AI WITH CYBER SECURITY

ASSIGNMENT-4

SHREYA SINGH

BURPSUITE

1)WHAT IS BURPSUITE?

Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger, which is also the alias of its founder Dafydd Stuttard. BurpSuite aims to be an all in one set of tools and its capabilities can be enhanced by installing add-ons that are called BApps. It is the most popular tool among professional web app security researchers and bug bounty hunters. Its ease of use makes it a more suitable choice over free alternatives like OWASP ZAP.

2)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

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

3)Features and Tools Offered by 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

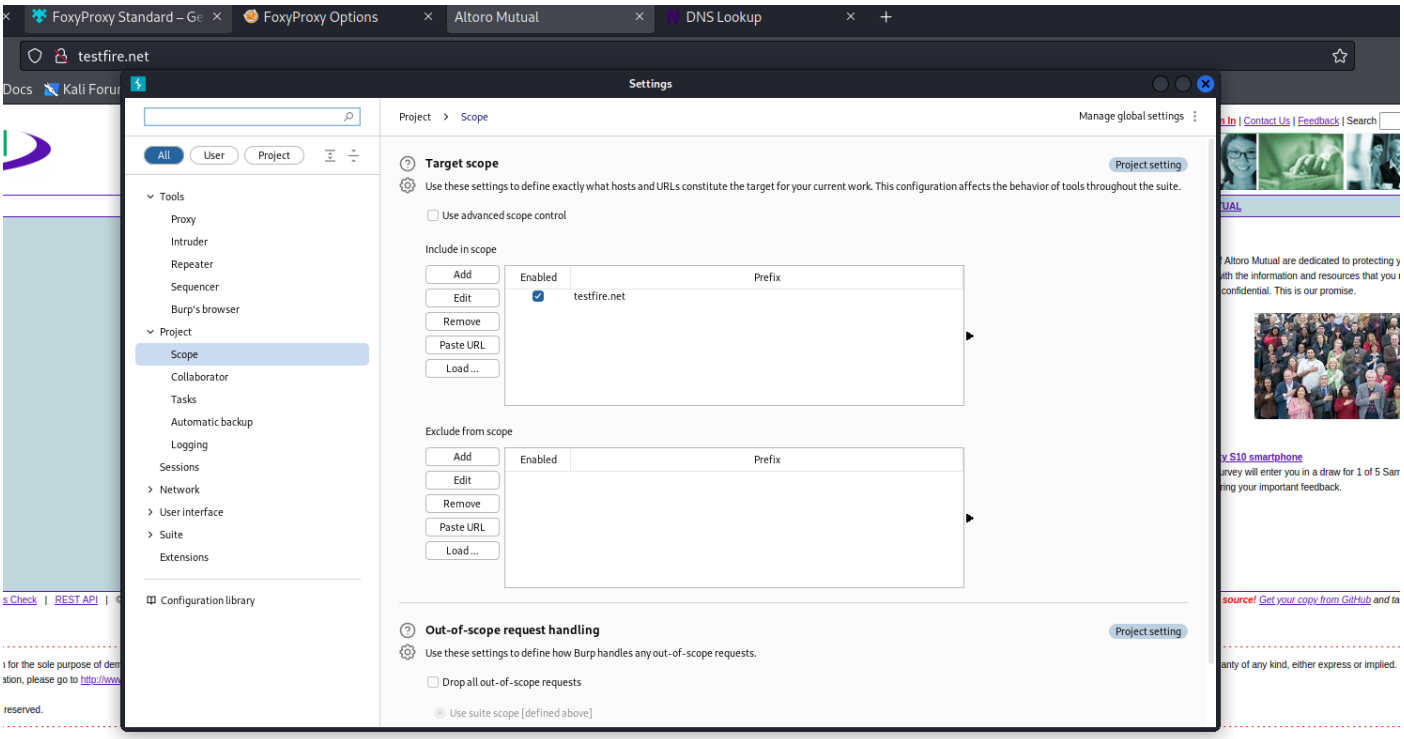
BurpSuite enables the integration of extra components into the toolkit to expand its functionality. These external components are referred to as BApps. These perform the same tasks as browser extensions... The Extender window allows you to **examine, modify, install, and remove them**. Some of them are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

8. Scanner

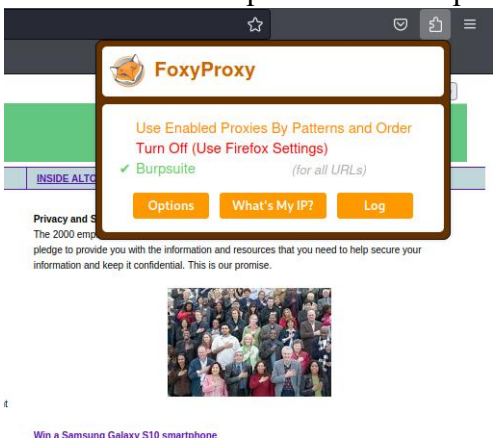
The community edition does not have a scanner. It automatically analyses the website for a variety of common vulnerabilities and provides them together with details on the reliability of each discovery and the difficulty of exploiting them. It is routinely updated to add brand-new, and lesser-known vulnerabilities.

WE ARE NOW GOING TO TRY BRUTE FORCE ATTACK ON TESTFIRE.NET

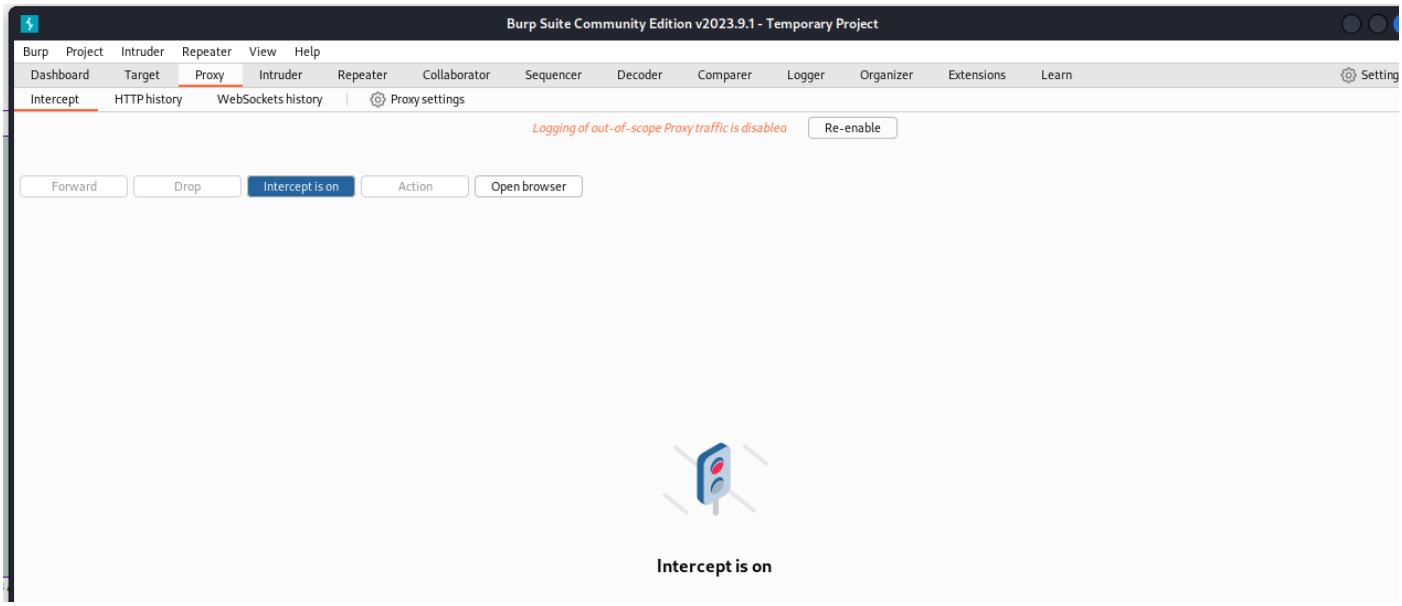
- First we add the website by going to target tab -> add

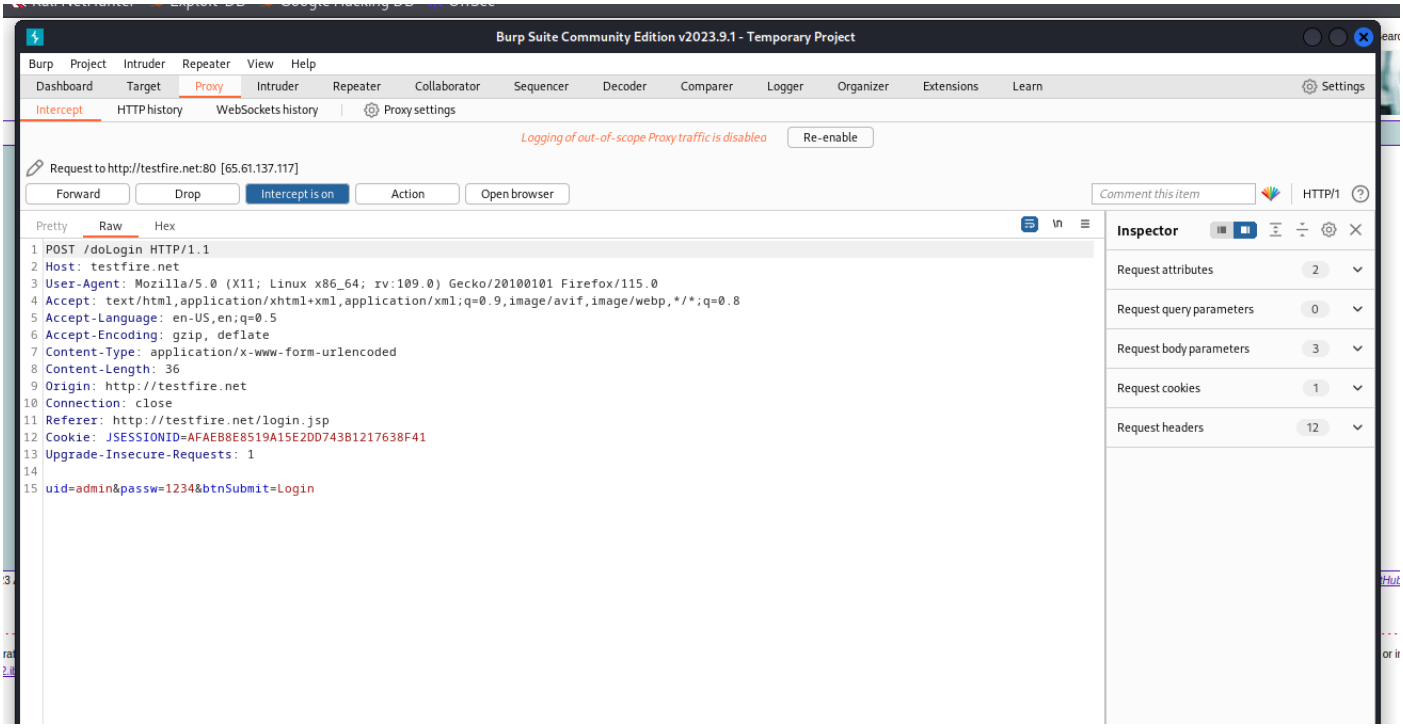


- Choose burp as our default proxy on foxyproxy.

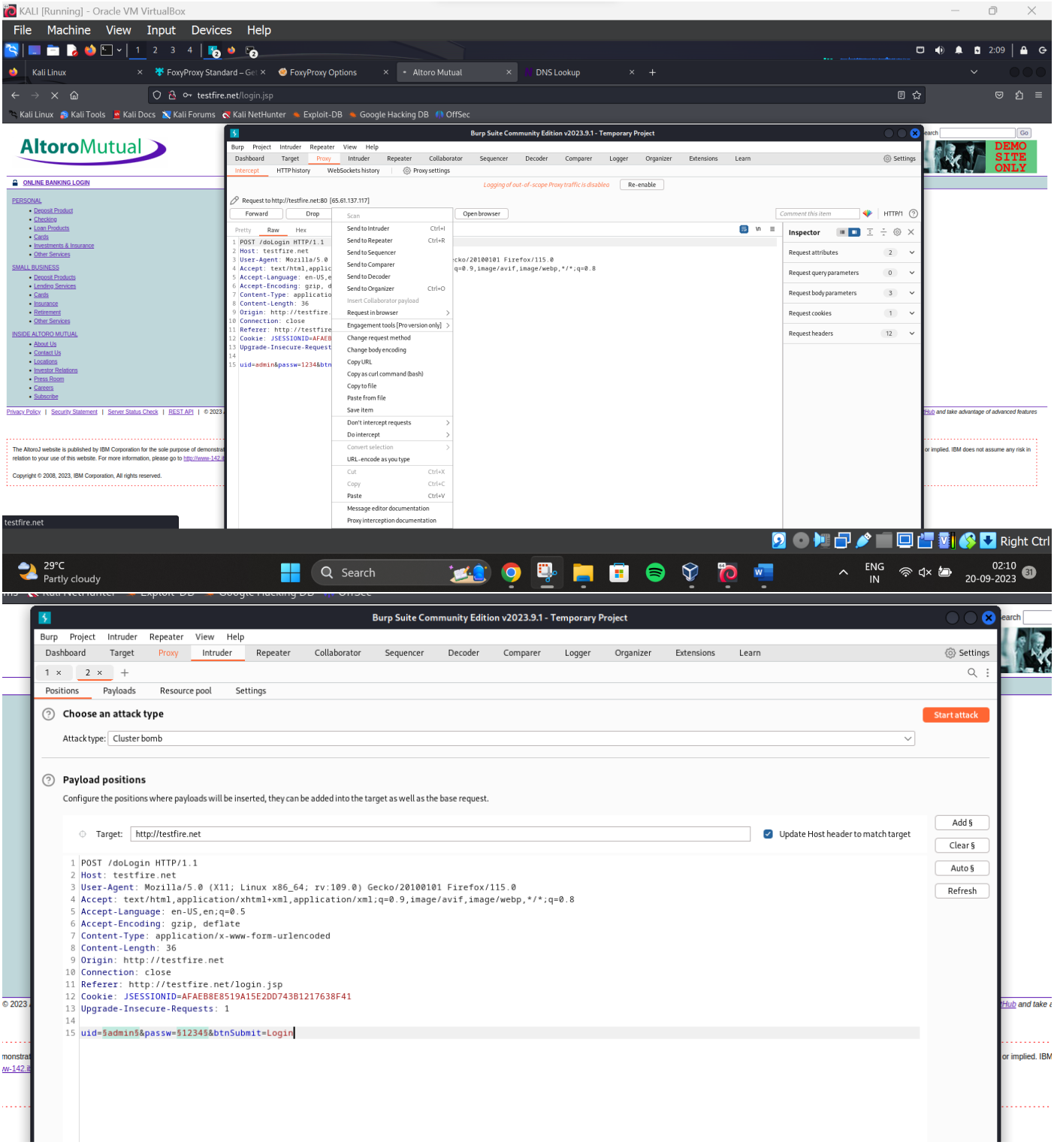


- Go to proxy and turn on the intercept and then click on the login page of the website and give in random username and password.

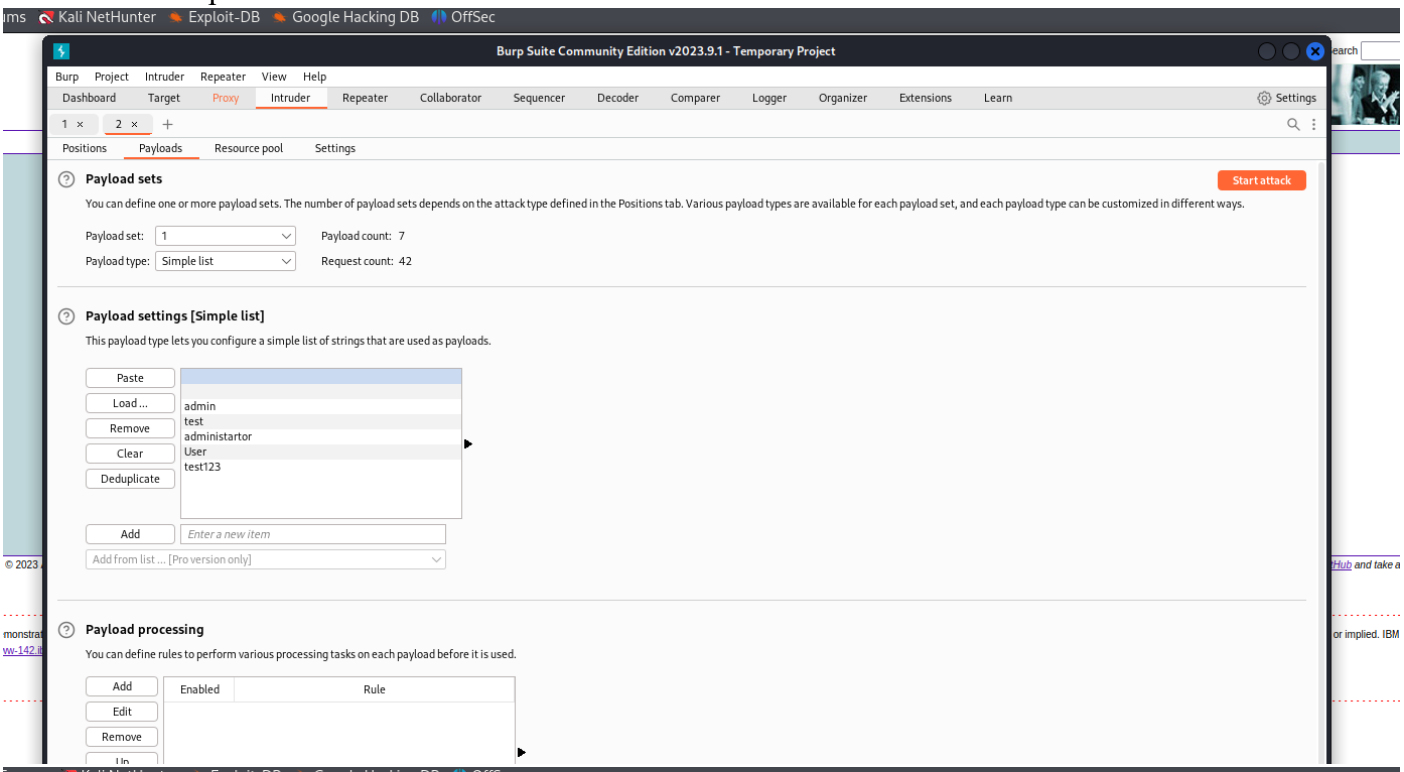


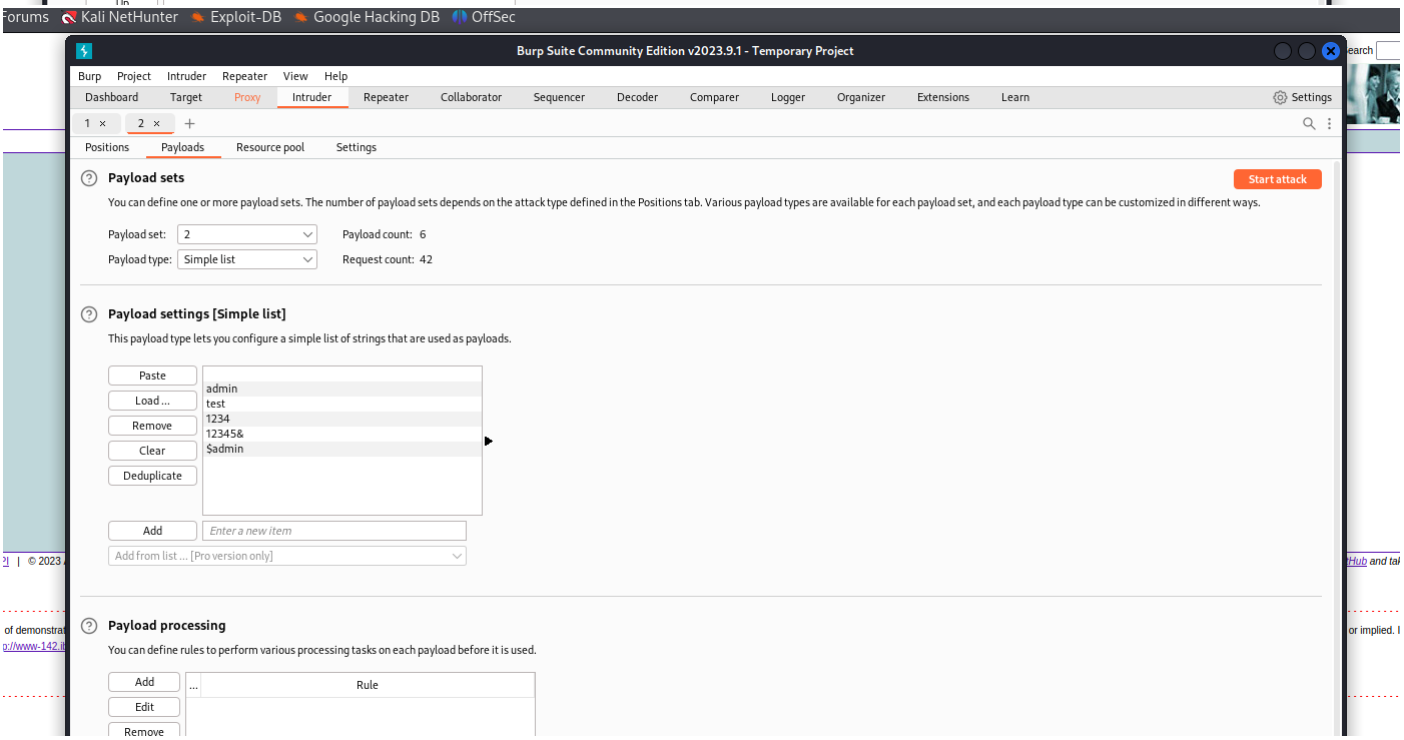


- Then we sent it to intruder and go to positions tab choose cluster bomb attack and select the given input of username as payload 1 and given input of password as payload 2 by clicking on add.

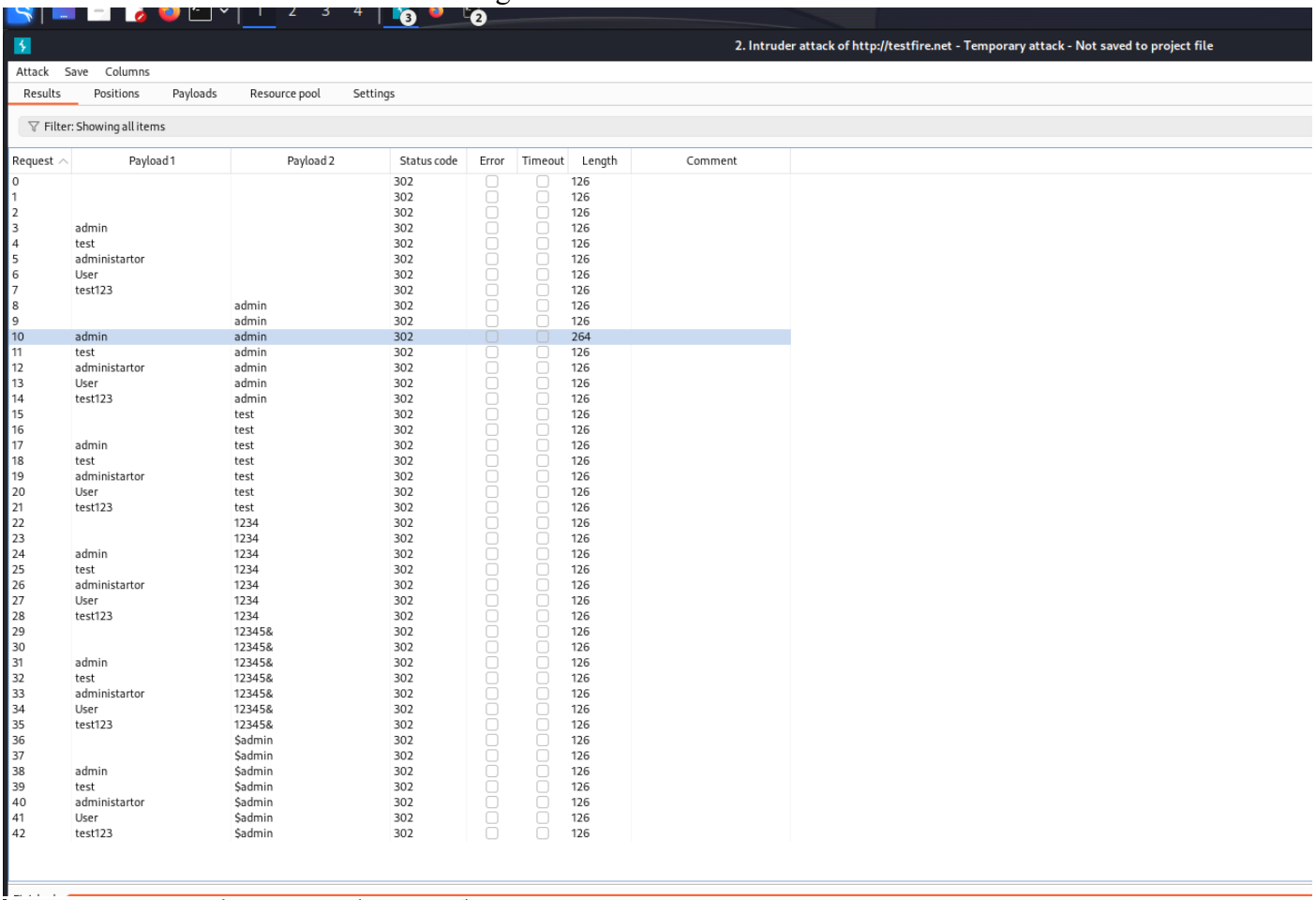


- Then we go to the payloads tab and select payload 1 that is our username in this case and choose simple text and below give some random expected usernames. We can also upload a file here but since I do not have one I did it this way. We do the same for payload 2 which is our passwords and then start the attack.

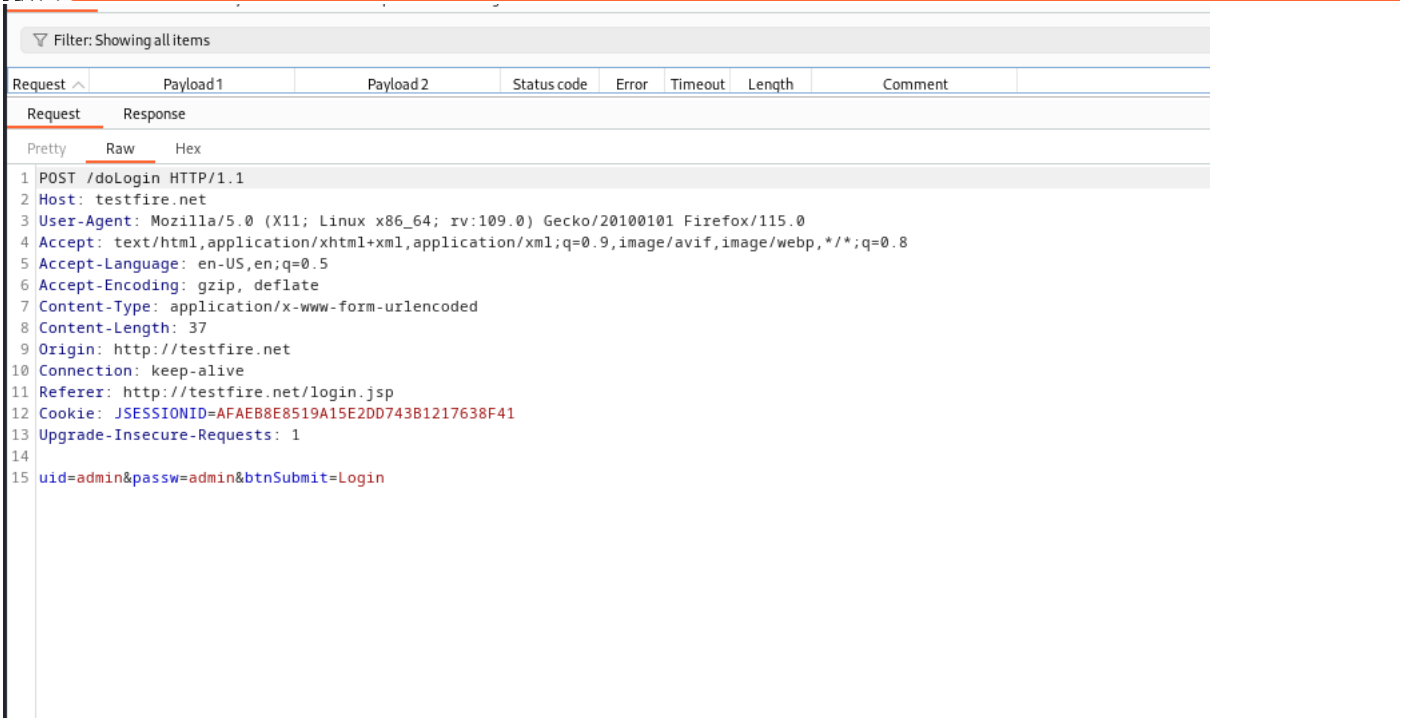




- After the attack is finished we can see that the highlighted admin admin has different length from the others. Thus it can be a probable solution. Upon checking Request and response we can assure that this is working.



Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			302			126	
1			302			126	
2			302			126	
3	admin		302			126	
4	test		302			126	
5	administartor		302			126	
6	User		302			126	
7	test123		302			126	
8		admin	302			126	
9		admin	302			126	
10	admin	admin	302			264	
11	test	admin	302			126	
12	administartor	admin	302			126	
13	User	admin	302			126	
14	test123	admin	302			126	
15		test	302			126	
16		test	302			126	
17	admin	test	302			126	
18	test	test	302			126	
19	administartor	test	302			126	
20	User	test	302			126	
21	test123	test	302			126	
22		1234	302			126	
23		1234	302			126	
24	admin	1234	302			126	
25	test	1234	302			126	
26	administartor	1234	302			126	
27	User	1234	302			126	
28	test123	1234	302			126	
29		12345&	302			126	
30		12345&	302			126	
31	admin	12345&	302			126	
32	test	12345&	302			126	
33	administartor	12345&	302			126	
34	User	12345&	302			126	
35	test123	12345&	302			126	
36		$admin	302			126	
37		$admin	302			126	
38	admin	$admin	302			126	
39	test	$admin	302			126	
40	administartor	$admin	302			126	
41	User	$admin	302			126	
42	test123	$admin	302			126	



- We then give the inputs in the login page and hence we are logged in.