

Week 1 Assignment: Top 5 OWASP

Overview:

To study the top 5 OWSAP (Open Web Application Security Project) security risks and provide a comprehensive report on them including their description and business impact.

A01:2021-Broken Access Control:

CWE: 284: Improper Access Control

Description: The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor

Business Impact: This weakness allows an attacker to bypass intended security restrictions and perform a variety of actions depending on the source of error and functionality of the application. An attacker might be able to perform certain actions by gaining elevated privileges, reading otherwise restricted information, executing commands, bypassing implemented security mechanisms, etc.

A02:2021-Cryptographic Failures

CWE-326: Inadequate Encryption Strength

Description: The product stores or transmits sensitive data using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required. A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current attack methods and resources.

Business Impact: An attacker may be able to decrypt the data using brute force attacks leading to data breaches which could further lead to legal consequences, reputational damage, financial losses, operational disruptions, competitive disadvantage, loss of intellectual property, and potential lawsuits. Strong encryption and compliance with regulations are crucial to mitigate these risks.

A03:2021-Injection

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Description: The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Business Impact: SQL injection vulnerabilities pose significant risks to a system's security. They can result in unauthorized reading of application data, undermining confidentiality, especially when databases store sensitive information. Additionally, these vulnerabilities can enable attackers to bypass protection mechanisms, potentially accessing the system without proper credentials and even modify or delete application data, compromising data integrity.

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

Altoro Mutual

Not secure | testfire.net

Sign In | Contact Us | Feedback | Search

Go

AltoroMutual

ONLINE BANKING LOGIN

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

PERSONAL

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

SMALL BUSINESS

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.

INSIDE ALTORO MUTUAL

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/SW110>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

Online Banking Login

Username:

Password:

Login

Altoro Mutual

Sign Off | Contact Us | Feedback | Search

Go

MY ACCOUNT

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

PERSONAL

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.

SMALL BUSINESS

INSIDE ALTORO MUTUAL

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/SW110>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

A04:2021 – Insecure Design

CWE-256: Plaintext Storage of a Password

Description: Storing a password in plaintext may result in a system compromise. Password management issues occur when a password is stored in plaintext in an application's properties, configuration file, or memory. Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. In some contexts, even storage of a plaintext password in memory is considered a security risk if the password is not cleared immediately after it is used.

Business Impact: Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. This can lead to unauthorized access, identity theft, financial loss, data breaches, and reputational damage. Developers sometimes feel they are helpless in safeguarding the application against someone with configuration file access, but this mindset aids potential attackers.

A05:2021 – Security Misconfiguration

CWE-611: Improper Restriction of XML External Entity Reference

Description: The product processes an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output.

Business Impact: Improper Restriction of XML External Entity Reference can have a significant impact on security. It can lead to unauthorized access to internal files, potential data exposure, and even denial of service. By exploiting this vulnerability, attackers may manipulate XML parsers to access or modify sensitive information, disrupting system functionality and compromising data integrity and confidentiality. Preventing and mitigating this vulnerability is crucial to maintaining a secure software environment.