

## Assignment 4

### Step 1: OWASP Top 10 Vulnerabilities Overview:

OWASP category: A01:2021 - Broken Access Control

Business Impact: Exploitation of broken access control vulnerabilities can lead to significant business disruption, causing downtime, productivity loss, and financial harm. Additionally, organisations may incur substantial expenses related to incident response, remediation efforts, and recovery procedures. The resulting disruption not only impacts operational efficiency but also tarnishes the organisation's reputation and erodes customer trust. Therefore, addressing these vulnerabilities is crucial to safeguarding business continuity and mitigating potential financial and reputational risks.

OWASP category: A02:2021 - Cryptographic failures

Business Impact: Cryptographic failures can result in significant financial losses, legal liabilities, and reputational damage for organisations. Moreover, the negative publicity and social media backlash that accompany security breaches can exacerbate the erosion of customer trust and confidence. Consequently, addressing these vulnerabilities is paramount to preserving the organisation's integrity and safeguarding its long-term viability in the market.

OWASP category: A03:2021 - Injection

Business Impact: Injection vulnerabilities pose significant risks to organisations, including financial losses, legal liabilities, and reputational damage. The negative impact on reputation can lead to customer churn and decreased market share, underscoring the urgent need for robust security measures to mitigate these risks effectively.

OWASP category: A04:2021 - Insecure Design

Business Impact: Insecure design can compromise proprietary information, leading to lost revenue, diminished market share, and reduced innovation. This exposure underscores the critical importance of prioritising security throughout the software development lifecycle to mitigate risks effectively and safeguard the organisation's business interests.

#### OWASP category: A05:2021 - Security Misconfiguration

**Business Impact:** Security misconfigurations can lead to a loss of trust among customers, resulting in reputational damage and negative publicity. This erosion of trust can have far-reaching consequences, impacting customer loyalty, brand perception, and overall business success. Therefore, it is imperative for organisations to prioritise the mitigation of security misconfigurations to safeguard their reputation and maintain the trust of their stakeholders.

#### OWASP category: A06:2021 - Vulnerable and Outdated Components

**Business Impact:** Exploitation of vulnerabilities in components can disrupt business operations, leading to downtime, loss of productivity, and financial impacts. These disruptions can impair customer service, revenue generation, and overall business performance, highlighting the critical importance of addressing vulnerable components to maintain operational resilience.

#### OWASP category: A07:2021 - Identification and Authentication Failures

**Business Impact:** A07:2021, Identification and Authentication Failures, present significant security risks to web applications. When identification and authentication mechanisms fail or are improperly implemented, it can lead to various business impacts, including:


**Unauthorised Access:** Failures in identification and authentication can result in unauthorised users gaining access to sensitive data, functionalities, or administrative interfaces within the application. Attackers may exploit weak or missing authentication controls to bypass security measures and perform malicious Activities.

**Data Breaches:** Authentication failures can lead to data breaches and exposure of sensitive information, such as personally identifiable information (PII), financial records, or intellectual property. Data breaches can result in financial losses, legal liabilities, and damage to the organisation's reputation.




**Regulatory Non-Compliance:** Many industries are subject to regulatory requirements regarding the protection of user credentials, authentication mechanisms, and access

controls (e.g., GDPR, HIPAA, PCI DSS). Failure to implement adequate identification and authentication controls can lead to non-compliance fines, legal actions, and reputational damage.

**Fraud and Identity Theft:** Weak or compromised authentication mechanisms can enable attackers to impersonate legitimate users, conduct fraudulent activities, or steal sensitive information for identity theft purposes. This can lead to financial







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

DEMO

SITE

ONLY

 <a href="#">ONLINE BANKING LOGIN</a>	<a href="#">PERSONAL</a>	<a href="#">SMALL BUSINESS</a>	<a href="#">INSIDE ALTORO MUTUAL</a>
<div> <a href="#">PERSONAL</a> <ul style="list-style-type: none"> <li><a href="#">Deposit Product</a></li> <li><a href="#">Checking</a></li> <li><a href="#">Loan Products</a></li> <li><a href="#">Cards</a></li> <li><a href="#">Investments &amp; Insurance</a></li> <li><a href="#">Other Services</a></li> </ul> </div> <div> <a href="#">SMALL BUSINESS</a> <ul style="list-style-type: none"> <li><a href="#">Deposit Products</a></li> <li><a href="#">Lending Services</a></li> <li><a href="#">Cards</a></li> <li><a href="#">Insurance</a></li> <li><a href="#">Retirement</a></li> <li><a href="#">Other Services</a></li> </ul> </div> <div> <a href="#">INSIDE ALTORO MUTUAL</a> <ul style="list-style-type: none"> <li><a href="#">About Us</a></li> <li><a href="#">Contact Us</a></li> <li><a href="#">Locations</a></li> <li><a href="#">Investor Relations</a></li> <li><a href="#">Press Room</a></li> <li><a href="#">Careers</a></li> <li><a href="#">Subscribe</a></li> </ul> </div>	<div> <a href="#">Online Banking with FREE Online Bill Pay</a>            No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.         </div>  <div> <a href="#">Real Estate Financing</a>            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         </div>	 <div> <a href="#">Business Credit Cards</a>            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.         </div> <div> <a href="#">Retirement Solutions</a>            Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.         </div>	<div> <a href="#">Privacy and Security</a>            The 2000 employees of Altoro Mutual are dedicated to protecting your <a href="#">privacy</a> and <a href="#">security</a>. 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.         </div>  <div> <a href="#">Win a Samsung Galaxy S10 smartphone</a>            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.         </div>

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2024 Altoro Mutual, Inc.

[This web application is open source! Get your copy from GitHub and take advantage of advanced features.](#)



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

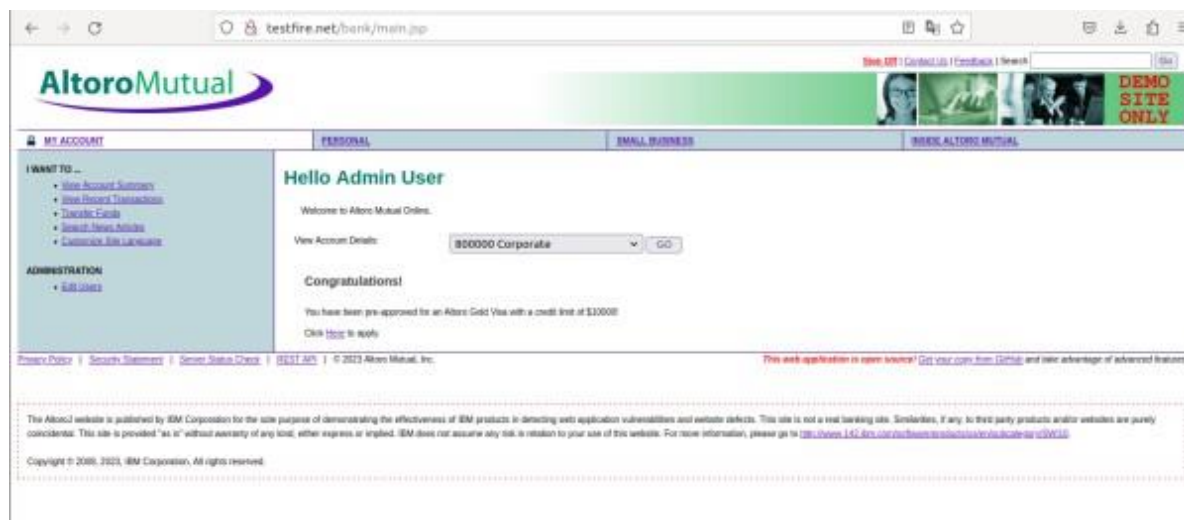
### Step 3: Vulnerability Identification Report: Alerts

- Cross Site Scripting (DOM Based)
- Cross Site Scripting (Reflected)
- SQL Injection
- URL Redirection Attack
- ClickJacking
- Link Injection
- Server Leaks Version Information
- X-Content-Type-Options Header Missing
- Information Disclosure

The screenshot displays the Burp Suite interface. The top menu bar includes Dashboard, Target, Intruder, Repeater, Window, and Help. Below the menu is a toolbar with icons for Intercepting, Target, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extensions, and Learn. The main panel shows a list of HTTP requests with columns for #, Host, Method, URL, Params, Edited, Status, Length, MIME type, Extension, and Title. The selected request is a POST to /sendFeedback with a status of 200 and a length of 7362. The right-hand pane shows the details of the selected request, including the Request attributes (Protocol: HTTP/1.1, Method: POST, Path: /sendFeedback) and the Request body parameters (cfile, name, email\_addr, subject, comments, submit).

These are the main alerts on this website.

After hitting the login button we sign in as administrators.

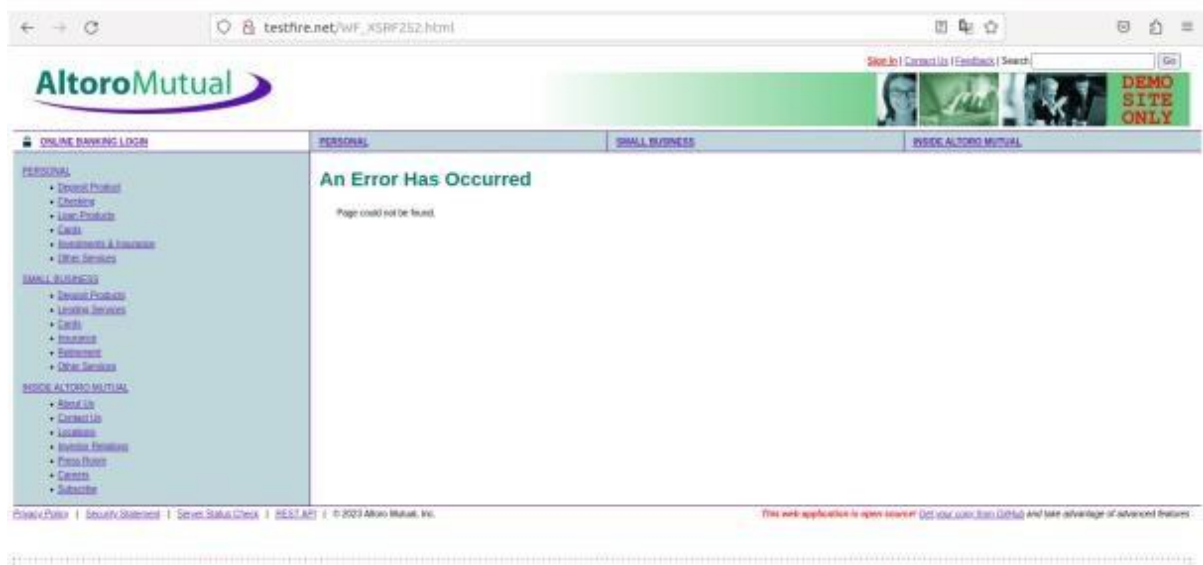


In the URL I embedded another URL “google.com” and I enter the site it redirects to google.com. This vulnerability can be used for the Phishing attack.



## Step 4: Vulnerability Exploitation Demonstration





## Step 5: Mitigation Strategy Proposal:

### Risk Level by alert type:

This table shows the risk level of each directed vulnerabilities

Alert type	Severity
Cross Site Scripting (DOM Based)	High
Cross Site Scripting (Reflected)	High
SQL Injection	High
URL Redirection Attack	High

ClickJacking	Medium
Link Injection	Medium
Server Leaks Version Information	Low
X-Content Header Missing	Low
Information Disclosure	Info