

Assignment 4

Step 1: OWASP Top 10 Vulnerabilities Overview:

- **OWASP Top 10 vulnerabilities represent the most critical security risks to web applications, including injection attacks, broken authentication, sensitive data exposure, XML external entities (XXE), etc.**
- **Discuss the potential impact of these vulnerabilities on web application security and the importance of addressing them to prevent exploitation by attackers.**

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 losses for both the organisation and its users, as well as damage to trust and reputation.

OWASP category: A08:2021 - Software and Data Integrity Failures

Business Impact: Integrity failures can result in legal liabilities, regulatory non-compliance, and reputational damage, posing significant risks to the organisation. Negative publicity, media coverage, and social media backlash can tarnish the organisation's brand image, leading to customer churn and decreased market share. Therefore, ensuring the integrity of software and data is essential for maintaining trust, compliance, and long-term business success.

OWASP category: A09:2021 - Security Logging and Monitoring Failure


Business Impact: Security breaches resulting from logging and monitoring failures can severely damage an organisation's reputation and erode customer trust. Negative publicity, media coverage, and social media backlash can tarnish the organisation's brand image, leading to customer churn and decreased market share.

OWASP category: A010:2021 - Server-Side Request Forgery




Business Impact: SSRF attacks can disrupt business operations by exploiting vulnerabilities in internal systems or third-party services, causing downtime, service interruptions, or degradation of application performance. These disruptions can impact customer service, revenue generation, and overall business performance.

Step 2: Altro Mutual Website Analysis:




- **Students should explore various sections of the Altro Mutual website, including the login page, user registration, payment portal, contact forms, and any other interactive features.**
- **They should identify vulnerabilities such as SQL injection, cross-site scripting (XSS), insecure authentication mechanisms, insecure direct object references, etc., based on their understanding of the OWASP Top 10 list.**




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

DEMO SITE ONLY

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

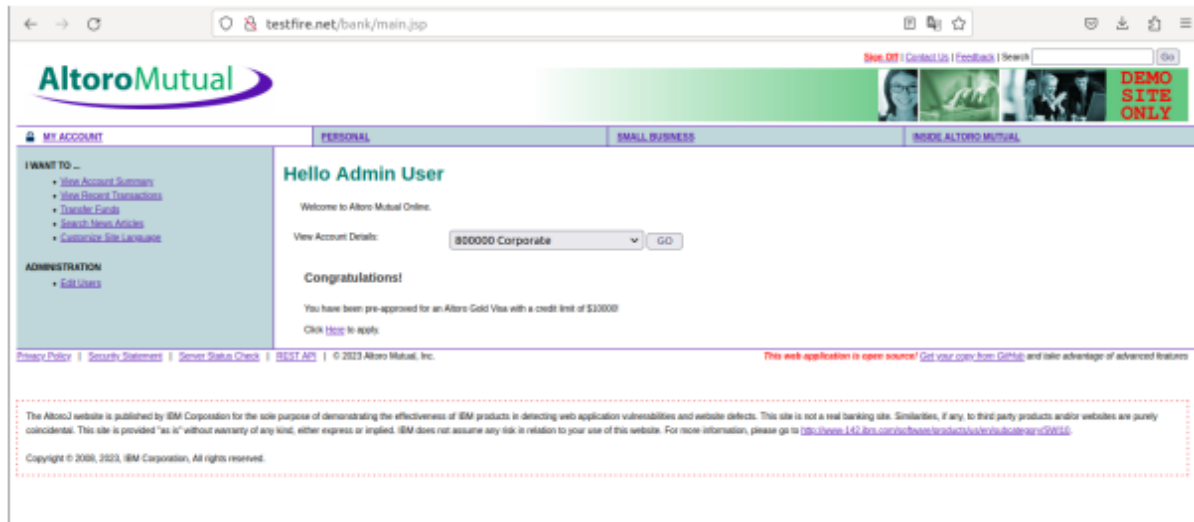
[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2024 Altoro Mutual, Inc.
 This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features!



ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS
<p>PERSONAL</p> <ul style="list-style-type: none"> Deposit Product Checking Loan Products Cards Investments & Insurance Other Services <p>SMALL BUSINESS</p> <ul style="list-style-type: none"> Deposit Products Lending Services Cards Insurance Retirement Other Services <p>INSIDE ALTORO MUTUAL</p> <ul style="list-style-type: none"> About Us Contact Us Locations 	<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:

- The report should include a detailed description of Altro Mutual's website structure and functionality, including potential areas of vulnerability.
- For each identified vulnerability, students should provide an explanation of how it could be exploited by attackers and the potential impact on Altro Mutual's business operations and users.
- Recommendations for mitigating each vulnerability should be provided, such as implementing input validation, using parameterized queries to prevent SQL injection, implementing secure authentication mechanisms like multi-factor authentication (MFA), etc.



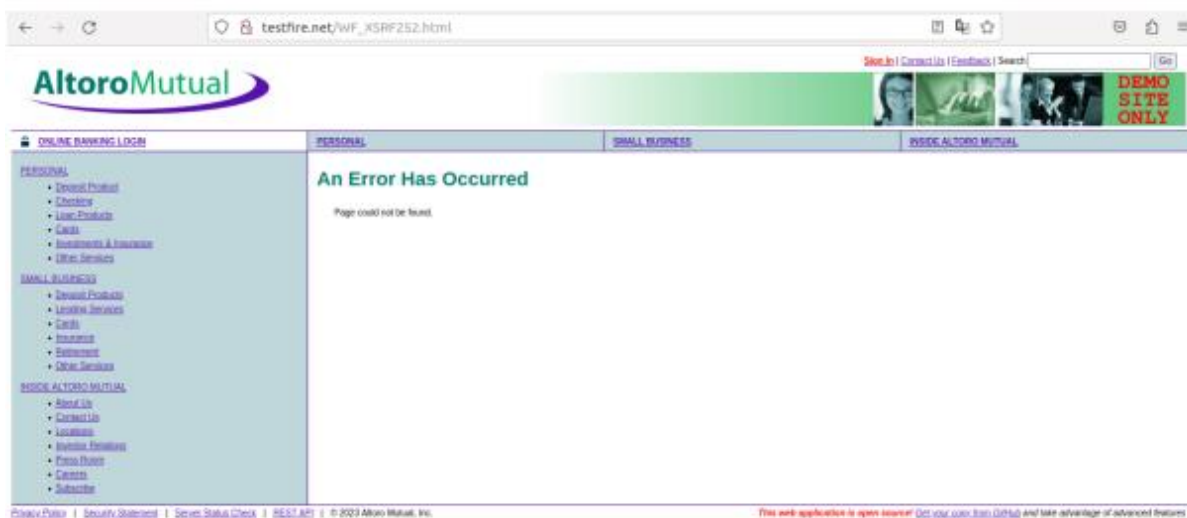
In the URL I embedded another URL “google.com” and I enter the site it redirects to google.com. This vulnerability can be used for the Phishing attack.



Step 4: Vulnerability Exploitation Demonstration

- Students can demonstrate how each identified vulnerability could be exploited using proof-of-concept attacks or simulation tools.
- For example, they could demonstrate how SQL injection attacks can be used to extract sensitive information from the database or how cross-site scripting (XSS) attacks can be used to execute malicious scripts in users' browsers.

Website is vulnerable to clickjacking!



Step 5: Mitigation Strategy Proposal:

- The mitigation strategy should prioritize addressing high-risk vulnerabilities identified in the vulnerability identification report.

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