PCP CS: PENETRATION TESTING

<u>Project</u>: Conducting and performing VAPT on a bank named Altoro Mutual.

<u>Name</u>: Ananya Mondal

<u>Batch</u>: pcp-cs-nov-2023-cohort-2

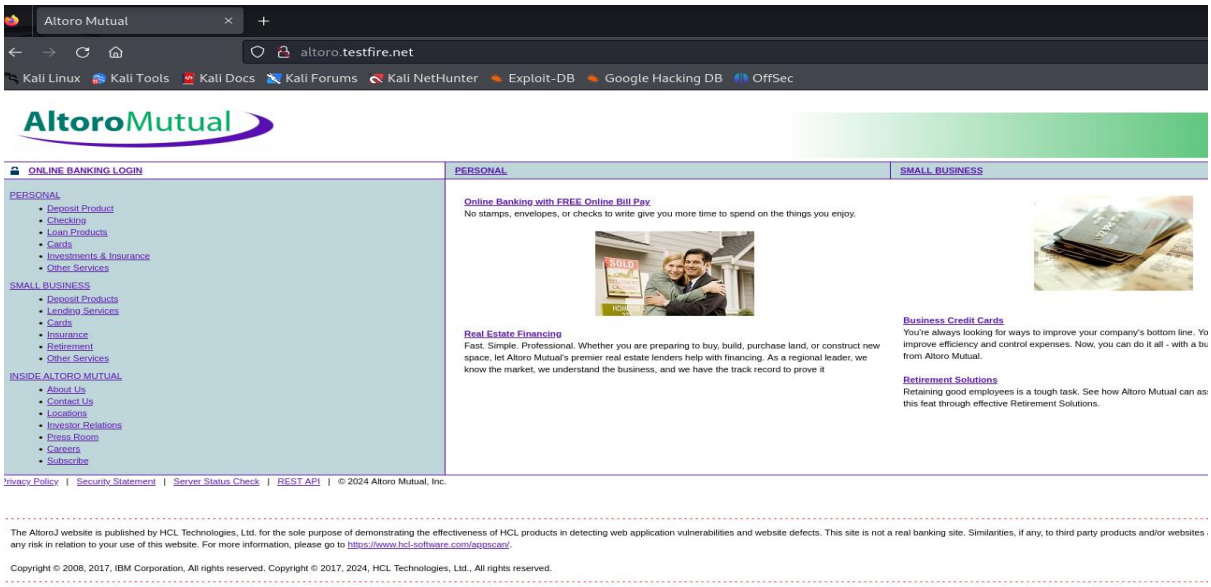
Task (Activities):

In this project, you will be testing the following vulnerabilities:

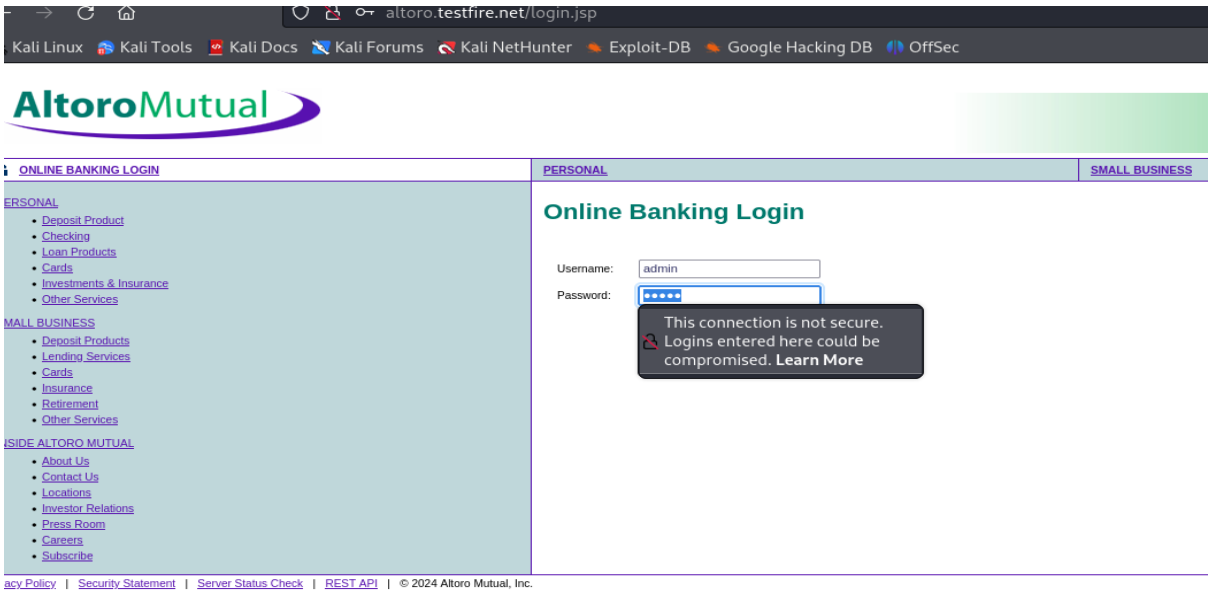
1. Cross Site Scripting (XSS) Vulnerability
2. SQL Injection
3. Brute Force Attack
4. Access Control Vulnerability
5. HTML Injection

TASK 1: Cross Site Scripting (XSS) Vulnerability

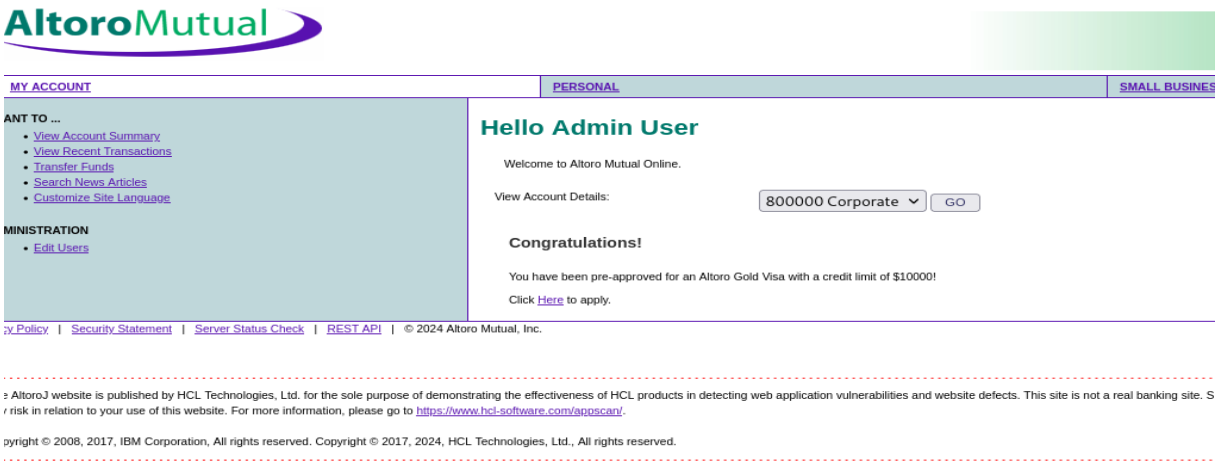
1.i) Opening the website of Altoro Mutual Bank



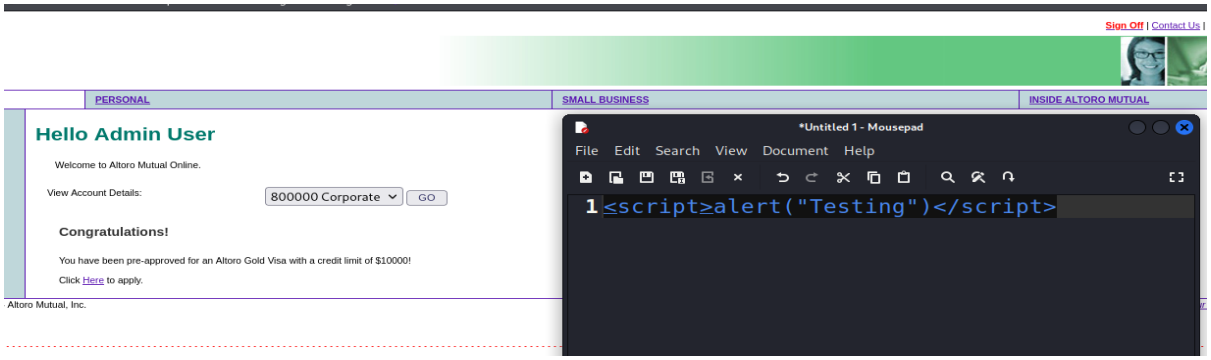
1.ii) Logging in by trying different login credentials. Here we successfully logged in using these credentials→ (login id- “admin”, password- “admin”)



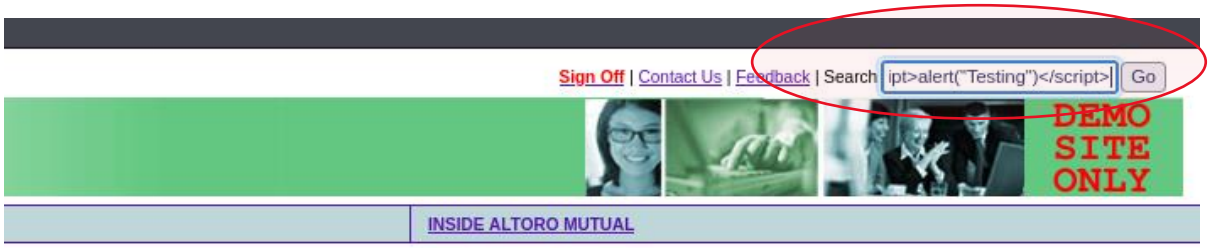
1.iii) Successfully logged in



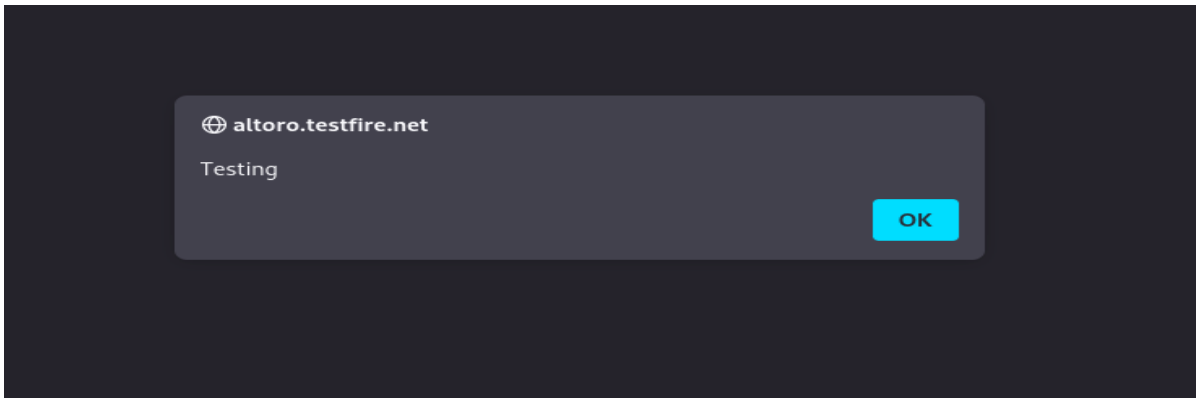
1.iv) Testing for the cross-site scripting vulnerability using the script given below



1.v) Using the script in the search area

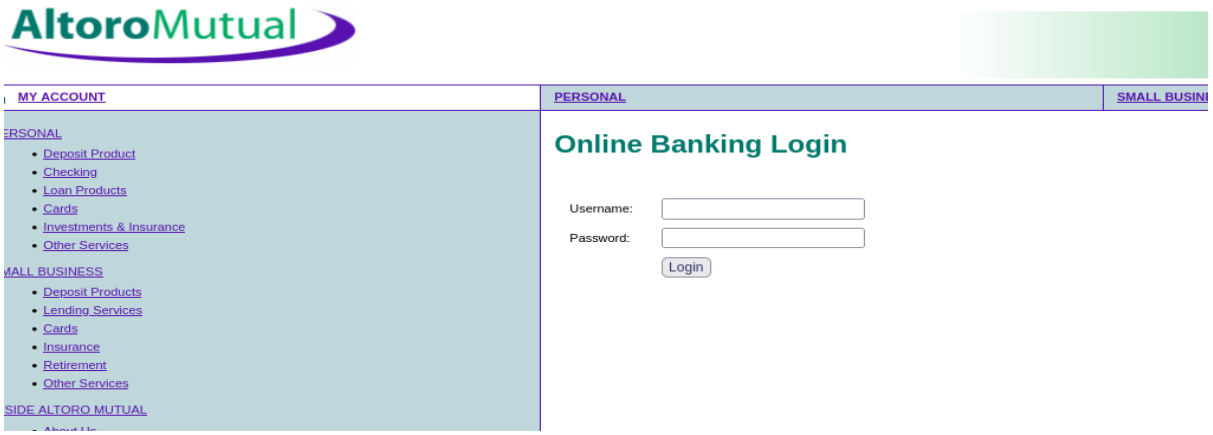


1.vi) Yes, the website is prone to cross-site scripting vulnerability

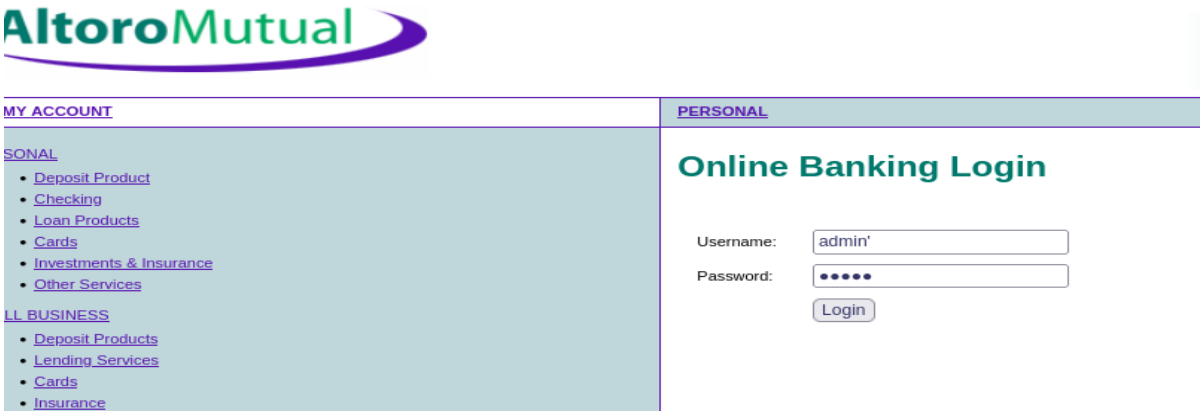


TASK 2: SQL Injection

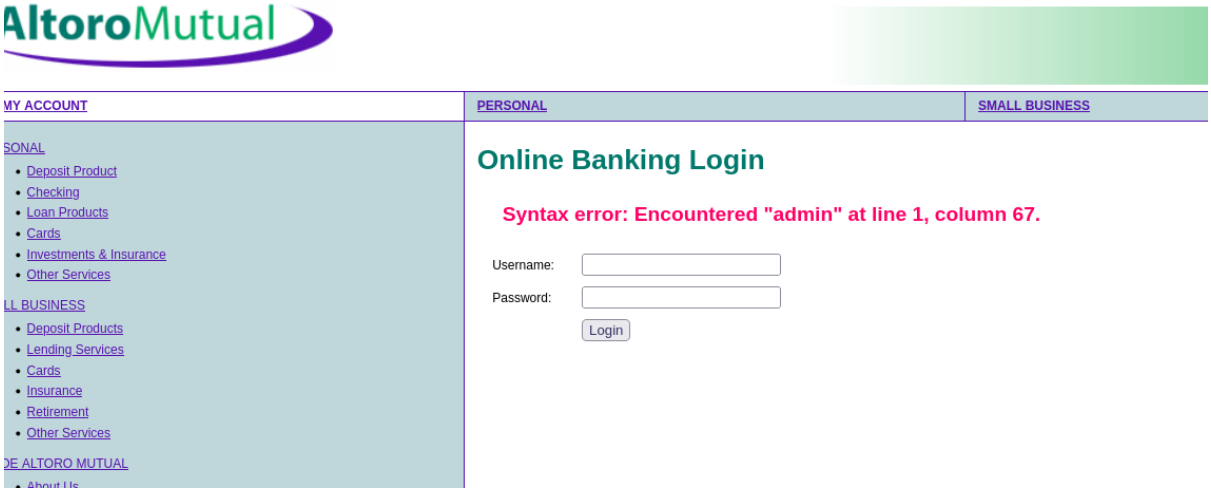
2.i) Opening the login page again for checking the SQL Injection vulnerability



2.ii) Checking for the SQL Injection vulnerability using a “single quote” after admin in the username box and using “admin” as password to see if it throws any error.



2.iii) The website throws an error



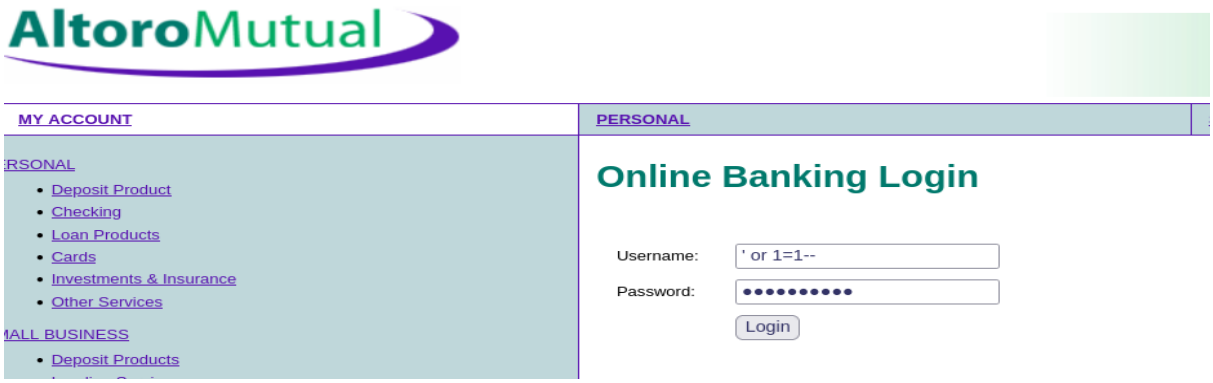
2.iv) Now we can use the Blind SQL Injection Cheat Sheet for various bypass logins

Bypassing login screens (SMO+)

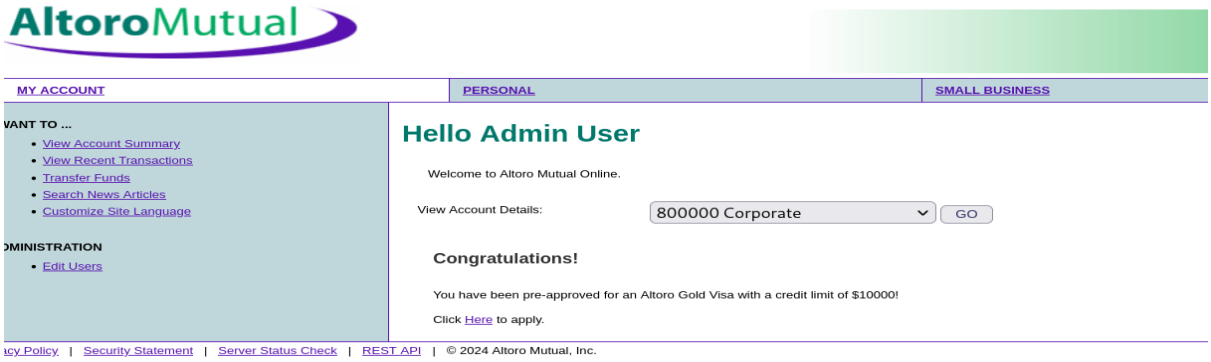
This is SQL injection 101—here are some typical login tricks that you can use with form fields and parameters:

- `admin' --`
- `admin' #`
- `admin'/*`
- `' or 1=1--`
- `' or 1=1#`
- `' or 1=1/*`
- `') or '1'='1--`
- `') or ('1'='1--`

2.v) We can try any of the logins and check if it bypasses. Here I used [`' or 1=1--`] as username and password both.

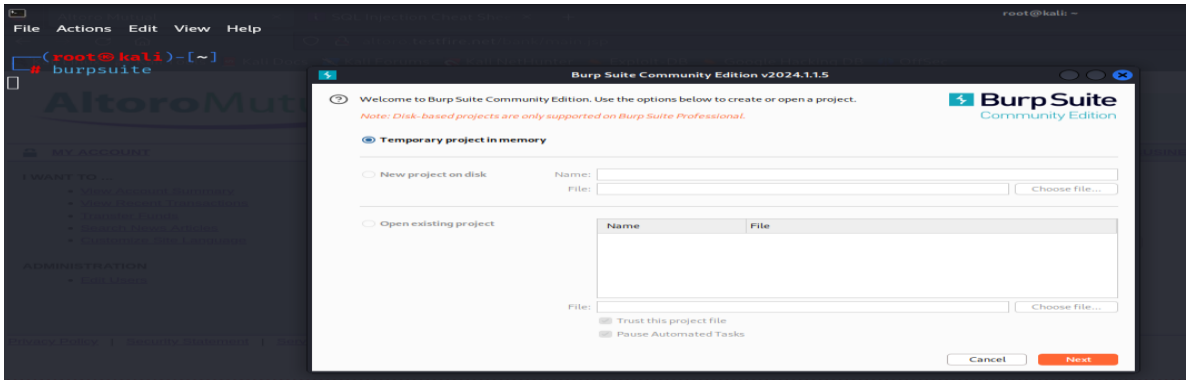


2.vi) So, we successfully bypassed the login screen and the target website is vulnerable to SQL Injection

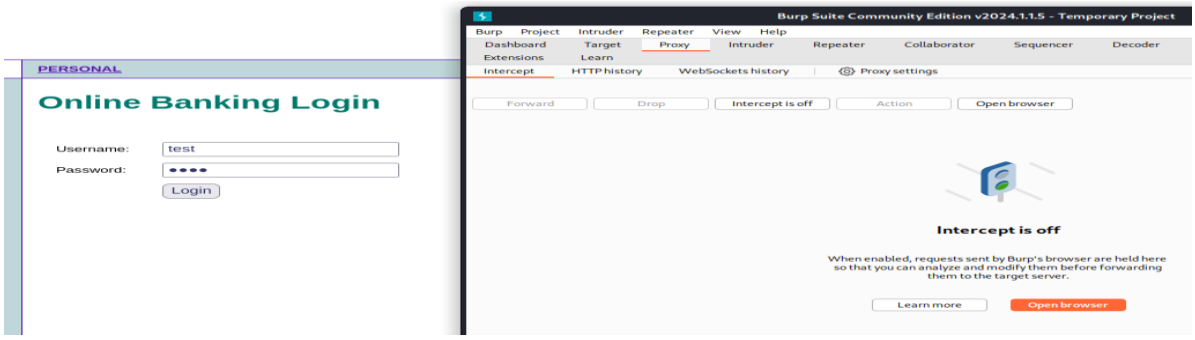


TASK 3: Brute Force Attack

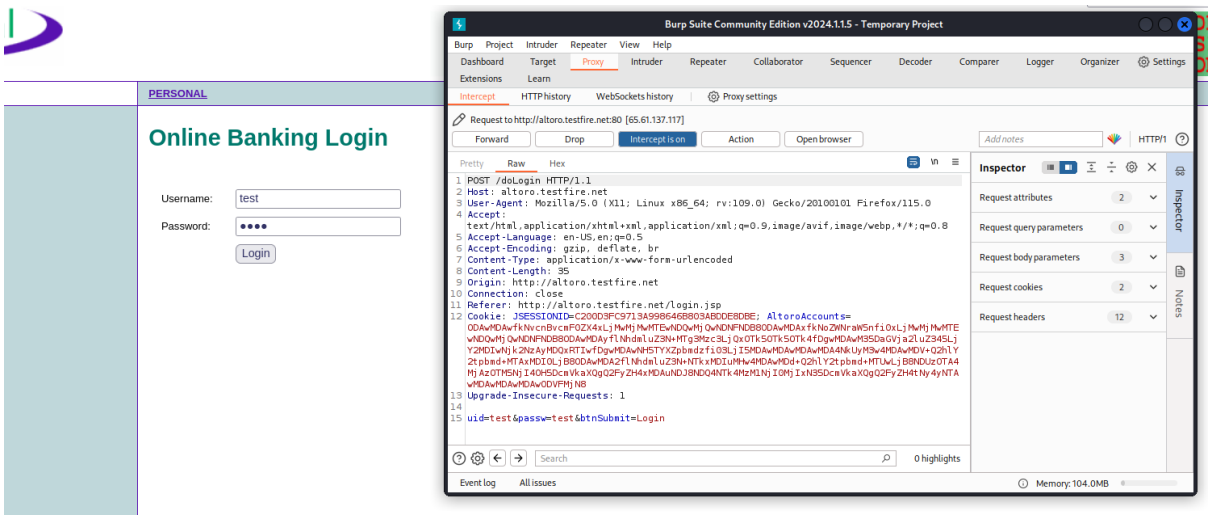
3.i) For the brute force attack, we are using Burpsuite community edition from Kali Linux platform



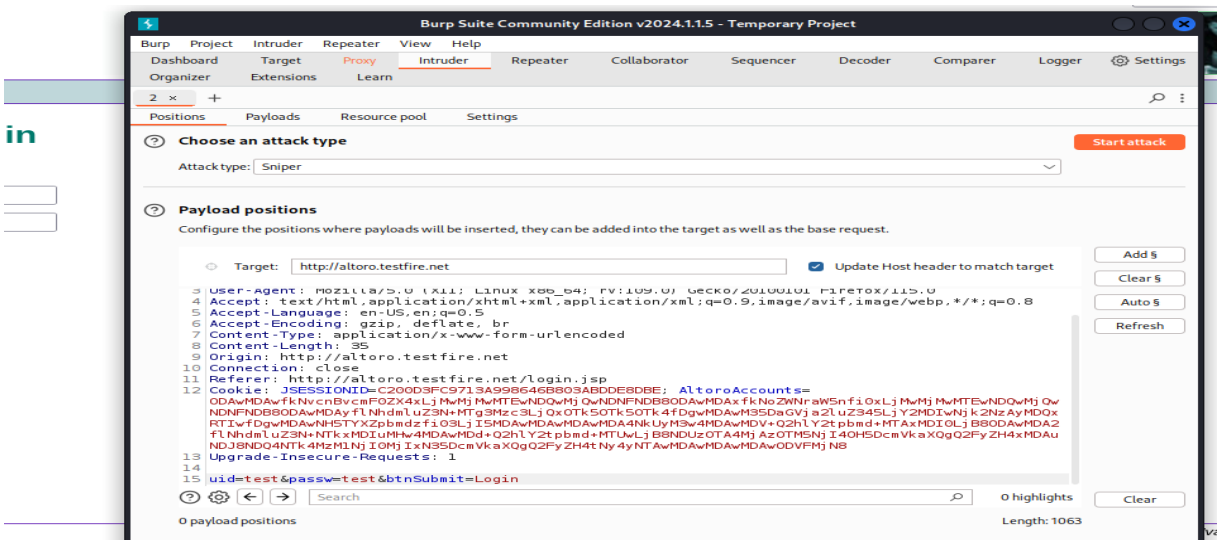
3.ii) We need to do a brute force attack in the login page, so we are using “test” as the login credentials



3.iii) Keeping the intercept on, we received the request in Burpsuite to brute force on the target page



3.iv) Once we received the response, send it to the Intruder for selecting the attack type



3.v) Selecting the attack type as “Cluster Bomb” as we need two payloads to do the brute force attack on the target

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organize

2 × +

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Cluster bomb

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://altoro.testfire.net

```
1  POST /doLogin HTTP/1.1
2  Host: altoro.testfire.net
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 35
9  Origin: http://altoro.testfire.net
10 Connection: close
11 Referer: http://altoro.testfire.net/login.jsp
12 Cookie: JSESSIONID=C200D3FC9713A998646B803ABDDE8DBE; AltoroAccounts=
   ODAwMDAwfkNvcnBvcmF0ZX4xLjMwMjMwMTEwNDQwMjQwNDNFNDB80DAwMDAxfkNoZWNraW5nfi0xLjMwMjMwMTEwNDQwMjQwNDNFNDB80DA
   DAwMDV+Q2hlY2tpbmd+MTAxMDI0LjB80DAwMDA2flNhdmluZ3N+NTkxMDIuMHw4MDAwMDd+Q2hlY2tpbmd+MTUwLjB8NDUzOTA4MjAzOTM5
13 Upgrade-Insecure-Requests: 1
14
15 uid=§test§&passw=§test§&btnSubmit=Login
```

3.vi) Now we are giving the 2 payloads set, 1st for username and 2nd for password

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer

2 × +

Positions Payloads Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available fo

Payload set: 1 Payload count: 4

Payload type: Simple list Request count: 0

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate
Add

```
test
12345
admin
admin123
```

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer E

2 × +

Positions Payloads Resource pool Settings

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each p

Payload set: 2 Payload count: 3

Payload type: Simple list Request count: 12

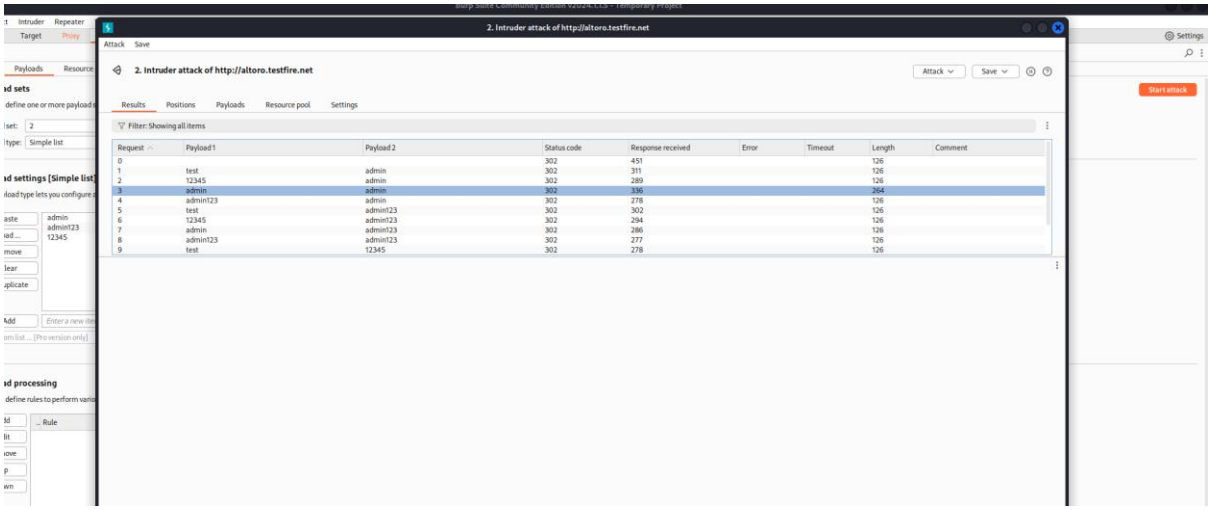
Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

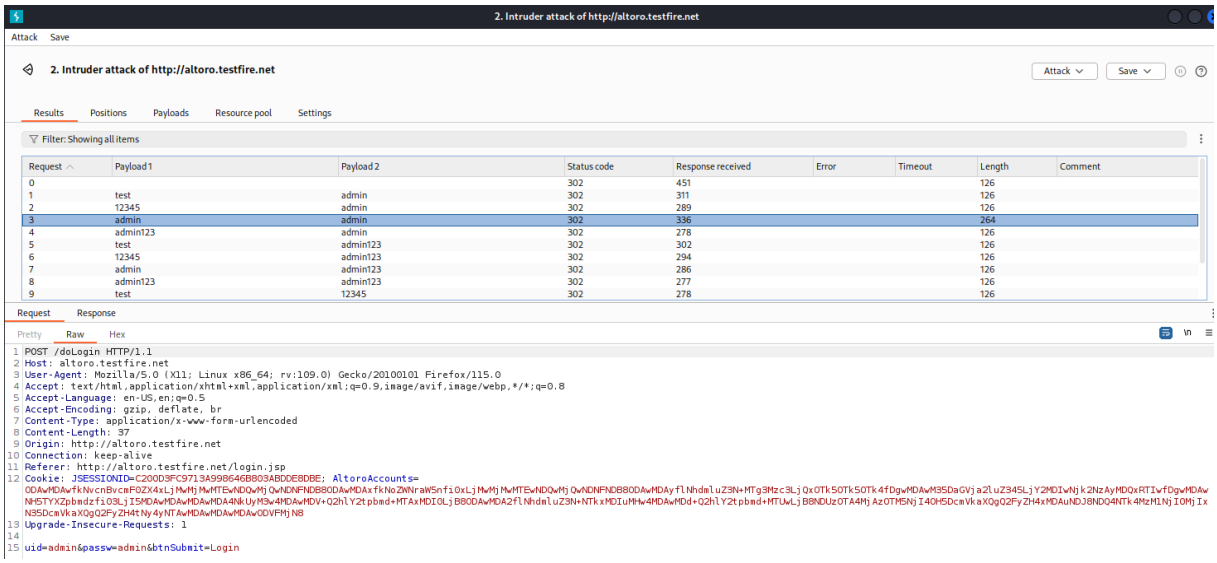
Paste
Load ...
Remove
Clear
Deduplicate
Add

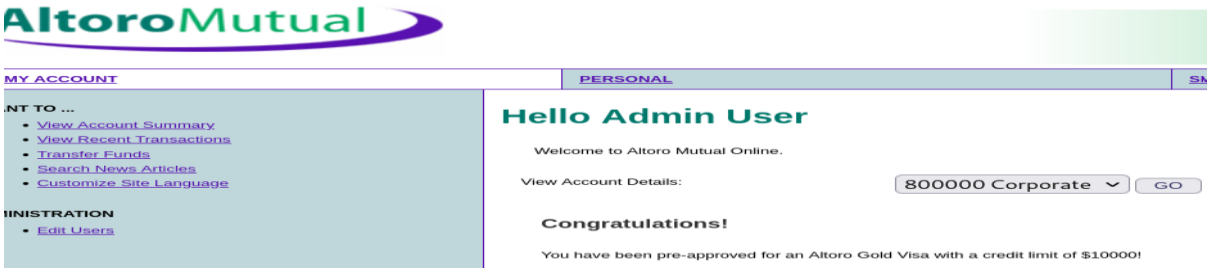
```
admin
admin123
12345
```

3.vii) Start the attack by clicking on the “start attack” button



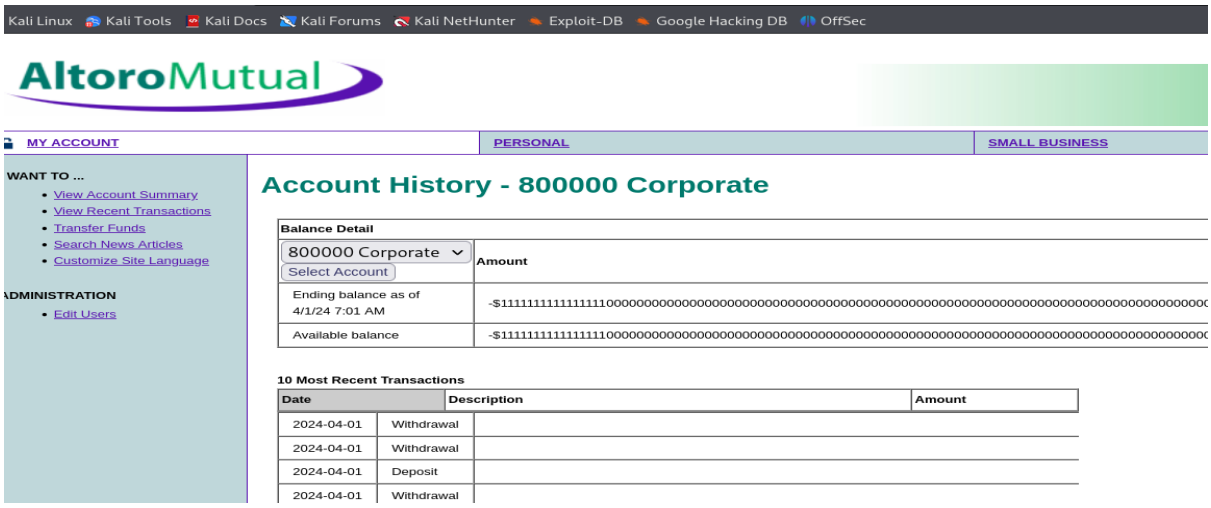
3.viii) We successfully did the brute force attack on the login page



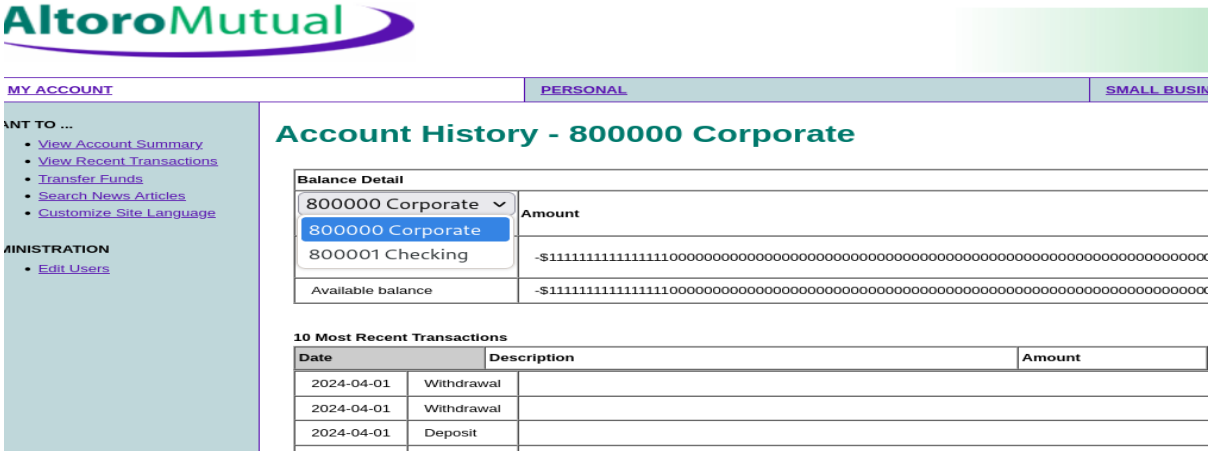


TASK 4: Access Control Vulnerability

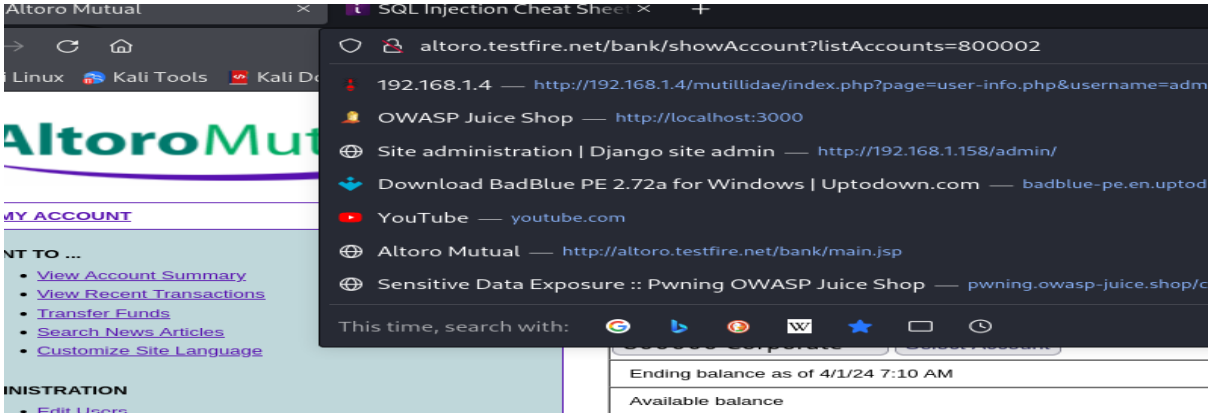
4.i) In My Account we can run some access control information



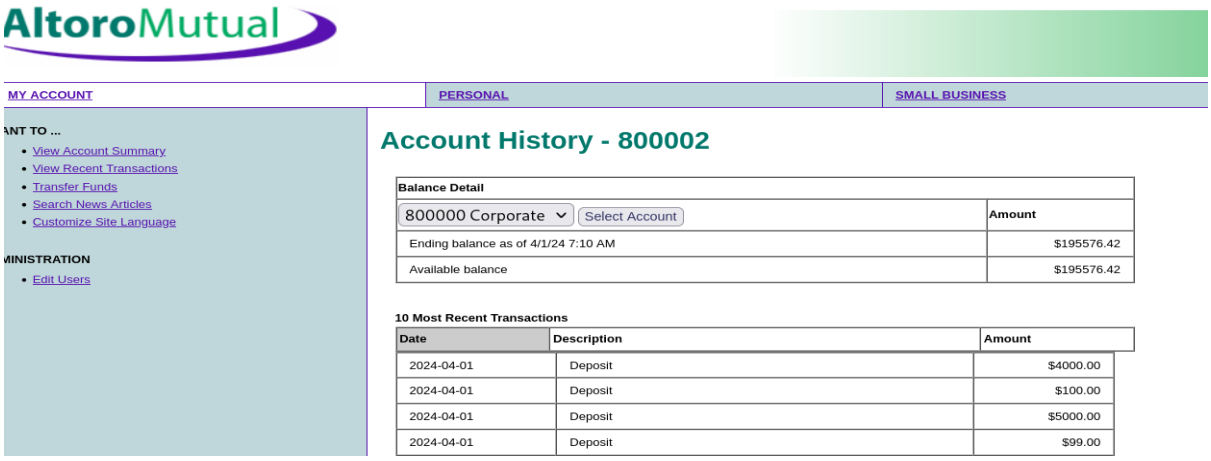
4.ii) Currently it only shows the information for “800000 and 800001” only

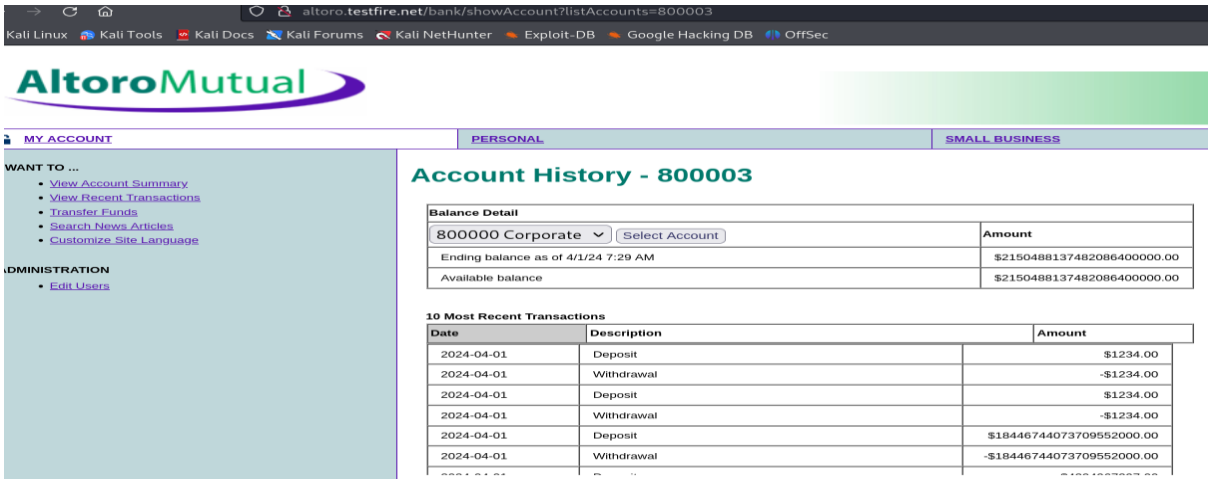


4.iii) We are checking for the information for “800002”



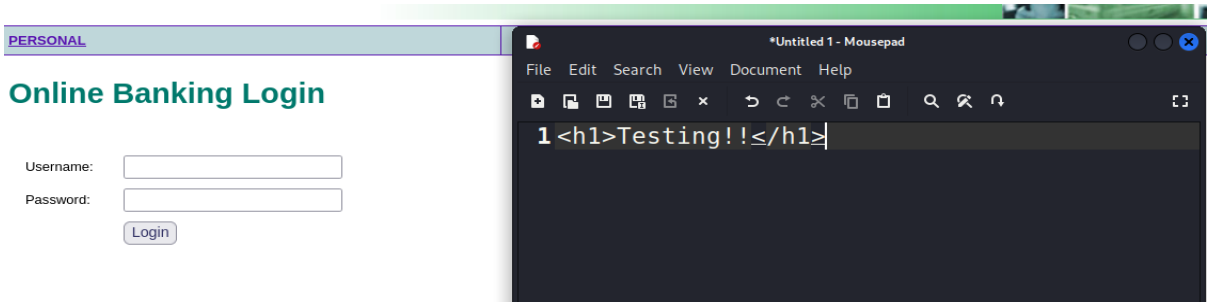
4.iv) Account History for 800002 and 800003 are not part of the account, but it is still showcasing to us. So, we can say that the application is prone to access control vulnerability



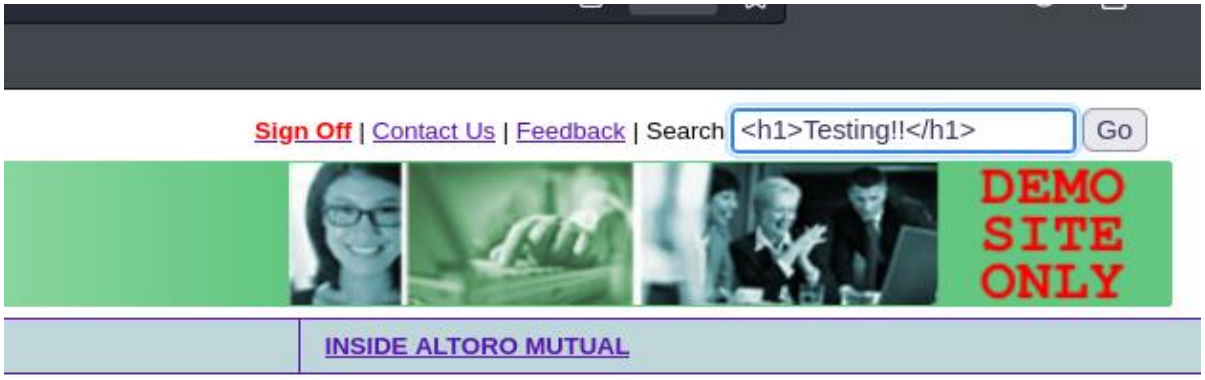


TASK 5: HTML Injection

5.i) Trying to do the HTML Injection on the target using HTML command



5.ii) Using the above HTML code in the search area to test



5.iii) So we inserted the information and the application responded which proves that it is vulnerable to HTML Injection