

Assignment-4

Shaik Sohail

Date:14-03-24

KHIT

Step 1: -

1. Broken Access Control

Potential Impact: -

Broken access control can affect companies severely by hurting them financially as well as damaging their reputation and business relationships. To prevent broken access control, it's important to implement and validate that your access controls are working properly on a continuous basis.

2. Cryptographic Failures

Potential Impact: -

Attackers can get hold of a complete database having thousands of sensitive information, data theft, public listing, breaches, and many critical problems with business-related data.

3. Injection

Potential Impact: -

Injections into the circular flow of income are a result of money borrowed by households and firms from different external sources, like financial institutions. However, this additional income does not result in an immediate expenditure.

4. Insecure Design

Potential Impact: -

Insecure design vulnerabilities result from non-adherence to security best practices during the design process. Today, it is one of the leading causes of functionality failures, data breaches, broken policies, and tarnished reputations.

5. Security Misconfiguration

Potential Impact: -

Security misconfigurations can allow attackers to gain unauthorized access to the networks, systems and data which in turn can cause significant monetary and reputational damage to your organization.

6. Vulnerable and Outdated Components

Potential Impact: -

A vulnerable and outdated component is a software component that is no longer being supported by the developer, making it susceptible to security vulnerabilities. Many times, a component has known vulnerabilities that don't get fixed due to a lack of maintainer.

7. Identification and Authentication Failure

Potential Impact: -

The failure of a system to identify and/or authenticate leaves the application susceptible to attacks and leaves user accounts/data at risk. Authentication failure poses a stringent and profound threat to an organization's security.

Assignment-4

Shaik Sohail

Date:14-03-24

KHIT

8. Software and Data Integrity Failure

Potential Impact: -

Addressing software and data integrity failures is crucial for maintaining the security of web applications. Failure to address these vulnerabilities can result in significant financial losses, reputational damage, legal liabilities, loss of customer trust, etc.

9. Security Logging and Monitoring Failure

Potential Impact: -

Insufficient logging and monitoring of systems can impact visibility, incident alerting, login failures, system failures and breaches. This makes it essential to have a fully operational logging and monitoring system to collect logs and give out alerts to Security Operation Center (SOC) staff and administrators.

10. Server Side Request Forgery (SSRF)

Potential Impact: -

successful SSRF attack can often result in unauthorized actions or access to data within the organization. This can be in the vulnerable application, or on other back-end systems that the application can communicate with.

Importance of addressing them to prevent exploitation by attackers.

Addressing OWASP vulnerabilities is crucial to prevent exploitation by attackers and ensure the security of software applications. OWASP (Open Web Application Security Project) identifies and categorizes common security risks in web applications, providing guidelines and best practices for mitigating these vulnerabilities. Failing to address OWASP vulnerabilities leaves applications susceptible to attacks such as SQL injection, cross-site scripting (XSS), and authentication bypass, which can lead to data breaches, financial losses, and reputational damage. By proactively addressing OWASP vulnerabilities through secure coding practices, regular security assessments, and timely patching, organizations can significantly reduce the risk of exploitation and protect sensitive data from malicious actors.

Step 2: -

Altro Mutual website



Assignment-4

Shaik Sohail

Date:14-03-24

KHIT

Login Page: Allows registered users to securely access their accounts by entering their credentials, typically username/email and password.

User Registration: New users can create accounts by providing personal information like name and email, and setting up a password, often with optional additional details.

Payment Portal: Enables users to make secure payments for services or products, requiring input of payment details like credit/debit card information in a protected environment.

Contact Forms: Users can send inquiries or feedback by submitting their name, email, and message details through a form, sometimes with optional fields for additional information.

Identification of Vulnerabilities

SQL Injection - SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.

Cross Site Scripting (XSS) - Cross-site scripting (XSS) is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website.

Insecure Authentication Mechanism - Insecure Authentication exploits vulnerable authentication schemes by faking or bypassing authentication.

Insecure direct object references - Insecure direct object references (IDOR) are a type of access control vulnerability that arises when an application uses user-supplied input to access objects directly.

Step 3: -

Altoro Mutual Website IP address is **65.61.137.117**. Vulnerability scan is done on Altoro Mutual Website

Starting Nmap 7.40 (<https://nmap.org>) at 2024-03-20 06:26 UTC

Nmap scan report for 65.61.137.117

Host is up (0.046s latency).

PORT	STATE	SERVICE
------	-------	---------

21/tcp	filtered	ftp
--------	----------	-----

22/tcp	filtered	ssh
--------	----------	-----

23/tcp	filtered	telnet
--------	----------	--------

80/tcp	open	http
--------	------	------

110/tcp	filtered	pop3
---------	----------	------

143/tcp	filtered	imap
---------	----------	------

443/tcp	open	https
---------	------	-------

3389/tcp	filtered	ms-wbt-server
----------	----------	---------------

Assignment-4

Shaik Sohail

Date:14-03-24

KHIT

Website Structure and Functionality

1. **Homepage:** Provides an overview of Altro Mutual's services, promotions, and news updates.
2. **Account Management:** Allows users to register, log in, view account details, and manage their profiles.
3. **Financial Products:** Showcases Altro Mutual's range of financial products such as savings accounts, loans, and investment options.
4. **Payment and Transactions:** Enables users to make payments, transfers, and view transaction history securely.
5. **Customer Support:** Offers customer service options such as FAQs, contact forms, and live chat for assistance.
6. **Educational Resources:** Provides resources like articles, guides, and tools to help users make informed financial decisions.

Potential Areas of Vulnerability

- **Input Validation:** Insufficient validation in forms may lead to SQL injection or XSS vulnerabilities.
- **Authentication:** Weak authentication measures or lax password policies can compromise accounts.
- **Session Management:** Poor session handling may result in session hijacking.
- **Data Protection:** Inadequate encryption or storage practices can lead to data breaches.
- **Third-Party Integrations:** Vulnerabilities in plugins or APIs pose security risks.
- **Access Control:** Weak access controls may allow unauthorized access to sensitive information or functionality.

Recommendations for mitigating Vulnerabilities

1. **Secure Coding Practices:** Follow secure coding guidelines such as OWASP's Secure Coding Practices Checklist, which covers topics like input validation, output encoding, authentication, and access control. Use secure coding frameworks and libraries that handle security concerns effectively.
2. **Regular Security Assessments:** Conduct regular security assessments, including penetration testing and code reviews, to identify and remediate vulnerabilities in your applications. Automated tools like OWASP ZAP (Zed Attack Proxy) can help scan for common vulnerabilities and provide actionable insights.
3. **Patch Management:** Keep your software and libraries up to date with the latest security patches and updates. Vulnerabilities in third-party components can expose your applications to attacks, so monitor vendor advisories and apply patches promptly.
4. **Web Application Firewalls (WAF):** Implement a WAF to filter and block malicious traffic, including attacks like SQL injection, XSS, and CSRF. Configure the WAF to enforce security policies and monitor for suspicious activity.

Assignment-4

Shaik Sohail

Date:14-03-24

KHIT

5. Secure Authentication and Session Management: Use strong authentication mechanisms (e.g., multi-factor authentication) to protect user accounts from unauthorized access. Implement secure session management practices to prevent session hijacking and fixation attacks.
6. Data Encryption: Encrypt sensitive data both at rest and in transit using strong encryption algorithms. Securely store and manage encryption keys to prevent unauthorized access to encrypted data.
7. Security Headers: Utilize security headers (e.g., Content Security Policy, X-Content-Type-Options, X-XSS-Protection) to enhance the security posture of your web applications. Properly configure these headers to mitigate common attack vectors.
8. Security Training and Awareness: Educate developers, testers, and other stakeholders about OWASP vulnerabilities and best practices for secure software development. Foster a security-aware culture within your organization to prioritize security throughout the software development lifecycle.

Step 4: -

Vulnerability Exploitation

SQL Injection - SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. Performing SQL Injection on Altoro Mutual Website by giving username as '**or 1=1**'— and password as **1234** in the login page.

The screenshot displays the Altoro Mutual Online Banking Login page. The page has a header with the Altoro Mutual logo and navigation links. The main content area is titled "Online Banking Login" and contains a login form with fields for "Username:" and "Password:". The "Username:" field contains the text "or 1=1" and the "Password:" field contains "1234". A "Login" button is visible below the password field. The page also features a sidebar with navigation links and a footer with copyright information.

Altoro Mutual

MY ACCOUNT PERSONAL SMALL BUSINESS ENTERPRISE ALTORO MUTUAL

Online Banking Login

Username: or 1=1

Password: 1234

Login

Privacy Policy | Security Information | Contact Us | Feedback | Search

© 2004 Altoro Mutual, Inc.

The Altoro website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and relative defects. This site is not a real banking site. 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <http://www.hcl-software.com/faq.asp>.

Copyright © 2006, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

Assignment-4

Shaik Sohail

Date:14-03-24

KHIT



Cross Site Scripting (XSS) - Cross-site scripting (XSS) is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website. Performing XSS on Altoro Mutual Website by using the command `<script>alert("you got hacked")</script>` in search bar.

Assignment-4

Shaik Sohail

Date:14-03-24

KHIT



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



crypt-alert("you are fac")
 [Go](#)



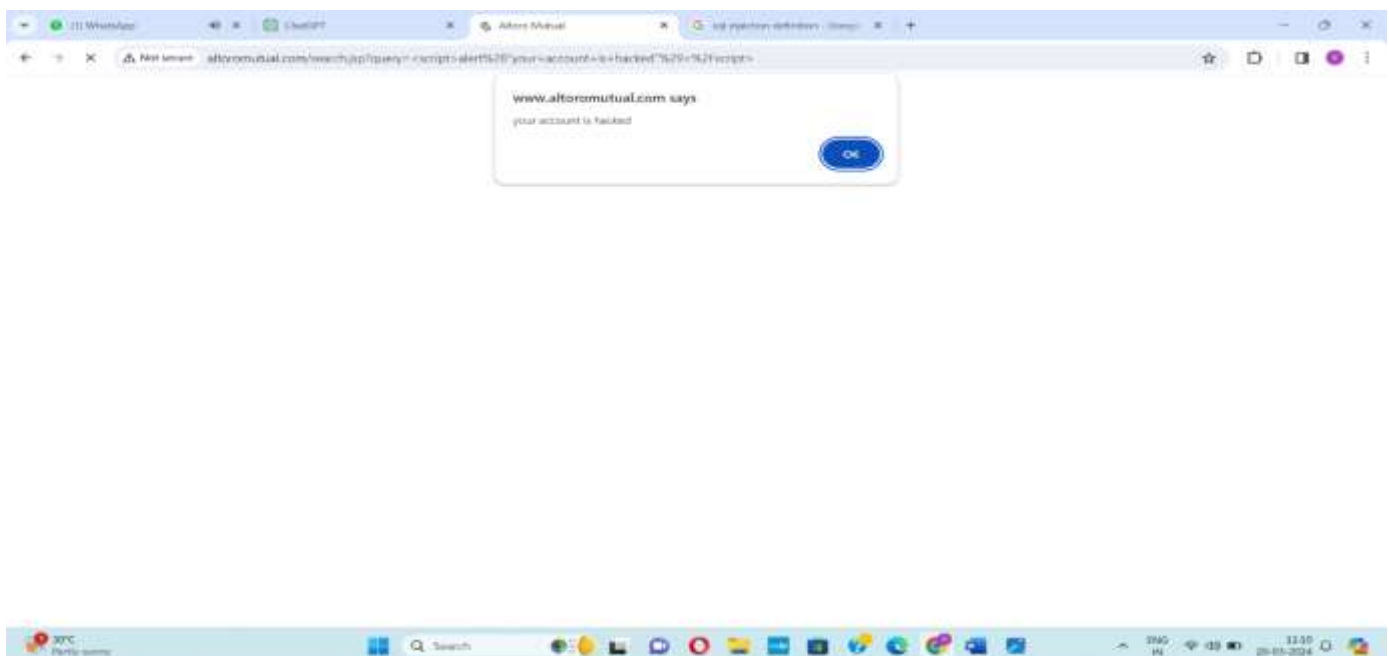
MY ACCOUNT	PERSONAL	SMALL BUSINESS	INSURE ALTORO MUTUAL
<p>PERSONAL</p> <ul style="list-style-type: none"> • General Product • Checking • Loan Products • Cards • Investments & Insurance • Other Services <p>SMALL BUSINESS</p> <ul style="list-style-type: none"> • General Products • Lending Services • Cards • Insurance • Retirement • Other Services <p>INSURE ALTORO MUTUAL</p> <ul style="list-style-type: none"> • About Us • Contact Us • Locations • Investor Relations • Press Room • Careers • Subscribe 	<p>Online Banking Login</p> <p> Username: <input type="text"/> Password: <input type="password"/> <input type="button" value="Login"/> </p>		

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [BEST API](#) | © 2014 Altoro Mutual, Inc.

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

The Above website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarly, 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/secure/>.

Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd. All rights reserved.



Insecure Authentication Mechanism - Insecure Authentication exploits vulnerable authentication schemes by faking or bypassing authentication. Performing Insecure Authentication Mechanism on Altoro Mutual Website by giving username as **username;** or **1=1--** and password as **1234** in the login page.

Assignment-4

Shaik Sohail

Date:14-03-24

KHIT

The screenshot shows the AltoroMutual website interface. The header includes the AltoroMutual logo, a 'Sign Off' link, and a search bar. The main navigation bar has links for 'MY ACCOUNT', 'PERSONAL', 'SMALL BUSINESS', and 'ENTER ALTORO MUTUAL'. The 'PERSONAL' section is active, displaying the 'Online Banking Login' page. The login form has a 'Username' field with a hint '(username)@1234', a 'Password' field with four asterisks, and a 'Login' button. The left sidebar lists various services under 'PERSONAL', 'SMALL BUSINESS', and 'ENTER ALTORO MUTUAL'. The footer contains a disclaimer: 'The Altoro website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-softwares.com/assessing>. Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.'

Insecure direct object references - Insecure direct object references (IDOR) are a type of access control vulnerability that arises when an application uses user-supplied input to access objects directly. Performing IDOR on Altoro Mutual Website by giving username as **jsmith'--** and password as **1234** in the

Assignment-4

Shaik Sohail

Date:14-03-24

KHIT

login page, with this attack we can enter into the public bank accounts and do whatever the transactions we want.

AltoroMutual

Sign Off | Contact Us | Feedback | Search

PERSONAL | SMALL BUSINESS | INDIVIDUAL ALTORO MUTUAL

Online Banking Login

Username:

Password:

Login

Privacy Policy | Security Statement | Service Status Check | RSS Feeds | © 2024 Altoro Mutual, Inc.

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

The Altoro website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarly, 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/privacy/>.

Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., all rights reserved.

AltoroMutual

Sign Off | Contact Us | Feedback | Search

PERSONAL | SMALL BUSINESS | INDIVIDUAL ALTORO MUTUAL

Hello John Smith

Welcome to Altoro Mutual Online.

View Account Details:

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$100,000.

Click [here](#) to apply.

Privacy Policy | Security Statement | Service Status Check | RSS Feeds | © 2024 Altoro Mutual, Inc.

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

The Altoro website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarly, 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/privacy/>.

Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., all rights reserved.

Step 5: -

Mitigation Strategy Proposal

Assignment-4

Shaik Sohail

Date:14-03-24

KHIT

1. **Identify High-Risk Vulnerabilities:** Use vulnerability assessments to find critical vulnerabilities.
2. **Assess Risks:** Evaluate the impact and likelihood of exploitation for each vulnerability.
3. **Prioritize based on Severity:** Use industry-standard metrics like CVSS to rank vulnerabilities.
4. **Establish Criteria:** Set clear criteria for prioritizing vulnerabilities, considering factors like system criticality and patch availability.
5. **Patch Management:** Quickly deploy patches for high-risk vulnerabilities and regularly monitor effectiveness.
6. **Remediation Plan:** Develop a plan to systematically address high-risk vulnerabilities, considering operational constraints.
7. **Continuous Monitoring:** Keep an eye on the effectiveness of mitigation efforts and adapt strategies as needed.
8. **Communication:** Maintain open communication with stakeholders to keep them informed about prioritized vulnerabilities and mitigation progress.

Step 6: -

Documented the Exploitation process and the commands used in the exploitation and attached the output the respective exploitations.