INSTITUTE FOR ADVANCED COMPUTING
AND
SOFTWARE DEVELOPMENT
AKURDI, PUNE

DOCUMENTATION ON

“Web Testing using VAPT”

PG-DITISS Mar-2023

SUBMITTED BY:

GROUP NO: 20

SANCHI DHABARDE (233442)

JANHAVI MORE (233419)

MR. KARTIK AWARI — **PROJECT GUIDE**

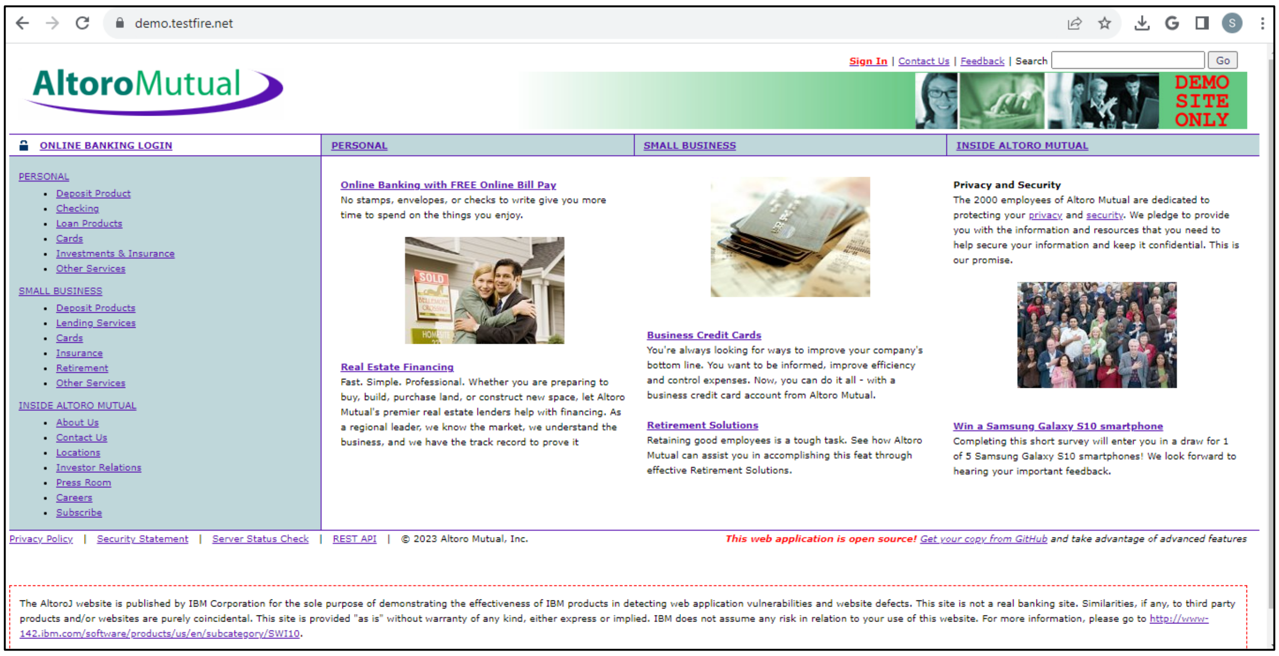
MR. ROHIT PURANIK — **CENTRE COORDINATOR**

TABLE OF CONTENTS

1. INTRODUCTION

This vulnerability assessment and penetration testing (VA/PT) activity was performed on http://demo.testfire.net/

Details	
In-Scope URL:	http://demo.testfire.net/
Testing Methodology	Black Box Testing
Application POC	



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

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

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

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

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

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

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.

Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ 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 "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

2. PROJECT OBJECTIVES

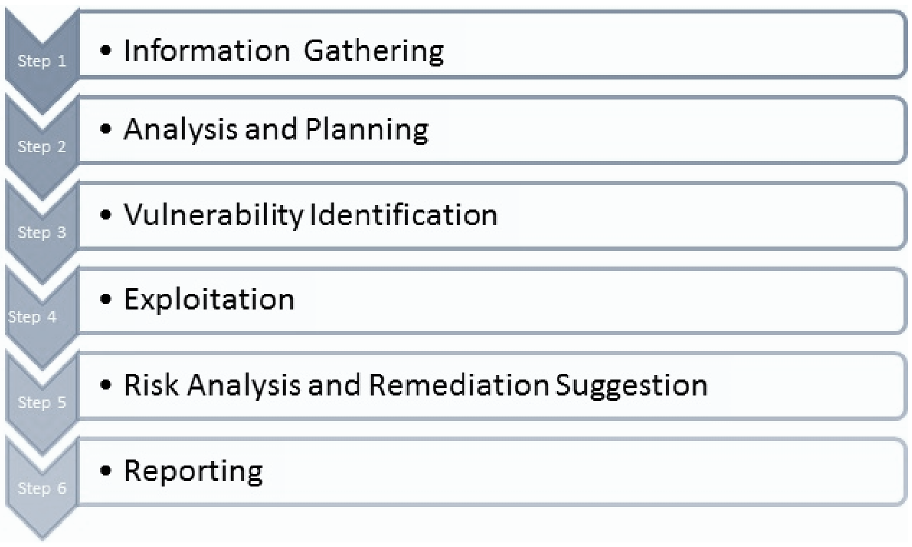
This Report summarizes the results of the Assessment carried out to analyze the risks to the AltoroMutual Web Application. Based on the agreed scope and objective of the engagement as per the request, the following activities were performed:

- Identification of the vulnerabilities related to AltoroMutual Web applications infrastructure.
- Assessing impact arising from any discovered vulnerabilities.
- Prioritization of the vulnerabilities depending upon the risk exposure and Development of recommendations to mitigate the vulnerabilities as SANS-25 and OWASP Top 10 Framework and CVE and CWE database.
- Providing recommendations to mitigate risks arising from the discovered vulnerabilities.

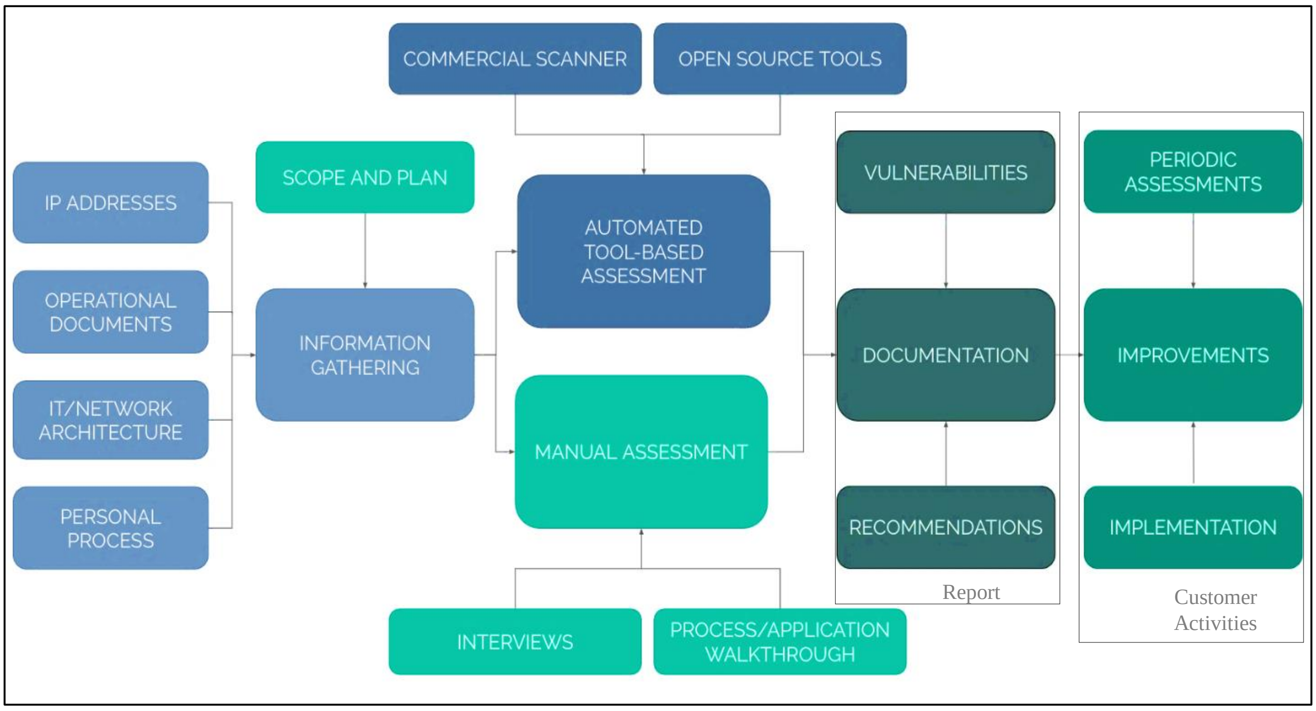
This report presents the results of the engagement and recommendations. For this exercise, we conducted Automated and Manual review, one to one assessment and used some set of tools.

3. APPROACH

We assumed that given hosts are externally hosted and the organization has implemented the security policies available with them and the systems were installed and updated with latest antivirus and antivirus definitions. All the system and software applications are updated or upgraded to latest security updates and patches as suggested by the respective OEM.



The workflow is represented below:



4. KEY OBSERVATION

Observed the following weaknesses in the application during the assessment:

- SQL Injection
- Reflected XSS
- Cleartext Submission of Username & Password
- Missing HTTP Headers
- Multiple Session Login
- Clickjacking
- Server Name Disclosed
- Secure Flag is not set
- HTTP method is enabled

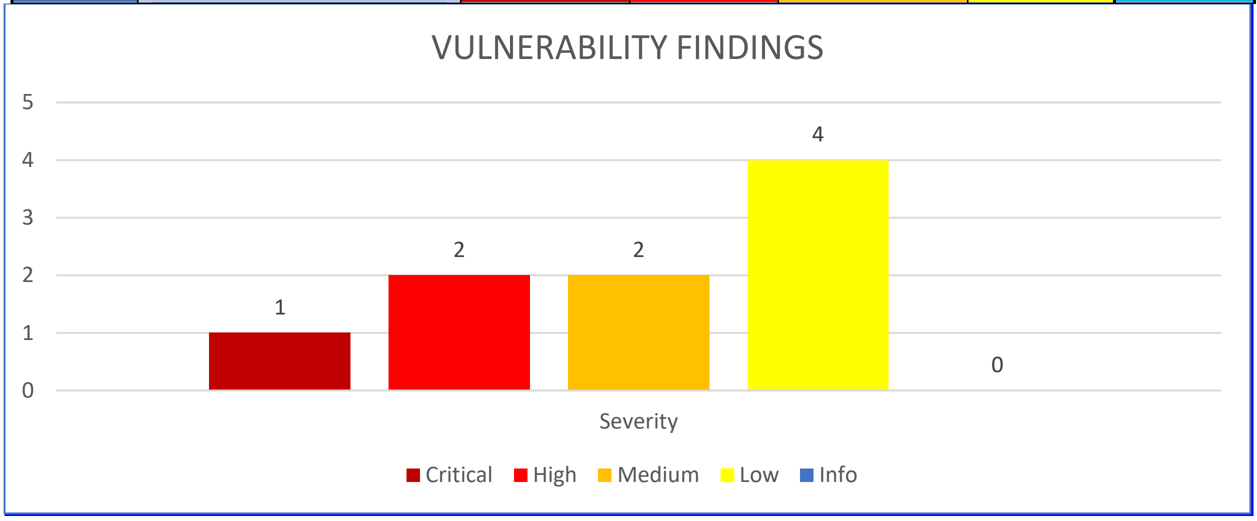
5. VULNERABILITY SEVERITY DEFINITIONS

Vulnerability Severity	Description
Critical	**The impacts of Critical severity vulnerabilities are as follows:** These vulnerabilities can allow attackers to take complete control of your Web applications and servers. In exploiting this type of vulnerability, attackers could carry out a range of malicious acts including (but not limited to): • Stealing information (for example, user data) • Tricking your users into supplying them with sensitive information (for example, credit card details) • Defacing your Web Application I. By exploiting a critical severity vulnerability, attackers can access your Web application's database. This allows them to acquire user and administrator information that might allow them to make changes such as delete or modify other user accounts. II. On exploiting such vulnerabilities, attackers can access and control logged-in user or administrator accounts, enabling them to hijack accounts and make changes that typically only those users can. **Suggested Action for Critical Severity Vulnerabilities:** A Critical severity vulnerability means that your Web Application can be hacked any time. You should make it your highest priority to fix these vulnerabilities immediately. Once you fix them, rescan the Web Application to make sure they have been eliminated.
High	**Impacts of High Severity Vulnerabilities**: 1. Attackers can find other vulnerabilities, and potentially your database passwords, by viewing your application's source code. 2. On exploiting such vulnerabilities, attackers can view information about your system that helps them find or exploit other vulnerabilities that enable them to take control of your Web Application and access sensitive user and administrator information. **Suggested Action for High Severity Vulnerabilities:** A High severity vulnerability means that your Web Application can be hacked and hackers can find other vulnerabilities which have a bigger impact. Fix these types of vulnerabilities immediately. Once you fix them, rescan your Web Application to make sure they have been eliminated
Medium	This level of vulnerability represents a moderate level of weakness in the current control environment and requires management action attention in the near term.
Low	This severity level provides for an opportunity to improve effectiveness and efficiency of the current control environment.
Informational	Serves as an informational purpose.

6. MANAGEMENT SUMMARY

6.1 Vulnerability Dashboard

S.NO	Findings Details	Critical	High	Medium	Low	Info
1	Web Application Findings	1	2	2	4	0



6.2 Vulnerability Analysis and Risk

Identified **1 Critical, 2 High, 2 Medium, 4 low & 0 Info** severity level vulnerabilities within the Application, https://demo.testfire.net/

S. No	Vulnerability Name	Severity	OWASP Top 10/SANS Top 25
1.	SQL Injection	Critical	Configuration Error
2.	Reflected XSS	High	Configuration Error
3.	Cleartext Submission of Username & Password	High	Deployment error
4.	Multiple Session Login	Medium	Configuration Error
5.	Missing HTTP Headers	Medium	Design error
6.	Clickjacking	Low	Configuration Error
7.	Server name disclosed	Low	Configuration Error
8.	Secure Flag is not set	Low	Configuration Error
9.	HTTP method is enabled	Low	Configuration Error

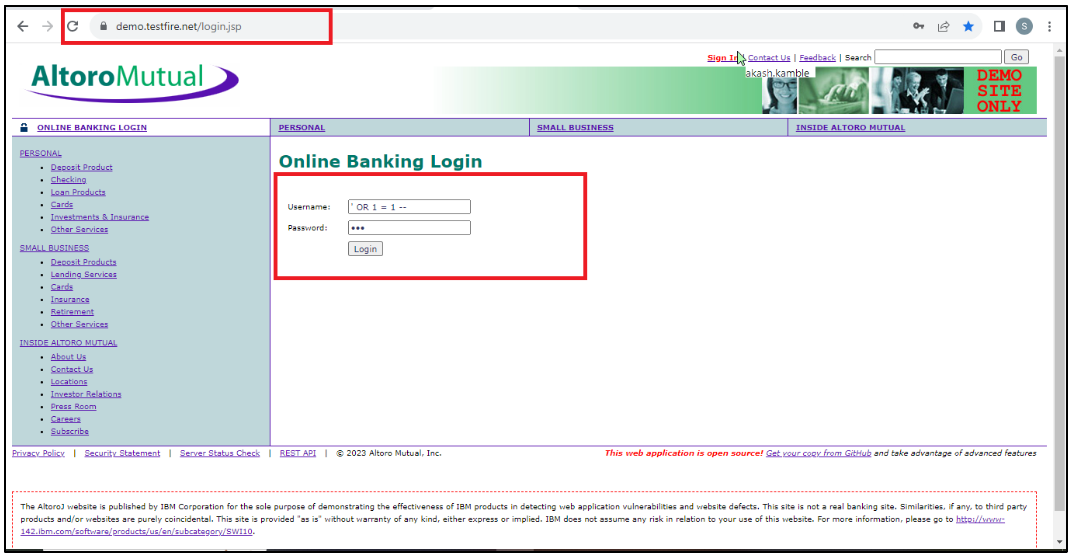
7. DETAILED VULNERABILITIES AND RECOMMENDATIONS

This section of the report provides detailed list of observed vulnerabilities with the following information:

- Vulnerability Name
- CVE/CWE ID
- Attributing Factor
- Severity Level
- Description
- Observation
- Proof of Concept (POC)
- Impact
- Recommendation
- References

8. OUTPUTS:

8.1 SQL Injection

Vulnerability Name	SQL Injection
CWE/CVE	CWE-89
Attributing Factor	Configuration Error
Severity Level	**Critical**
Description	SQL Injection is a type of cyberattack where an attacker injects malicious SQL code into an application's input fields. This code is then executed by the application's database, allowing the attacker to perform unauthorized actions on the database. These actions can include extracting, modifying, or deleting data, or even taking control of the entire database.
Observation	**Steps to reproduce the issue:** 1. Go to the browser (i.e., Chrome, Firefox) 2. Enter the URL - https://demo.testfire.net/ 3. Go to login page 4. Enter payload: ' OR 1 = 1 – in username and give any password 5. It is observed that the application is vulnerable to SQL Injection
Proof Of Concept (POC)	

demo.testfire.net/login.jsp

Online Banking Login

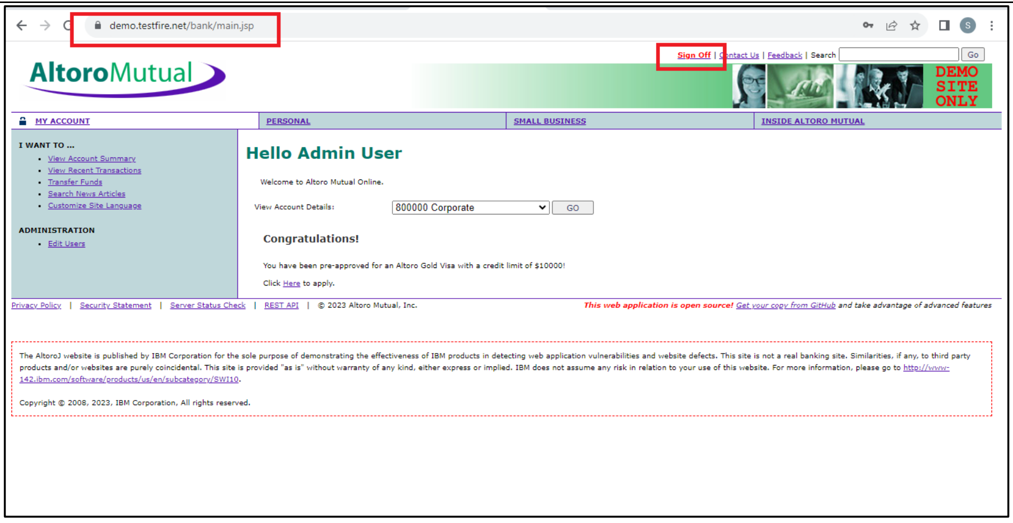
Username: ' OR 1 = 1 --

Password: •••

© 2023 Altoro Mutual, Inc.

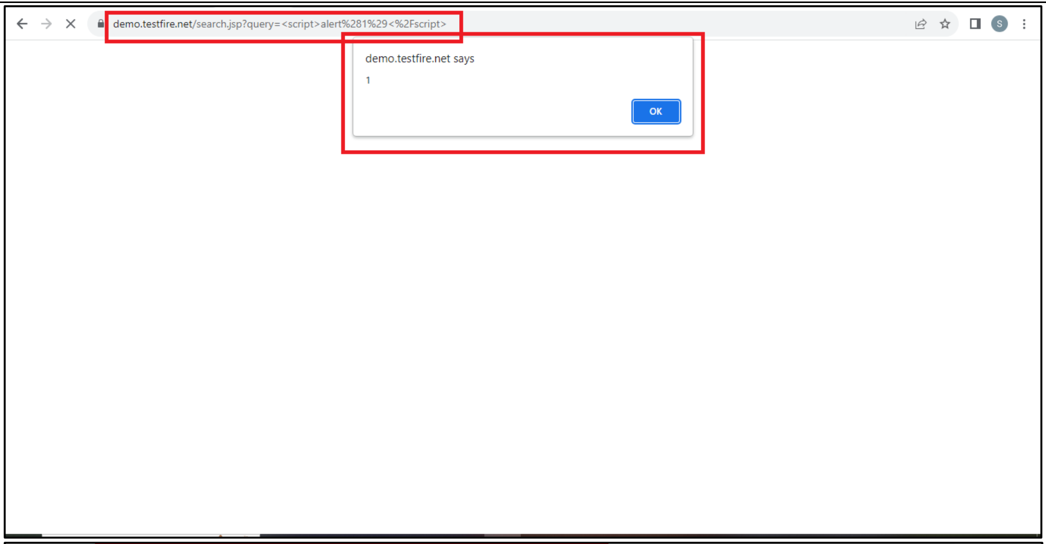
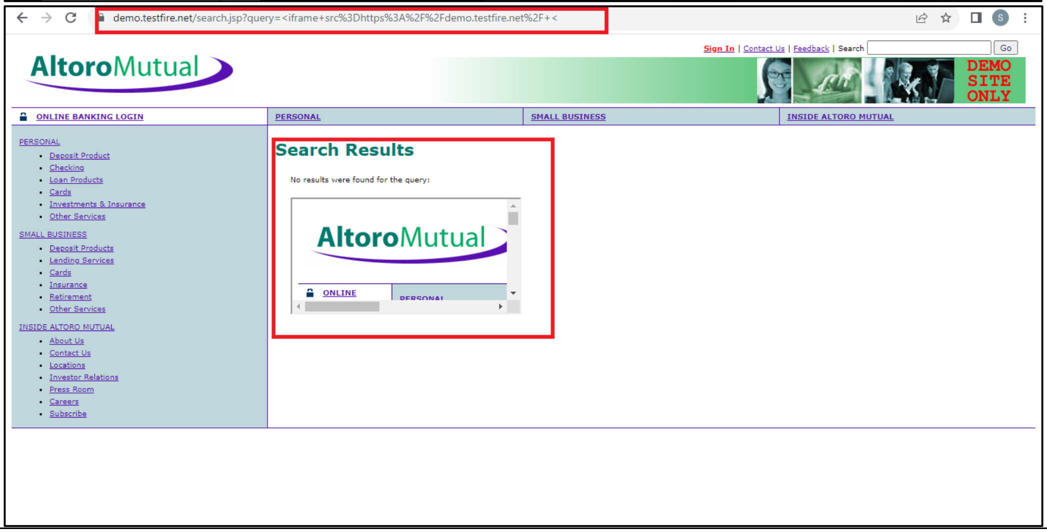
This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ 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 "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

	 demo.testfire.net/bank/main.jsp Sign Off | Contact Us | Feedback | Search Go AltoroMutual 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 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. Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc. *This web application is open source! Get your copy from GitHub and take advantage of advanced features* The AltoroJ 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 "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10. Copyright © 2008, 2023, IBM Corporation, All rights reserved.
Impact	The impact of SQL Injection can be severe. Depending on the vulnerability and the application's permissions on the database, an attacker can: • Retrieve sensitive data (such as usernames and passwords). • Modify or delete data. • Execute administrative commands on the database. • Take control of the entire system.
Recommendation	To prevent SQL Injection, developers should: • Use parameterized statements (prepared statements) in their code. • Validate and sanitize user inputs. • Apply the principle of least privilege, ensuring that the application's database user has minimal permissions.
Reference(s)	https://owasp.org/www-community/attacks/SQL_Injection

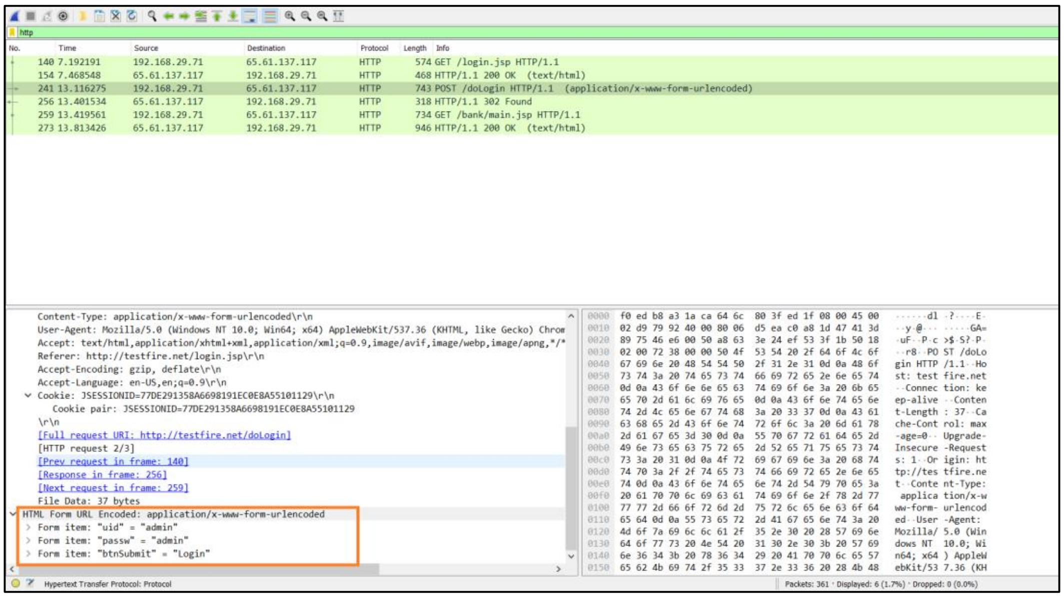
8.2Reflected XSS

Vulnerability Name	Reflected XSS
CWE/CVE	CWE-79
Attributing Factor	Configuration Error
Severity Level	🟥 **High**
Description	Reflected XSS is a type of web security vulnerability where an attacker injects malicious scripts into web pages viewed by other users. These scripts are then executed by the users' web browsers, allowing the attacker to steal information, impersonate users, or perform actions on behalf of users without their consent.

Observation	**Steps to reproduce the issue:** 1. Go to the browser (i.e., Chrome, Firefox) 2. Enter the URL - https://demo.testfire.net/ 3. Go to search bar 4. Enter payload: <script>alert(1)</script> or (Iframe Injection)- <iframe src=https://demo.testfire.net/ < 5. It display a pop-up 6. It is observed that the application is vulnerable to Reflected XSS
Proof Of Concept (POC)	 demo.testfire.net/search.jsp?query=<script>alert%281%29<%2Fscript> demo.testfire.net says 1 OK  demo.testfire.net/search.jsp?query=<iframe+src%3Dhttps%3A%2F%2Fdemo.testfire.net%2F+< Search Results No results were found for the query: AltoroMutual Sign In | Contact Us | Feedback | Search Go DEMO SITE ONLY ONLINE BANKING LOGIN PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL PERSONAL Deposit Product Checking Loan Products Cards Investments & Insurance Other Services SMALL BUSINESS Deposit Products Lending Services Cards Insurance Retirement Other Services INSIDE ALTORO MUTUAL About Us Contact Us Locations Investor Relations Press Room Careers Subscribe AltoroMutual ONLINE PERSONAL
Impact	The impact of XSS can be significant. Depending on the vulnerability and the attacker's goals, they can: Steal cookies or session tokens, allowing unauthorized access to user accounts. • Deface websites. • Redirect users to malicious websites. • Impersonate users and perform actions on their behalf. • Perform actions on a user's behalf without their consent.

Recommendation	To prevent Cross-Site Scripting, developers should: • Validate and sanitize user inputs. • Use security libraries and frameworks that offer built-in protection against XSS (e.g., Content Security Policy or CSP headers). • Educate users about the risks of XSS and encourage them to keep their browsers and plugins up to date.
Reference(s)	https://owasp.org/www-community/attacks/xss/

8.3 Cleartext submission of username and password

Vulnerability Name	Cleartext submission of username and password
CWE/CVE	CWE-319
Attributing Factor	Deployment error
Severity Level	🟥 **High**
Description	User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users
Observation	**Steps to reproduce the issue:** 1. Go to the Wireshark tool 2. Enter the URL - https://demo.testfire.net/ 3. Enter valid user credentials and Capture the HTTP traffic in Wireshark, the sensitive like username and password is disclosed.
Proof Of Concept (POC)	

```
http
No.   Time          Source          Destination     Protocol  Length  Info
140   7.192191      192.168.29.71   65.61.137.117   HTTP      574 GET /login.jsp HTTP/1.1
154   7.468548      65.61.137.117   192.168.29.71   HTTP      468 HTTP/1.1 200 OK  (text/html)
241   13.116275     192.168.29.71   65.61.137.117   HTTP      743 POST /doLogin HTTP/1.1  (application/x-www-form-urlencoded)
256   13.401534     65.61.137.117   192.168.29.71   HTTP      318 HTTP/1.1 302 Found
259   13.419561     192.168.29.71   65.61.137.117   HTTP      734 GET /bank/main.jsp HTTP/1.1
273   13.813426     65.61.137.117   192.168.29.71   HTTP      946 HTTP/1.1 200 OK  (text/html)
```

```
    Content-Type: application/x-www-form-urlencoded\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
    Referer: http://testfire.net/login.jsp\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  ˅ Cookie: JSESSIONID=77DE291358A6698191EC0E8A55101129\r\n
      Cookie pair: JSESSIONID=77DE291358A6698191EC0E8A55101129
    \r\n
    [Full request URI: http://testfire.net/doLogin]
    [HTTP request 2/3]
    [Prev request in frame: 140]
    [Response in frame: 256]
    [Next request in frame: 259]
    File Data: 37 bytes
˅ HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "uid" = "admin"
  > Form item: "passw" = "admin"
  > Form item: "btnSubmit" = "Login"
```

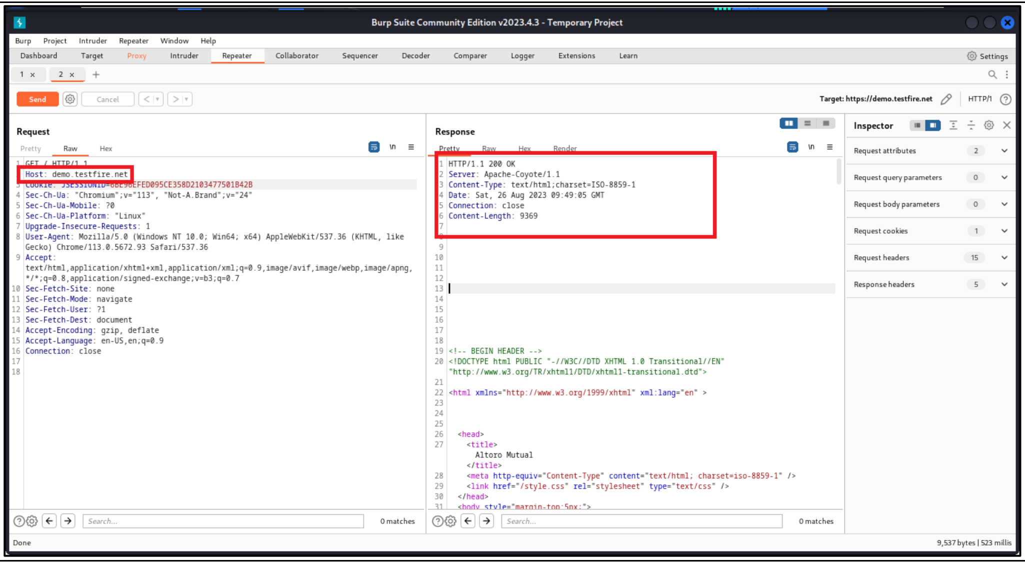
```
0000  f0 ed b8 a3 1a ca 64 6c  80 3f ed 1f 08 00 45 00   ······dl ·?····E·
0010  02 d9 79 92 40 00 80 06  d5 ea c0 a8 1d 47 41 3d   ··y·@··· ·····GA=
0020  89 75 46 e6 00 50 a8 63  3e 24 ef 53 3f 1b 50 18   ·uF··P·c >$·S?·P·
0030  02 00 72 38 00 00 50 4f  53 54 20 2f 64 6f 4c 6f   ··r8··PO ST /doLo
0040  67 69 6e 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   gin HTTP /1.1··Ho
0050  73 74 3a 20 74 65 73 74  66 69 72 65 2e 6e 65 74   st: test fire.net
0060  0d 0a 43 6f 6e 6e 65 63  74 69 6f 6e 3a 20 6b 65   ··Connec tion: ke
0070  65 70 2d 61 6c 69 76 65  0d 0a 43 6f 6e 74 65 6e   ep-alive ··Conten
0080  74 2d 4c 65 6e 67 74 68  3a 20 33 37 0d 0a 43 61   t-Length : 37··Ca
0090  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20 6d 61 78   che-Cont rol: max
00a0  2d 61 67 65 3d 30 0d 0a  55 70 67 72 61 64 65 2d   -age=0·· Upgrade-
00b0  49 6e 73 65 63 75 72 65  2d 52 65 71 75 65 73 74   Insecure -Request
00c0  73 3a 20 31 0d 0a 4f 72  69 67 69 6e 3a 20 68 74   s: 1··Or igin: ht
00d0  74 70 3a 2f 2f 74 65 73  74 66 69 72 65 2e 6e 65   tp://tes tfire.ne
00e0  74 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   t··Conte nt-Type:
00f0  20 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 2d 77    applica tion/x-w
0100  77 77 2d 66 6f 72 6d 2d  75 72 6c 65 6e 63 6f 64   ww-form- urlencod
0110  65 64 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   ed··User -Agent: 
0120  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 57 69 6e   Mozilla/ 5.0 (Win
0130  64 6f 77 73 20 4e 54 20  31 30 2e 30 3b 20 57 69   dows NT  10.0; Wi
0140  6e 36 34 3b 20 78 36 34  29 20 41 70 70 6c 65 57   n64; x64 ) AppleW
0150  65 62 4b 69 74 2f 35 33  37 2e 33 36 20 28 4b 48   ebKit/53 7.36 (KH
```

```
Hypertext Transfer Protocol: Protocol          Packets: 361 · Displayed: 6 (1.7%) · Dropped: 0 (0.0%)
```

Impact	A third party will be able to read the user credentials by intercepting an unencrypted HTTP connection.

Recommendation	• Applications should use transport-level encryption (SSL or TLS) to protect all sensitive communications passing between the client and the server. • Communications should be protected include the login mechanism and related functionality, and any functions where sensitive data can be accessed or privileged actions can be performed.
Reference(s)	https://www.cvedetails.com/cwe-details/319/Cleartext-Transmission-of-Sensitive-Information.html

8.4 Missing HTTP Headers

Vulnerability Name	Missing HTTP Headers
CWE/CVE	CWE-644
Attributing Factor	Configuration Error
Severity Level	**Medium**
Description	HTTP security headers are a subset of HTTP headers that are related specifically to security. They are exchanged between a client (usually a web browser) and a server to specify the security details of HTTP communication. There are also other HTTP headers that, although not directly related to privacy and security, can also be considered HTTP security headers.
Observation	**Steps to reproduce the issue:** 1. Go to the browser (i.e., Chrome, Firefox) 2. Enter the URL - https://demo.testfire.net/ 3. Intercept the request in the burp suite and send it to the repeater. 4. In Response it is observed that standard necessary headers are not set.
Proof Of Concept (POC)	

Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Send
Cancel
Target: https://demo.testfire.net
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 15
Response headers 5
0 matches
Done
9,537 bytes | 523 millis

```
GET / HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=6BE96EFED095CE358D2103477501B42B
Sec-Ch-Ua: "Chromium";v="113", "Not-A.Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/113.0.5672.93 Safari/537.36
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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

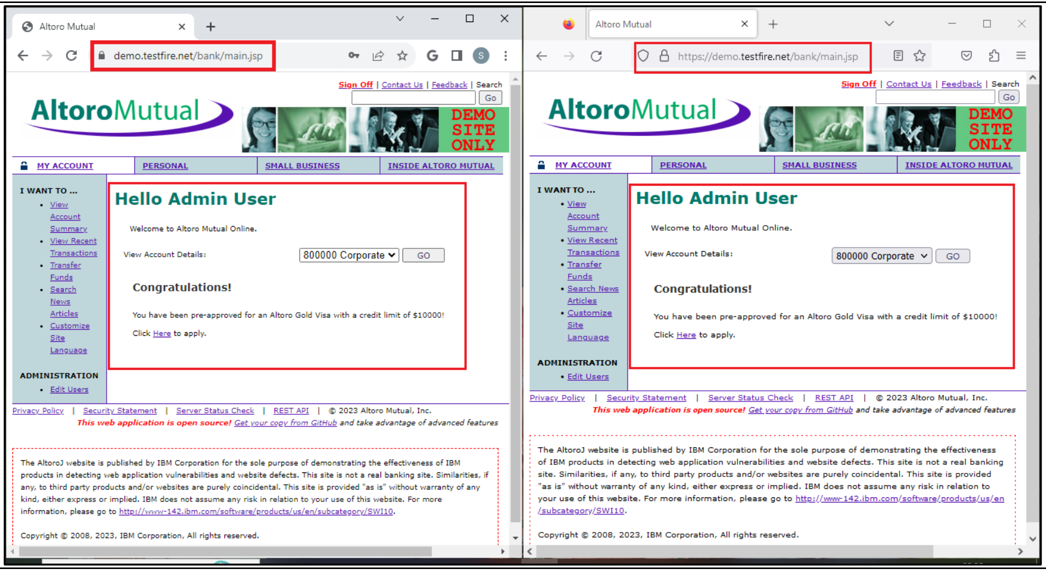
```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Sat, 26 Aug 2023 09:49:05 GMT
Connection: close
Content-Length: 9369







<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



  <head>
    <title>
      Altoro Mutual
    </title>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <link href="/style.css" rel="stylesheet" type="text/css" />
  </head>
  <body style="margin-top:5px;">
```

Impact	An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for

	attacks against its users when HSTS header is missing. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. The server did not return an X-Frame-Options header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack.
Recommendation	Implement below HTTP security headers on the webserver for the overall application: **HTTP Strict Transport Security (HSTS)** Strict-Transport-Security: max-age=31536000; include Subdomains **X-XSS-Protection** X-XSS-Protection: 1; mode=block **Content-Security-Policy (CSP)** Content-Security-Policy: script-src 'self' **X-Frame-Options** X-Frame-Options: deny (and other as per business requirement) **X-Content-Type-Options** X-Content-Type-Options: no sniff **Cache-Control**
Reference(s)	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

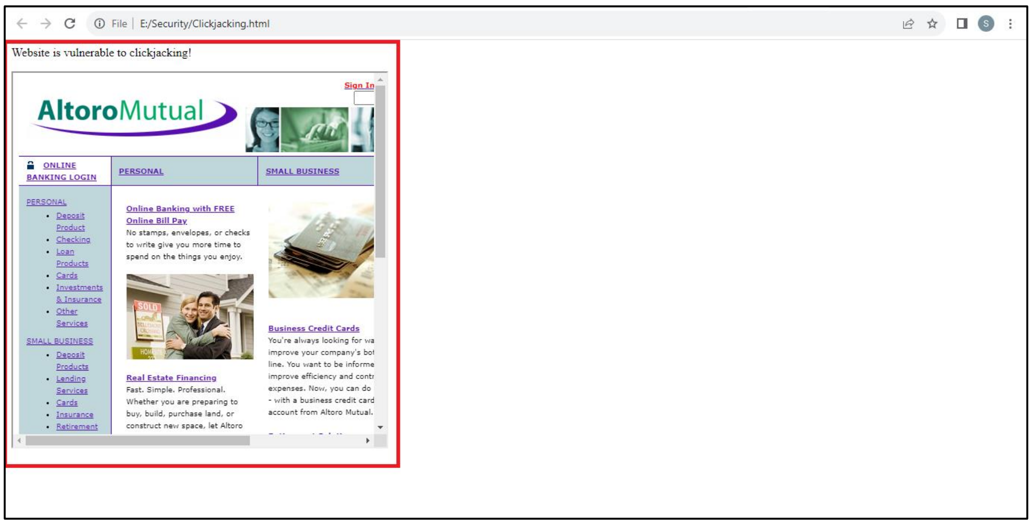
8.5Multiple Session Login

Vulnerability Name	Multiple Session Login
CWE/CVE	CWE-1018
Attributing Factor	Design error
Severity Level	**Medium**
Description	Weaknesses in this category are related to the design and architecture of session management. Frequently these deal with the information or status about each user and their access rights for the duration of multiple requests. The weaknesses in this category could lead to a degradation of the quality of session management if they are not addressed when designing or implementing a secure architecture
Observation	**Steps to reproduce the issue:** 1. Go to the browser (i.e., Chrome, Firefox) 2. Enter the URL - https://demo.testfire.net/ 3. Login one user in chrome. 4. Login same user in different browser like Firefox.

Proof Of Concept (POC)	 demo.testfire.net/bank/main.jsp Sign Off | Contact Us | Feedback | Search Go AltoroMutual 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 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. Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc. This web application is open source! Get your copy from GitHub and take advantage of advanced features The AltoroJ 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 "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10. Copyright © 2008, 2023, IBM Corporation, All rights reserved. https://demo.testfire.net/bank/main.jsp
Impact	Session was not logout after creating new session for same user, it leads to account take over.
Recommendation	Solution 1- Session id should be changed after logging or it should be changed while accessing critical page of the application. Solution 2- You may also specify a limit for concurrent users. A user who enters a URL to one of this realm's sign-in pages must meet any access management and concurrent user requirements specified for the authentication policy before the system presents the sign-in page to the user.
Reference(s)	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

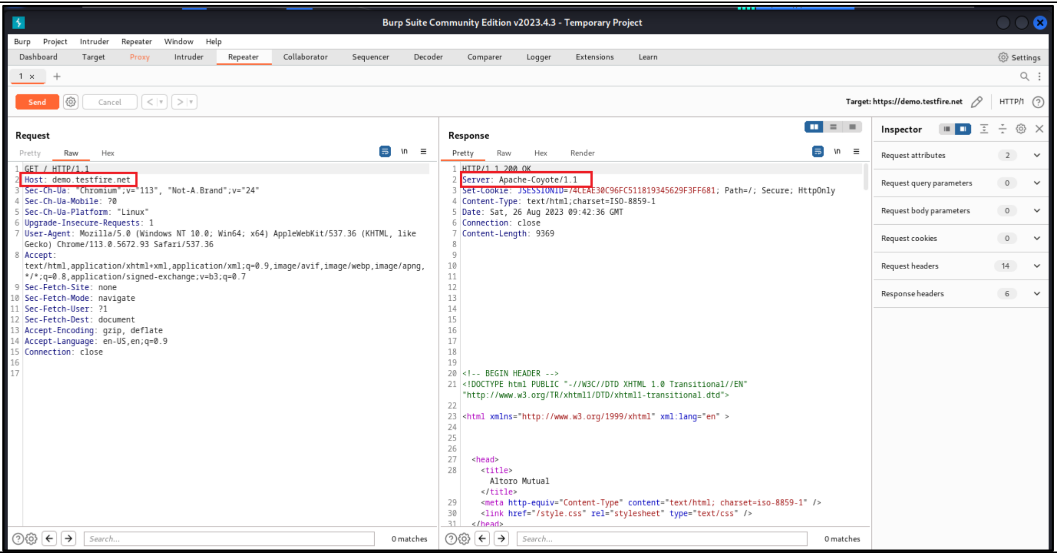
8.6 Clickjacking

Vulnerability Name	Clickjacking
CWE/CVE	CWE-1021
Attributing Factor	Configuration Error
Severity Level	**Low**
Description	Clickjacking is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages.
Observation	**Steps to reproduce the issue:** 1. Go to the browser (i.e., Chrome, Firefox) 2. In clickjacking payload, insert the website URL and test it in browser 3. It is observed that the application is vulnerable to clickjacking autoClickjacking.html

Proof Of Concept (POC)	 File | E:/Security/Clickjacking.html Website is vulnerable to clickjacking! Sign In ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS PERSONAL • Deposit Product • Checking • Loan Products • Cards • Investments & Insurance • Other Services SMALL BUSINESS • Deposit Products • Lending Services • Cards • Insurance • Retirement Online Banking with FREE Online Bill Pay No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy. Real Estate Financing Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Business Credit Cards You're always looking for wa improve your company's bot line. You want to be informe improve efficiency and contr expenses. Now, you can do - with a business credit card account from Altoro Mutual.
Impact	The hacker has several ways they can use the redirected clicks for their own gain. A common form of clickjacking involves mirroring a login and password form on a website. The user assumes that they're entering their information into a usual form but they're actually entering it in fields the hacker has overlaid on the UI. Hackers will target passwords or any other valuable data they can exploit.
Recommendation	To implement this protection, you need to add the X-Frame-Options HTTP Response header to any page that you want to protect from being clickjacked. One way to do this is to add the HTTP Response Header manually to every page. A possibly simpler way is to implement a filter that automatically adds the header to every page or to add it at the Web Application Firewall of Web/Application Server level.
Reference(s)	https://owasp.org/www-community/attacks/Clickjacking

8.7 Server name disclosed

Vulnerability Name	Server name disclosed
CWE/CVE	CWE-205
Attributing Factor	Configuration Error
Severity Level	**Low**
Description	Server name and version disclosure occur when a web server or application server inadvertently reveals information about its identity and version in the HTTP response headers or error messages sent to clients. This information can include details like the server software's name (e.g., Apache, Nginx, Microsoft IIS) and the specific version number.

Observation	**Steps to reproduce the issue:** 1. Go to the browser (i.e., Chrome, Firefox) 2. Enter the URL - https://demo.testfire.net/ 3. Intercept the request in the burp suite and send it to the repeater. 4. In Response it is observed that the server name and version is being disclosed.
Proof Of Concept (POC)	

Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Send
Cancel
Target: https://demo.testfire.net
HTTP/1
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 14
Response headers 6
Search...
0 matches

Request

```
GET / HTTP/1.1
Host: demo.testfire.net
Sec-Ch-Ua: "Chromium";v="113", "Not-A.Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/113.0.5672.93 Safari/537.36
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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

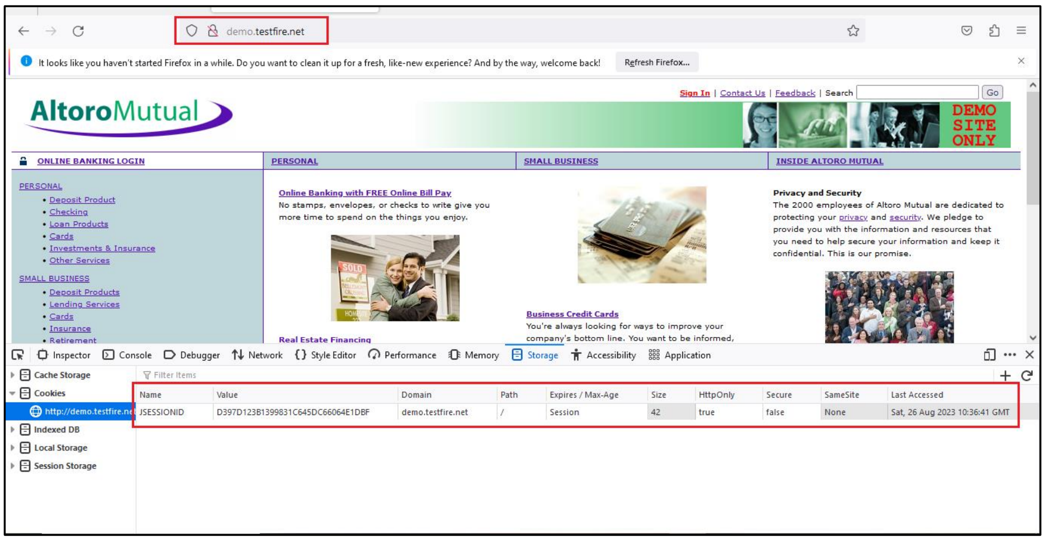
Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=74CEAE30C96FC511819345629F3FF681; Path=/; Secure; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Date: Sat, 26 Aug 2023 09:42:36 GMT
Connection: close
Content-Length: 9369











<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >



  <head>
    <title>
      Altoro Mutual
    </title>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
    <link href="/style.css" rel="stylesheet" type="text/css" />
  </head>
```

Impact	While server name and version disclosure, by itself, doesn't pose a direct threat, it can have the following indirect impacts: • **Information leakage:** Attackers can use this information as part of their reconnaissance efforts to identify potential vulnerabilities or misconfigurations associated with a specific server version. • **Increased attack surface:** It can contribute to targeted attacks, as attackers may tailor their exploits based on known vulnerabilities in a particular server version.
Recommendation	To mitigate server name and version disclosure: • **Disable or modify server headers:** Configure your web server to suppress or modify the "Server" header in its responses to provide minimal information about the server. • **Custom error pages:** Customize error pages to provide minimal information and avoid disclosing server details. • **Regular updates:** Keep your server software up to date with security patches to address any known vulnerabilities.
Reference(s)	https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server

8.8 Secure Flag is not set

Vulnerability Name	Secure Flag is not set

CWE/CVE	CWE-614, CWE-1004
Attributing Factor	Configuration Error
Severity Level	**Low**
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site
Observation	**Steps to reproduce the issue:** 1. Open a browser (i.e., Firefox, Chrome) 2. Enter the URL – http://demo.testfire.net/ 3. Login with default credentials and go to inspect element. 4. It is observed that HTTP Only and Secure flag are not set.
Proof Of Concept (POC)	
Impact	Failing to set the "Secure Flag" for cookies can have various impacts, including: • Session hijacking: Attackers can intercept session cookies and impersonate legitimate users. • Data exposure: Sensitive information stored in cookies, such as user credentials or authentication tokens, can be exposed. • Reduced confidentiality and integrity: Without encryption over HTTPS, data transmitted via cookies can be tampered with or eavesdropped on. • An attacker can intercept the traffic and hijack a victim's session by stealing the cookie. The attacker can carry out a man-in-the-middle attack and can force the victim to make an HTTP request to steal the cookie.

demo.testfire.net

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
JSESSIONID	D397D123B1399831C645DC66064E1DBF	demo.testfire.net	/	Session	42	true	false	None	Sat, 26 Aug 2023 10:36:41 GMT

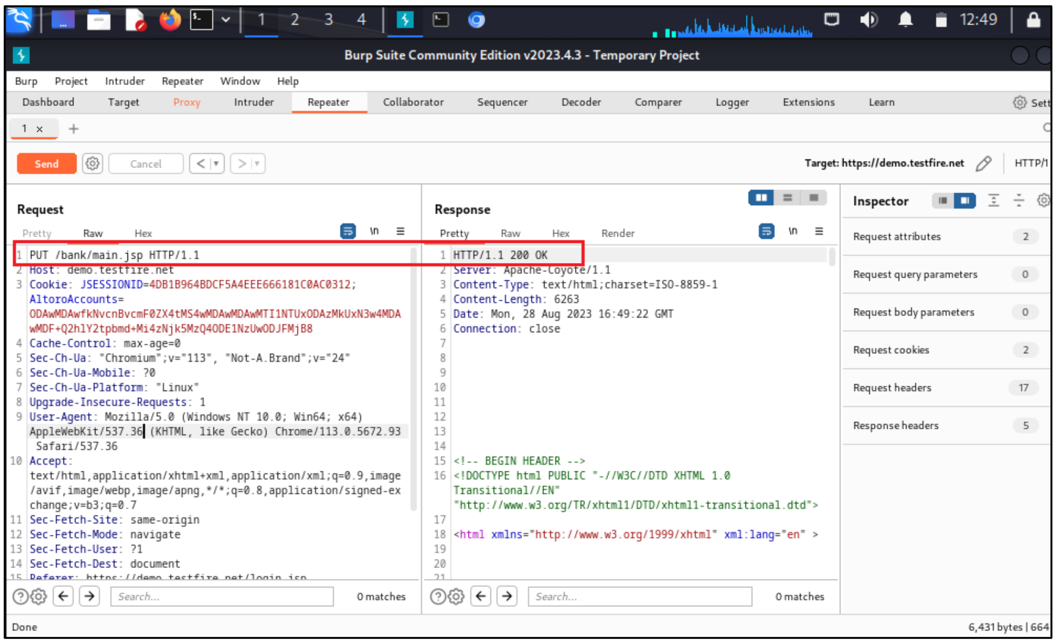
Recommendation	Set the Secure flag as true.
Reference(s)	https://owasp.org/www-community/HttpOnly

8.9 HTTP Method is Enabled

Vulnerability Name	HTTP Method is Enabled
CWE/CVE	CWE-319
Attributing Factor	Configuration Error
Severity Level	**Low**
Description	**PUT:** HTTP method used for updating or replacing a resource on the server. **DELETE:** HTTP method used to request the removal of a resource on the server. **OPTIONS:** HTTP method used to request information about the communication options available for a resource. **CONNECT:** HTTP method used to establish a network connection to a resource. **HEAD:** HTTP method used to request headers and metadata about a resource, without the actual content. **DEBUG:** Not a standard HTTP method; often used for debugging purposes in some development environments. **PATCH:** HTTP method used for applying partial modifications to a resource on the server.
Observation	**Steps to reproduce the issue:** 1. Go to the browser (i.e., Chrome, Firefox) 2. Enter the URL: https://demo.testfire.net/ 3. Capture the request in the Proxy tool. 4. Send the request to Repeater and change the HTTP method to OPTIONS and TRACE. 5. In response it shows PUT, DELETE, OPTIONS, CONNECT, HEAD, DEBUG & PATCH methods is enabled.

Proof Of Concept (POC)

PUT:



Burp Suite Community Edition v2023.4.3 - Temporary Project

Target: https://demo.testfire.net

Request

```
PUT /bank/main.jsp HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=4DB1B964BDCF5A4EEE666181C0AC0312;
AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tMS4wMDAwMDAwMTI1NTUxODAzMkUxN3w4MDA
wMDF+Q2hlY2tpbmd+Mi4zNjk5MzQ4ODE1NzUwODJFMjB8
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="113", "Not-A.Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
```

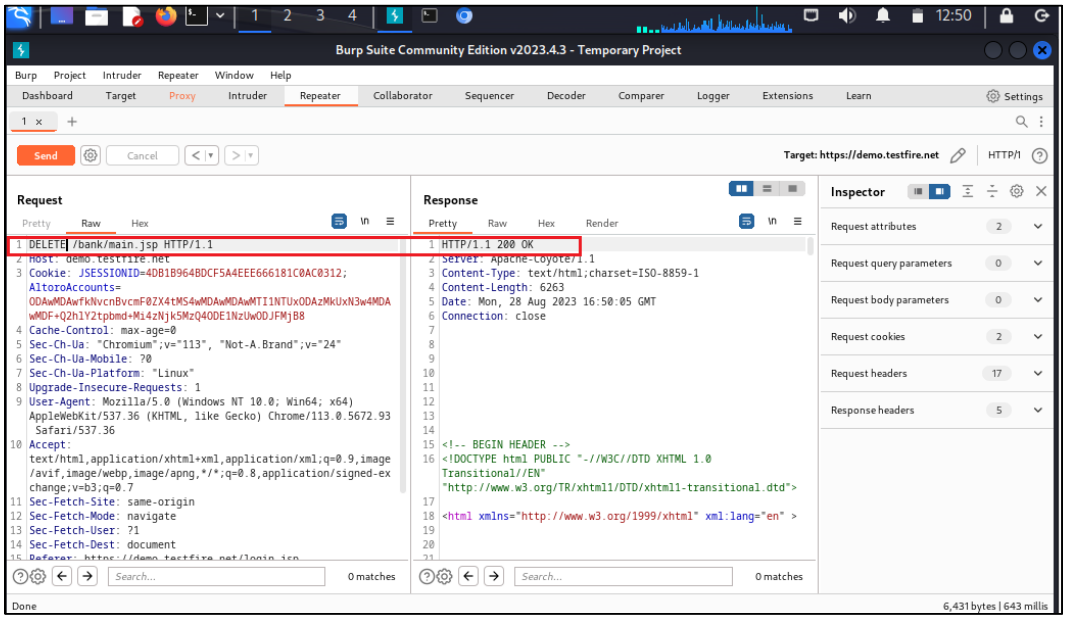
Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6263
Date: Mon, 28 Aug 2023 16:49:22 GMT
Connection: close








<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	2
Request headers	17
Response headers	5

Done 6,431 bytes | 664

DELETE:



Burp Suite Community Edition v2023.4.3 - Temporary Project

Target: https://demo.testfire.net

Request

```
DELETE /bank/main.jsp HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=4DB1B964BDCF5A4EEE666181C0AC0312;
AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tMS4wMDAwMDAwMTI1NTUxODAzMkUxN3w4MDA
wMDF+Q2hlY2tpbmd+Mi4zNjk5MzQ4ODE1NzUwODJFMjB8
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="113", "Not-A.Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
```

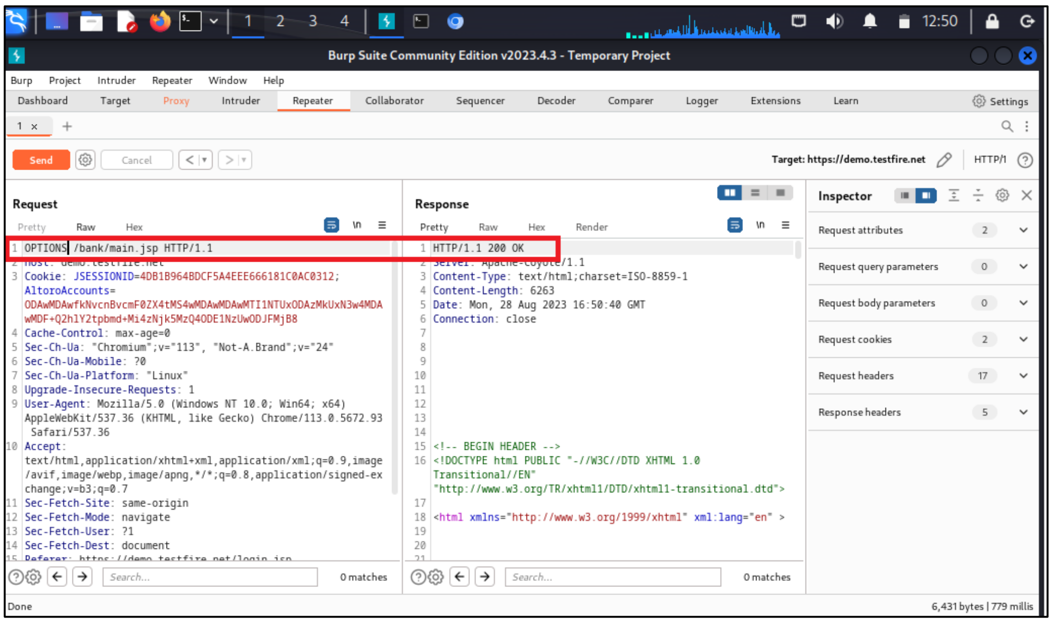
Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6263
Date: Mon, 28 Aug 2023 16:50:05 GMT
Connection: close








<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	2
Request headers	17
Response headers	5

Done 6,431 bytes | 643 millis

OPTIONS:



Burp Suite Community Edition v2023.4.3 - Temporary Project

Target: https://demo.testfire.net

Request

```
OPTIONS /bank/main.jsp HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=4DB1B964BDCF5A4EEE666181C0AC0312;
AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tMS4wMDAwMDAwMTI1NTUxODAzMkUxN3w4MDA
wMDF+Q2hlY2tpbmd+Mi4zNjk5MzQ4ODE1NzUwODJFMjB8
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="113", "Not-A.Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;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/login.jsp
```

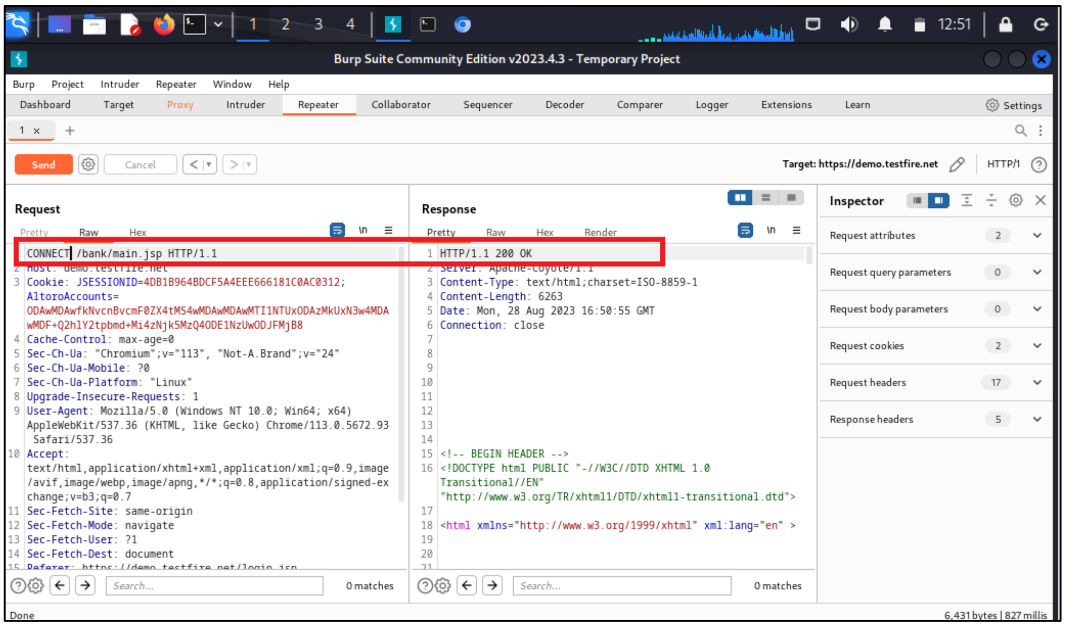
Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6263
Date: Mon, 28 Aug 2023 16:50:40 GMT
Connection: close








<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	2
Request headers	17
Response headers	5

Done 6,431 bytes | 779 millis

CONNECT:



Burp Suite Community Edition v2023.4.3 - Temporary Project

Target: https://demo.testfire.net

Request

```
CONNECT /bank/main.jsp HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=4DB1B964BDCF5A4EEE666181C0AC0312;
AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tMS4wMDAwMDAwMTI1NTUxODAzMkUxN3w4MDA
wMDF+Q2hlY2tpbmd+Mi4zNjk5MzQ4ODE1NzUwODJFMjB8
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="113", "Not-A.Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;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/login.jsp
```

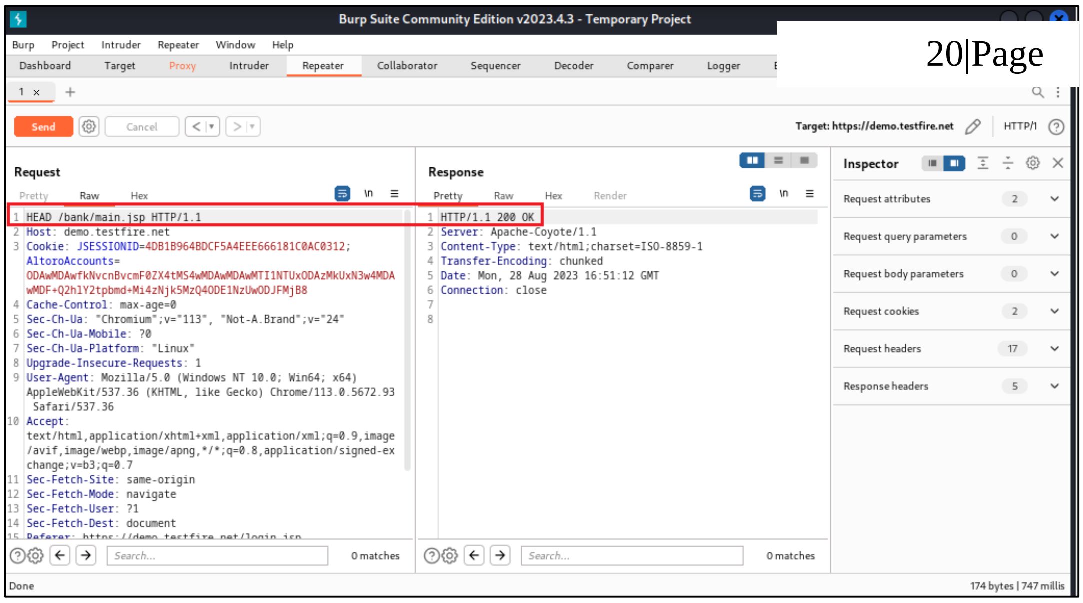
Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6263
Date: Mon, 28 Aug 2023 16:50:55 GMT
Connection: close








<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	2
Request headers	17
Response headers	5

Done 6,431 bytes | 827 millis

HEAD:



Burp Suite Community Edition v2023.4.3 - Temporary Project

Target: https://demo.testfire.net

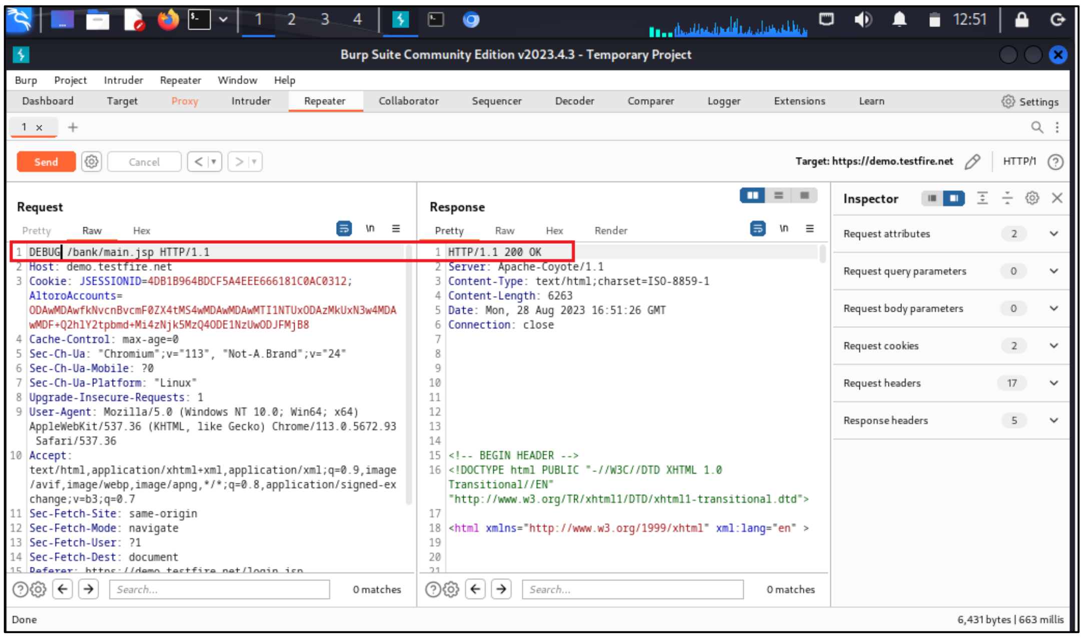
Request

```
HEAD /bank/main.jsp HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=4DB1B964BDCF5A4EEE666181C0AC0312;
AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tMS4wMDAwMDAwMTI1NTUxODAzMkUxN3w4MDA
wMDF+Q2hlY2tpbmd+Mi4zNjk5MzQ4ODE1NzUwODJFMjB8
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="113", "Not-A.Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Mon, 28 Aug 2023 16:51:12 GMT
Connection: close
```

DEBUG:



Burp Suite Community Edition v2023.4.3 - Temporary Project

Target: https://demo.testfire.net

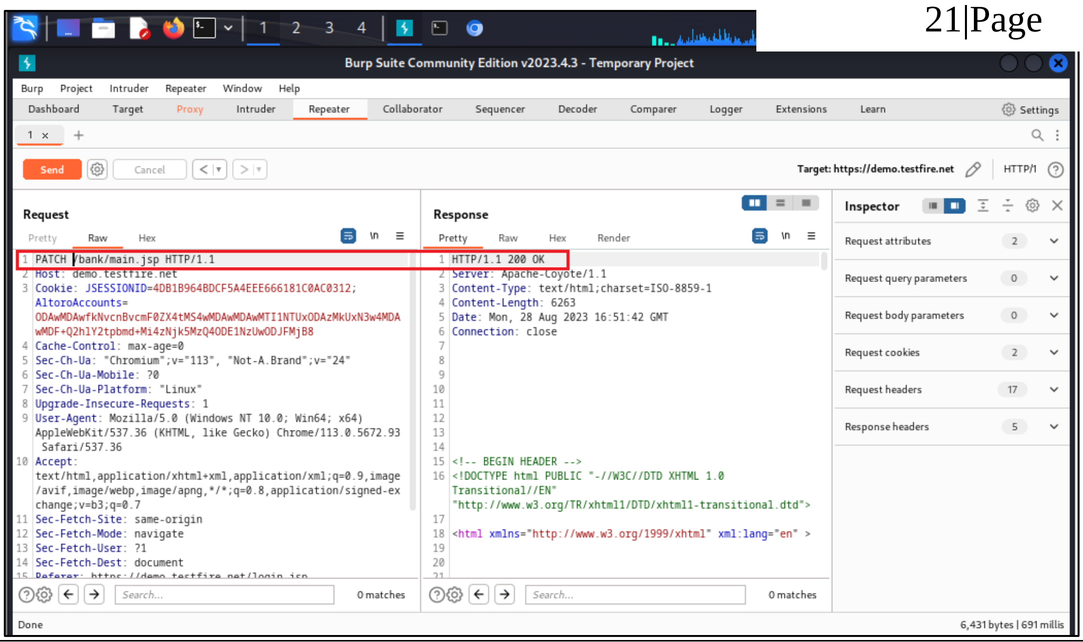
Request

```
DEBUG /bank/main.jsp HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=4DB1B964BDCF5A4EEE666181C0AC0312;
AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tMS4wMDAwMDAwMTI1NTUxODAzMkUxN3w4MDA
wMDF+Q2hlY2tpbmd+Mi4zNjk5MzQ4ODE1NzUwODJFMjB8
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="113", "Not-A.Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
```

Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6263
Date: Mon, 28 Aug 2023 16:51:26 GMT
Connection: close








<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
```

PATCH:



Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Send Cancel
Target: https://demo.testfire.net HTTP/1
Request Pretty Raw Hex
Response Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 17
Response headers 5
0 matches
Done
6,431 bytes | 691 millis

```
PATCH /bank/main.jsp HTTP/1.1
Host: demo.testfire.net
Cookie: JSESSIONID=4DB1B964BDCF5A4EEE666181C0AC0312;
AltoroAccounts=
ODAwMDAwfkNvcnBvcmF0ZX4tMS4wMDAwMDAwMTI1NTUxODAzMkUxN3w4MDA
wMDF+Q2hlY2tpbmd+Mi4zNjk5MzQ4ODE1NzUwODJFMjB8
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="113", "Not-A.Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93
 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;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/login.jsp
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 6263
Date: Mon, 28 Aug 2023 16:51:42 GMT
Connection: close








<!-- BEGIN HEADER -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
```

Impact	It leads to the disclosure of sensitive information such as internal authentication headers appended by reverse proxies.
Recommendation	Risky Access Control Allow Methods (PUT, DELETE, OPTIONS, CONNECT, HEAD, DEBUG & PATCH method) Should be disabled.
Reference(s)	https://portswigger.net/kb/issues/00500a00_http-trace-method-is-enabled

9. FUTURE SCOPE

The Web Application Penetration Testing performed was focused on AltoroMutual Web Application. This result is intended to be an overall assessment of AltoroMutual Web application that fall within the scope of this project.

Furthermore, the findings in this report reflect the conditions found during the testing, and do not necessarily reflect current conditions.

10. CONCLUSION

In this project we explained how Vulnerability Assessment and Penetration Testing can be used as an effective cyber defence technology. We described why VAPT should be made a compulsory activity for cyber defence. We explained complete life cycle of VAPT, prevalent VAPT techniques. This project provide complete overview of Vulnerability Assessment and Penetration Testing, and its use as a cyber-defence technology. This project clearly explain necessity to increase use of VAPT for complete system security. This project would be very helpful for future researchers to get complete knowledge of VAPT process, tools, techniques and its use as a cyber-defence technology. It would be helpful to develop new VAPT techniques and tools. Security testing was performed on the subject application. Report submitted and Management attention was sought to take up mitigation of the reported vulnerabilities, in preference of its Risk ranking / Severity. Recommendations were given in the report for closure of the reported observations as a guidance. We note that there are still open vulnerabilities and advice to take up suitable measures of closure of the same. You may refer the detailed section of this report, which includes the updated comments and testing status.

10. REFERENCES

1. *https://owasp.org/www-community/attacks/SQL_Injection*
2. *https://owasp.org/www-community/attacks/xss/*
3. *https://www.cvedetails.com/cwe-details/319/Cleartext-Transmission-of-Sensitive-Information.html*
4. *https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html*
5. *https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/*
6. *https://owasp.org/www-community/attacks/Clickjacking*
7. *https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server*
8. *https://owasp.org/www-community/HttpOnly*
9. *https://portswigger.net/kb/issues/00500a00_http-trace-method-is-enabled*