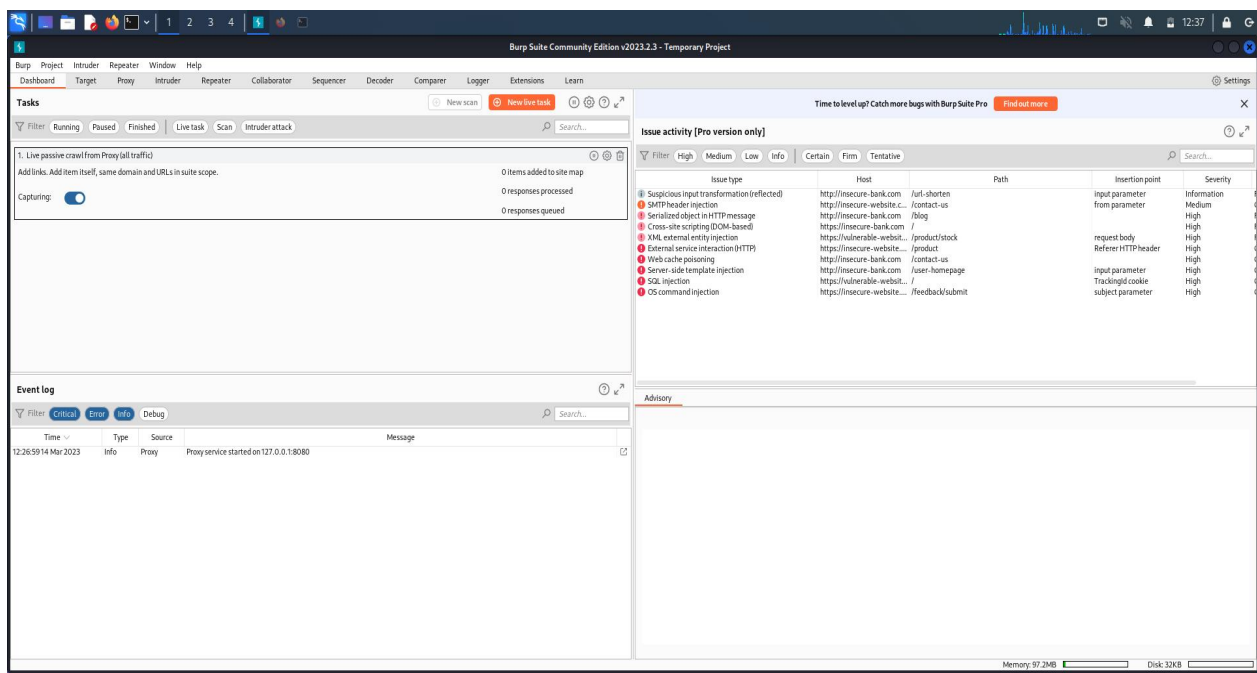


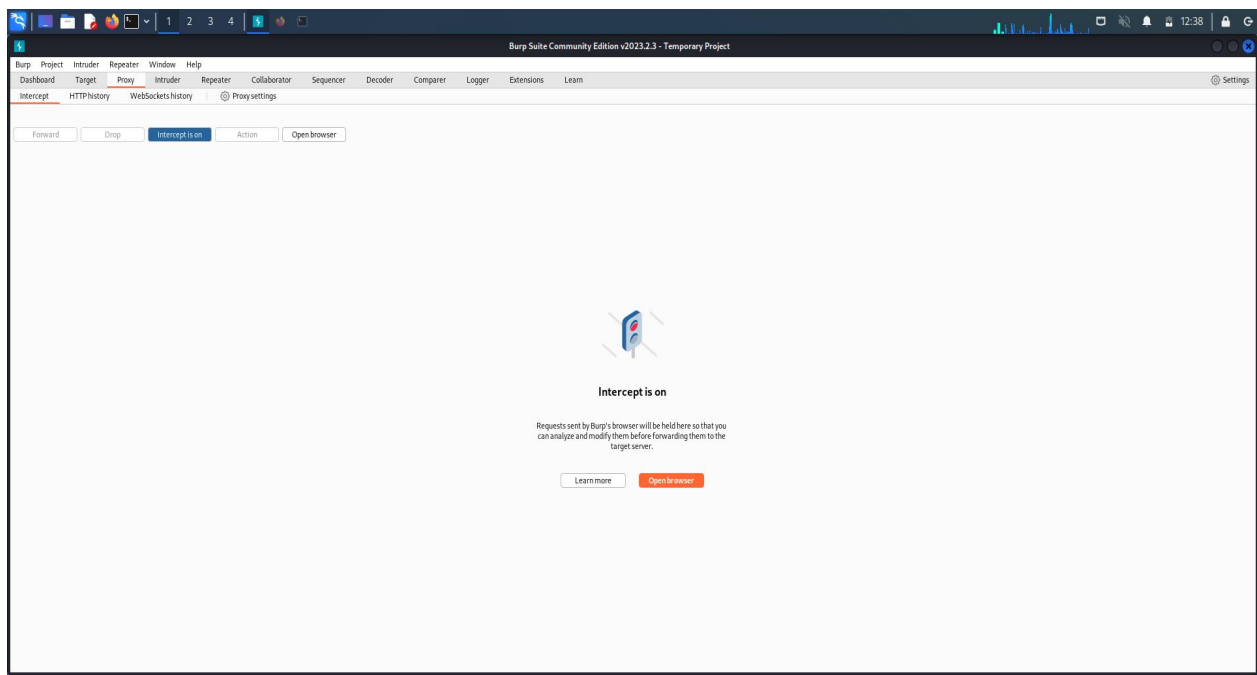
# PASSWORD CRACKING OF ONLINE VULNERABLE WEBSITE(testfire.net) USING BURPSUITE

Burp Suite, by Port Swigger, is a versatile and powerful tool for web app pentesting. Besides web form authentication testing, it can also be used to test for session ID randomization, injection attacks, fuzzing and numerous other attacks.

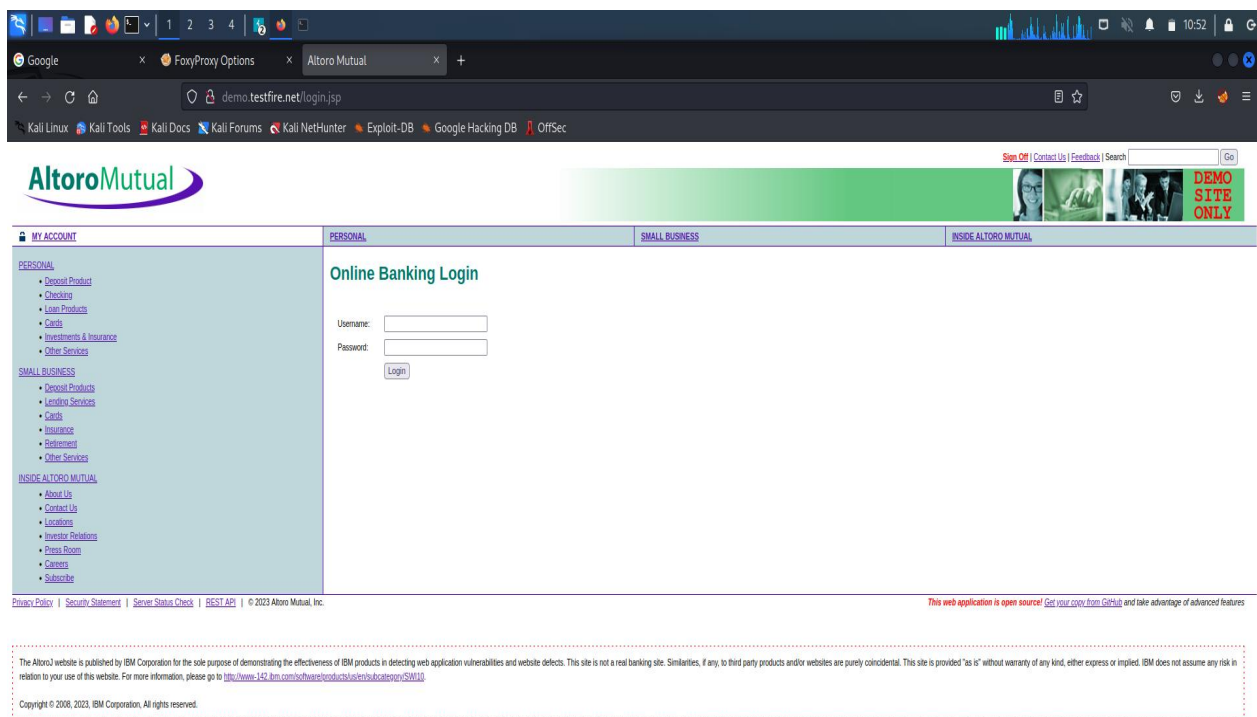
Password cracking of testfire.net:

Step 1: Open Burp Suite and switch on the intercept.





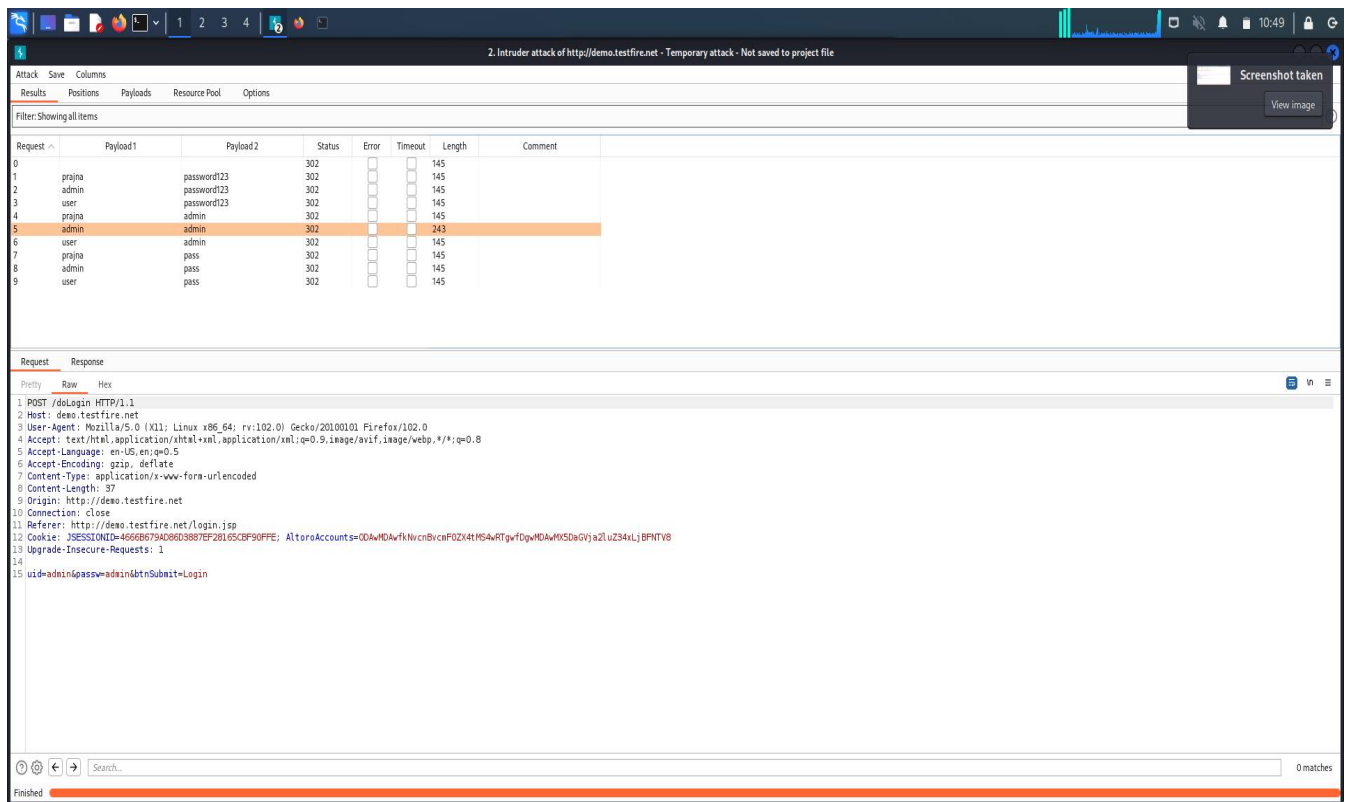
Step 2: Open demo.testfire.net and try to login.



Step 3: Open Burp Suite and go to proxy. Search for “doLogin” and send the host id to the intruder.

In intruder select the payloads for username and password. Select attack type as cluster bomb. In payload options , enter different usernames and passwords. Then start the attack.

Check for change in length. If length changes, then that is the correct username and password.

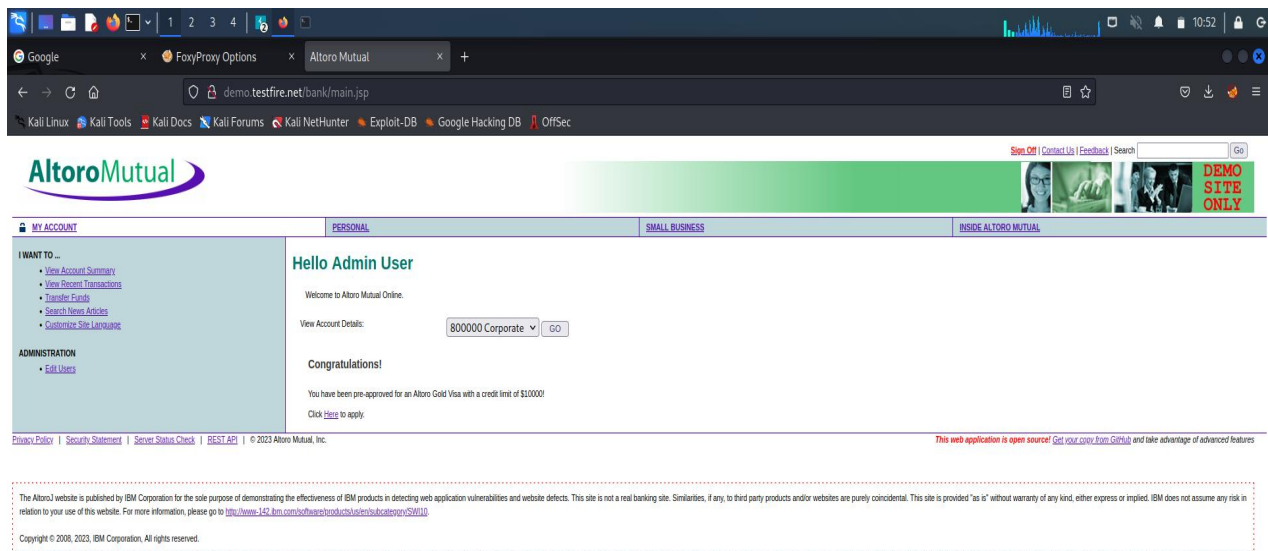


Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302			145	
1	prajna	password123	302			145	
2	admin	password123	302			145	
3	user	password123	302			145	
4	prajna	admin	302			145	
5	admin	admin	302			243	
6	user	admin	302			145	
7	prajna	pass	302			145	
8	admin	pass	302			145	
9	user	pass	302			145	

The screenshot also shows the HTTP request details for the successful login attempt (Request 5):

```
1 POST /doLogin HTTP/1.1
2 Host: demo.testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 37
9 Origin: http://demo.testfire.net
10 Connection: close
11 Referer: http://demo.testfire.net/login.jsp
12 Cookie: JSESSIONID=4666B679AD086D3887EF28165CBF90FFE; AltoraAccounts=0D&MD&wFkNvcnBvcnFOZi4tMS4vRTgwVjDpYwMD&wSDaGVpZlUz34xLjBfNTV8
13 Upgrade-Insecure-Requests: 1
14
15 uid=admin&pass=admin&btnSubmit=Login
```

In the above example, username is admin and password is admin. Enter this in testfire.net. By this, the password cracking of online vulnerable website using Burp Suite is successful.



The screenshot shows the website interface for 'AltoraMutual'. The user is logged in as 'Admin User'. The account details show a balance of '800000 Corporate'. The website also displays a 'DEMO SITE ONLY' banner and a footer with legal disclaimers.