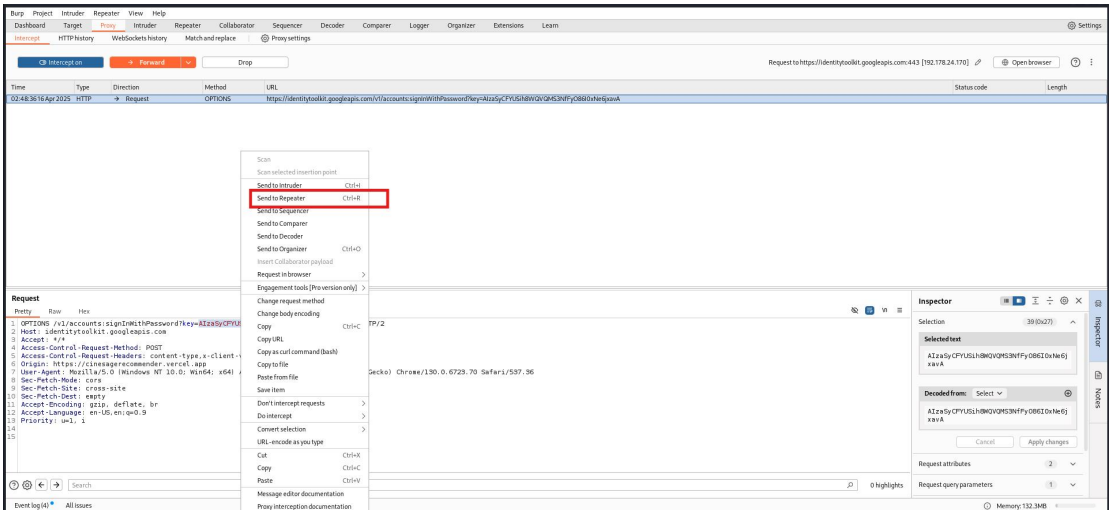
Made by Moeez Javed



Repeater

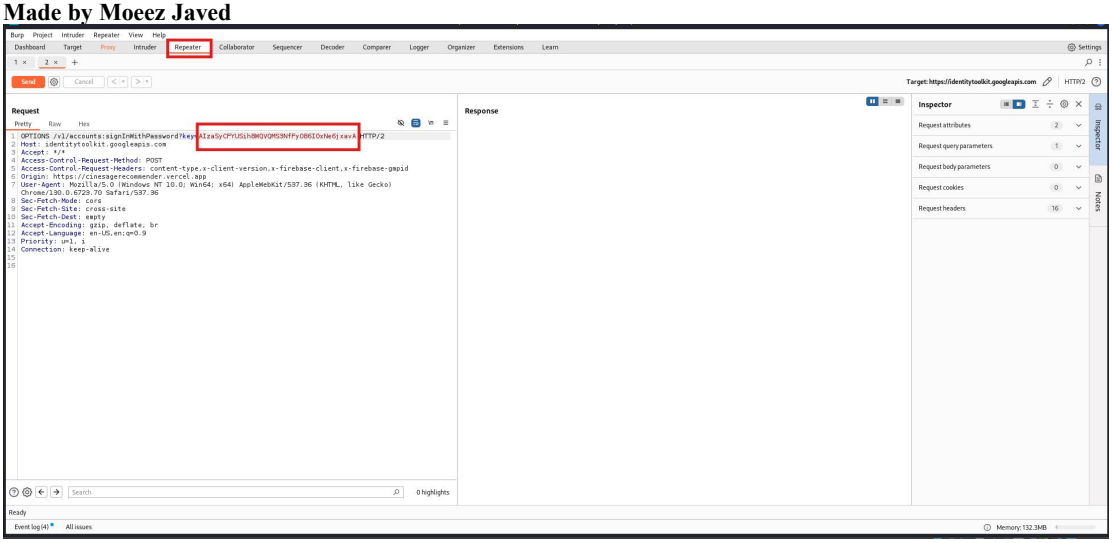
The Repeater tool is used to manually modify and resend individual HTTP or HTTPS requests to the server.
What It Does:\
Allows you to manually edit requests (headers, parameters, cookies, body, etc.)
Send the same request multiple times with different data.
View the server response for each modified request.
Useful for testing input values, checking for vulnerabilities, or analyzing how the app reacts.

Step1:



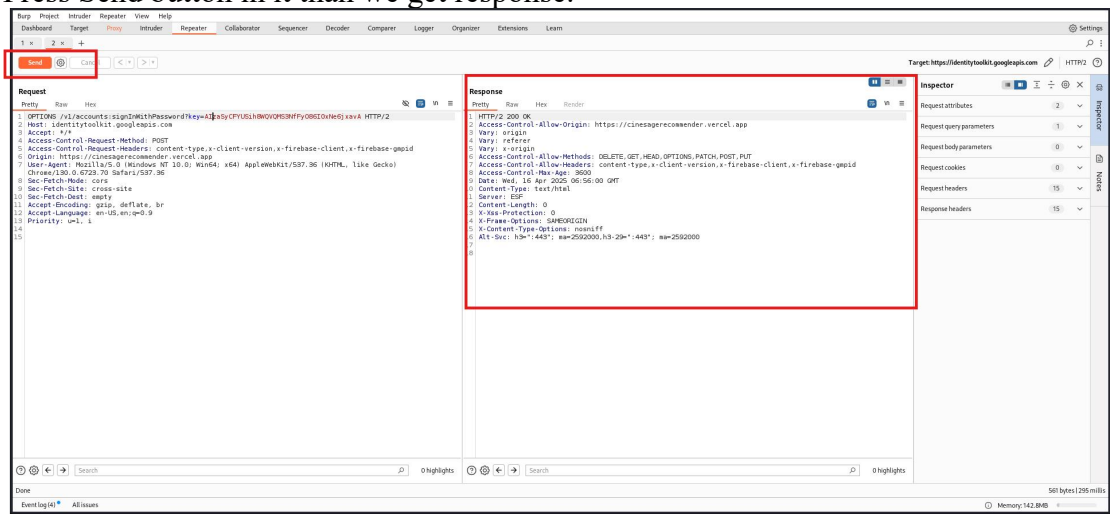
Step 2:
Move to the repeat than change in ID or any other things you want.

Made by Moeez Javed



Step3 :

Press Send button in it than we get response.



Sequence:

Sequencer in Burp Suite

The Sequencer is a tool in Burp Suite used to analyze the randomness and predictability of tokens or session IDs (such as cookies, API keys, CSRF tokens, etc.).

Why We Use It:

To check if the tokens generated by a web application (like session IDs, auth tokens, CSRF tokens) are truly random and secure.

Weak or predictable tokens can be guessed or brute-forced, which is a serious security risk.

Helps identify poor implementation of random number generators in token creation.

How It Works:

You configure Sequencer to capture a large number of tokens from the application (e.g., by replaying requests).

It then performs statistical analysis on the captured tokens.

It gives you a "randomness score" and various graphs (like character distribution, bit-level entropy, etc.).

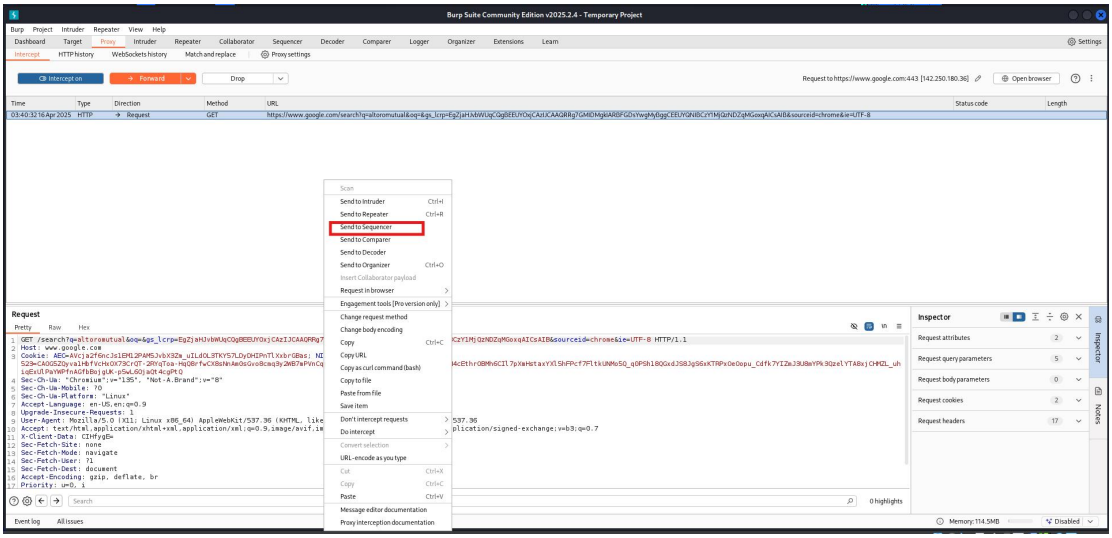
Based on this, you can determine if the tokens are predictable or secure.

Step1:

In browser go to the http://testfire.net/login.jsp we any thing in login and password

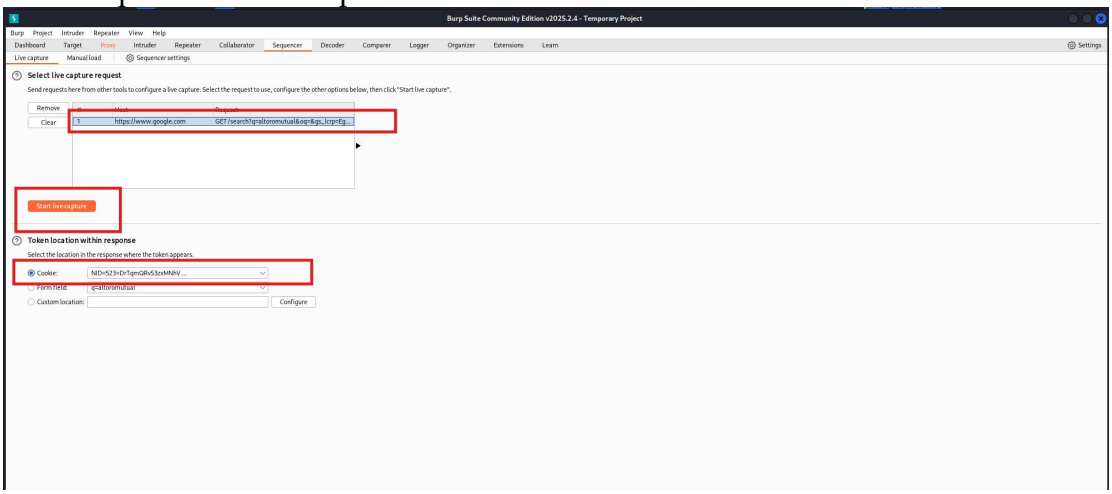
Right click on the request section and click on send to sequence.

Made by Moeez Javed



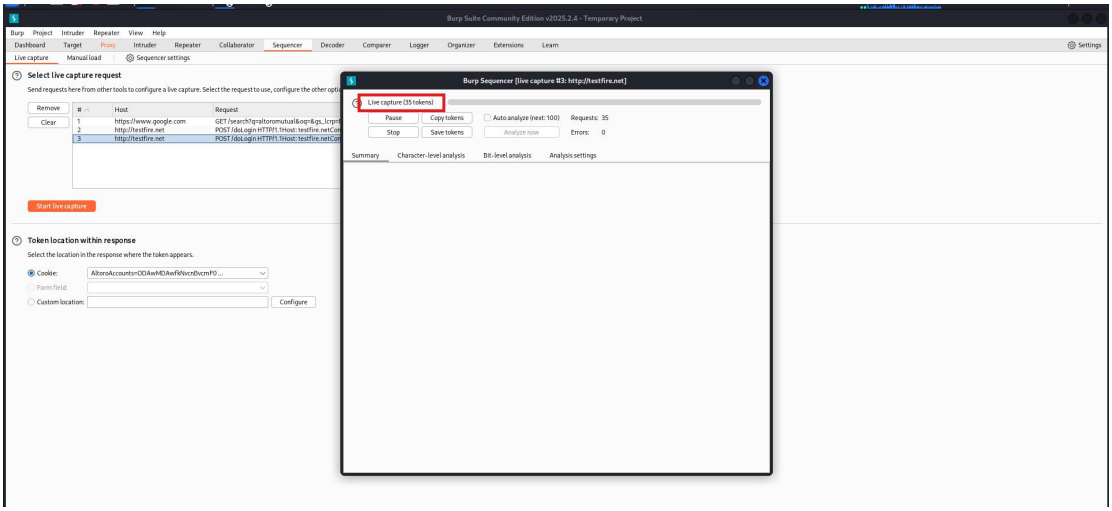
Step 2:

Now we press start live capture button.

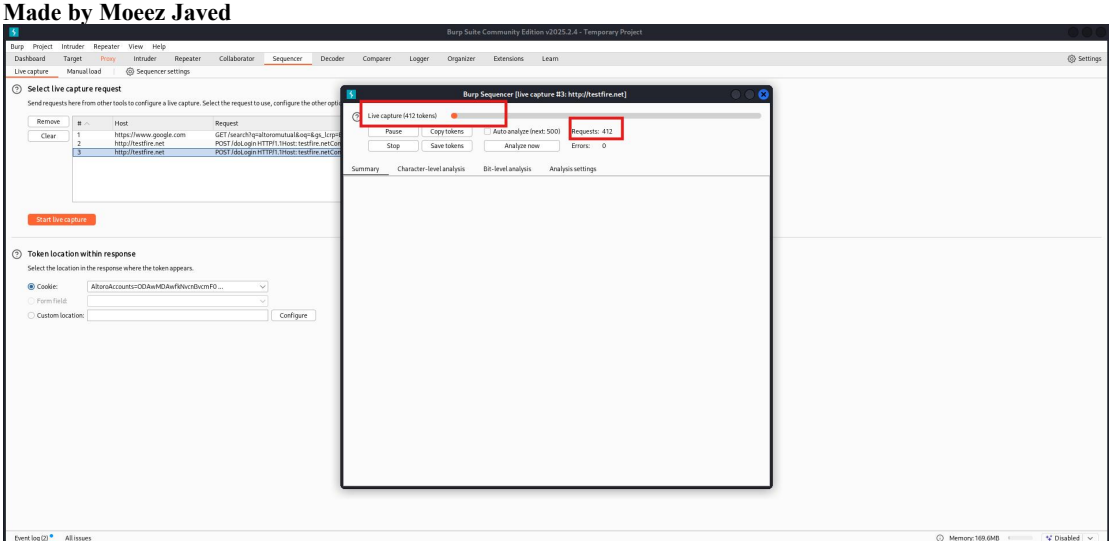


Step3:

Than it start capturing tokens.

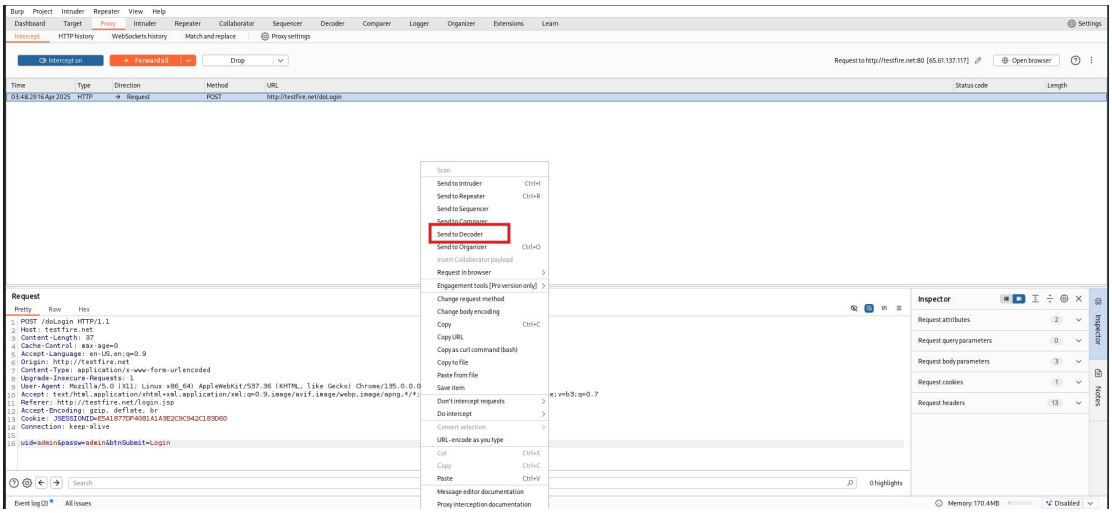


Made by Moeez Javed

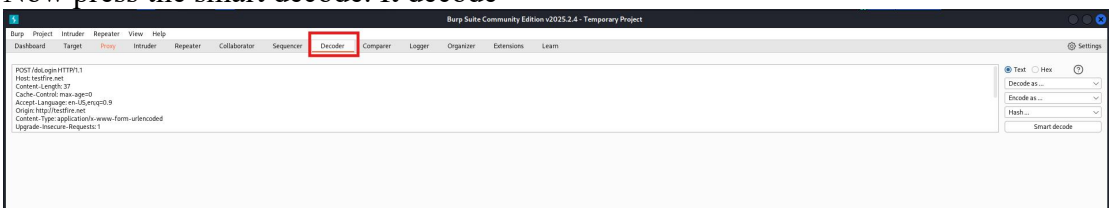


Decoder:

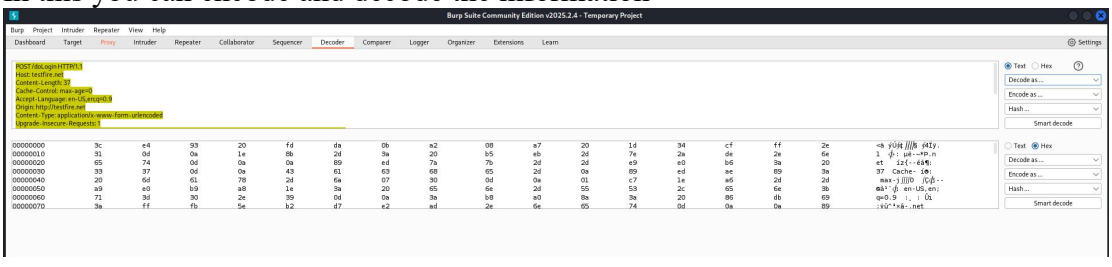
Step1:
Same step and click the send to Decoder.



Step2:
Now press the smart decode. It decode

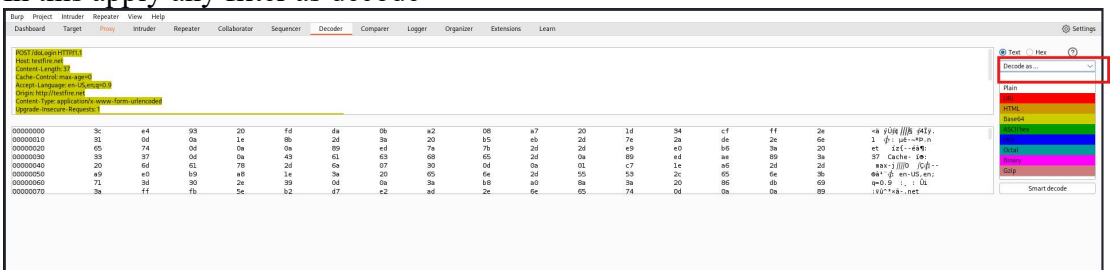


Step3:
In this you can encode and decode the information

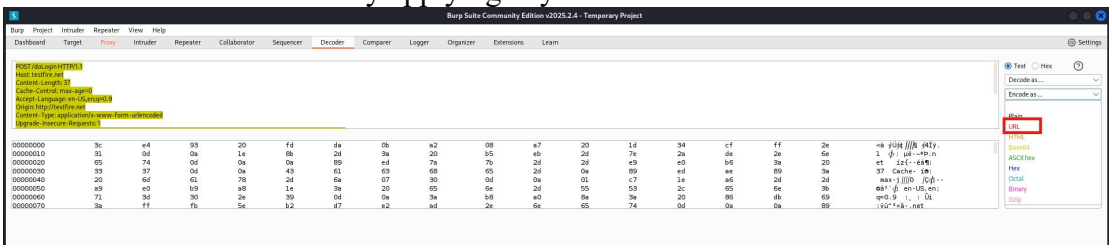


Made by Moeez Javed

In this apply any filter as decode



In this encode information by applying any filter.



Comparer

The Comparer tool is used to compare two pieces of data, such as HTTP requests, responses, tokens, or parameters.

What You Can Do With It:

Spot differences between two responses, cookies, session tokens, etc.

Highlight changes in content, making it easier to identify:

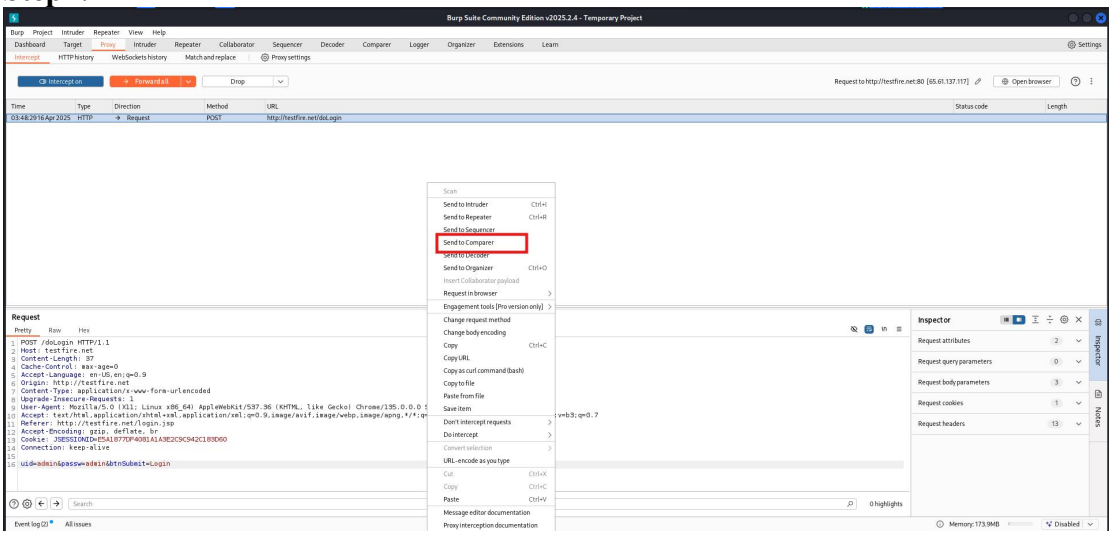
Parameter reflection

Token updates

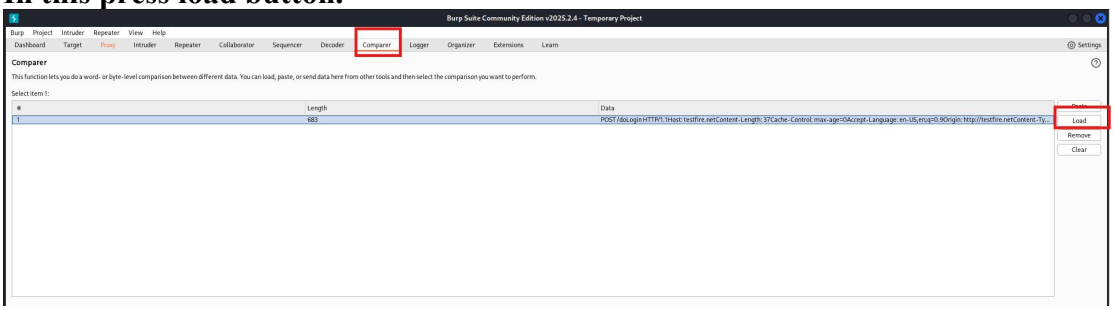
Response behavior

Made by Moeez Javed

Step1:



Step2:
In this press load button.



Task 1: Interception & Forward

Steps to Implement:
1. Open Burp Suite and your browser (ensure the proxy is configured).
2. Turn Intercept ON from the Proxy tab.
3. Visit: http://testfire.net/login.jsp.
4. Enter any username and password, and submit.
5. Burp Suite should intercept the request. Modify the username or password to something else.
6. Press the Forward button to send the request to the server.
7. Observe the server response.

- Evidence Required:
- - Screenshot of the intercepted request
- - Screenshot of the modified request before forwarding
- - Final response in the browser or Burp

Task 2: Intruder – Sniper Attack

Steps to Implement:
1. From the Proxy tab, right-click the login request → Send to Intruder.
2. Select only the password as payload position.
3. Go to the Payload tab, load a password wordlist (/usr/share/wordlists/rockyou.txt or a custom file).
4. Choose Sniper as the attack type.
5. Start the attack and observe the response lengths/status codes.

- Evidence Required:
- - Screenshot of payload positions
- - Wordlist preview
- - Screenshot of Intruder results (showing different responses)

A: Intruder – Battering Ram

Steps to Implement:
1. Set payload positions for both username and password.
2. Load a single wordlist for both positions.

3. Set attack type to Battering Ram.
4. Start the attack.
- Evidence Required:
- - Screenshot of configuration
- - Attack results showing matching username/password tests

B: Intruder – Pitchfork & Cluster Bomb

Pitchfork Steps:
1. Set two payload positions (username & password).
2. Load two different wordlists.
3. Choose Pitchfork and start attack.

Cluster Bomb Steps:
1. Same setup, but choose Cluster Bomb instead.
2. Observe all combinations being tested.
- Evidence Required (for both):
- - Payload position screenshot
- - Wordlist examples
- - Response comparison showing differences

Task 3: Repeater Tool

Steps to Implement:
1. Right-click on the login request → Send to Repeater.
2. Change the password value multiple times manually.
3. Click Send after each modification and observe response changes.
- Evidence Required:
- - Screenshot of each modified request
- - Corresponding server response

Task 4: Sequencer

Steps to Implement:
1. Intercept a login request with a session token.
2. Right-click → Send to Sequencer.
3. Start Live Capture and collect ~100 tokens.
4. Analyze randomness score and character distribution.
- Evidence Required:
- - Screenshot of Sequencer setup
- - Screenshot of randomness analysis

Task 5: Decoder

Steps to Implement:
1. Copy any encoded value (e.g., Base64).
2. Go to Decoder tab → Paste → Smart Decode.
3. Try encoding it again with different formats.
- Evidence Required:
- - Screenshot before and after decoding