Date: 18/10/2023

Team ID: 2.10

Project Name: Practice Website Development

Team Members:

Sohan

Pratheek

Shaz

Atharva

**Vulnerabilities**

**Invalid Forgot Password Process**

CWE: CWE-640

OWASP Category: A04:2021 – Insecure Design

Description: Architectural flaws can result in security vulnerabilities if appropriate security mitigations are not taken in the design phase of the practice website. Specifically, this vulnerability pertains to the "Forgot Password" process, which may have security weaknesses due to design flaws.

Business Impact: Insecure design of the "Forgot Password" process can make the practice website susceptible to a range of weaknesses. This documentation section addresses the potential impacts and suggests mitigation strategies to improve the security of this process.

Vulnerability Path

URL: <http://yourpracticewebsite.com/forgot_password>

Vulnerability Parameter: http://yourpracticewebsite.com/forgot\_password

Steps to Reproduce:

Access the URL: http://yourpracticewebsite.com/forgot\_password

Navigate to the login page.

Enter a random password for testing.

Observe the auto-generated password below the "Forgot Password" section.

Recommendation:

Establish and use a library of secure mechanisms.

Implement a strong validation process to enhance the security of the "Forgot Password" feature.

**Cross-Site Scripting (Stored)**

CWE: 79

OWASP Category: A03:2021 – Injections

Description: Cross-Site Scripting (Stored) occurs when a malicious script is injected directly into the practice website. This vulnerability pertains to the storage and subsequent reflection of a malicious script in the web application, particularly within user-generated content.

Business Impact: Storing dangerous data, such as malicious scripts, in a database can have severe security implications. If executed, these scripts can potentially compromise user data and the overall integrity of the practice website.

Vulnerability Path

URL: http://yourpracticewebsite.com/admin/user.php

Vulnerability Parameter: http://yourpracticewebsite.com/admin/user.php

Steps to Reproduce:

Access the URL: http://yourpracticewebsite.com/admin/user.php

Log in with your credentials.

Attempt to register as a new user.

In the registration form, insert a malicious script within the contact box.

Observe the effects of the injected script.

**Insecure File Upload**

CWE: CWE-434

OWASP Category: A8:2017 – Insecure Deserialization

Description: Insecure file upload allows users to upload potentially malicious files, which can lead to remote code execution and other security threats.

Business Impact: Insecure file uploads can result in the execution of malicious code on the server, leading to unauthorized access and data breaches.

Vulnerability Path

URL: http://yourpracticewebsite.com/upload

Vulnerability Parameter: http://yourpracticewebsite.com/upload

Steps to Reproduce:

Access the file upload feature.

Attempt to upload a file containing executable code.

Observe if the website allows and executes the file.

**SQL Injection Vulnerability**

CWE: CWE-89

OWASP Category: A1:2017 – Injection

Description: SQL Injection is a type of security vulnerability that occurs when an attacker is able to manipulate an SQL query in a web application, potentially allowing unauthorized access to databases and data manipulation.

Business Impact: SQL Injection can lead to unauthorized access to sensitive data, data manipulation, and in some cases, complete control over the application's database.

Vulnerability Path

URL: http://yourpracticewebsite.com/search

Vulnerability Parameter: http://yourpracticewebsite.com/search?q=

Steps to Reproduce:

Access the search functionality on the website.

In the search bar, enter a malicious SQL query.

Observe if the website handles the query securely.

**Insecure File Upload**

CWE: CWE-434

OWASP Category: A8:2017 – Insecure Deserialization

Description: Insecure file upload allows users to upload potentially malicious files, which can lead to remote code execution and other security threats.

Business Impact: Insecure file uploads can result in the execution of malicious code on the server, leading to unauthorized access and data breaches.

Vulnerability Path

URL: http://yourpracticewebsite.com/upload

Vulnerability Parameter: http://yourpracticewebsite.com/upload

Steps to Reproduce:

Access the file upload feature.

Attempt to upload a file containing executable code.

Observe if the website allows and executes the file.

**Broken Session Management**

CWE: CWE-613

OWASP Category: A2:2017 – Broken Authentication

Description: Broken session management vulnerabilities can allow attackers to hijack sessions, impersonate users, and gain unauthorized access to sensitive data.

Business Impact: Broken session management can lead to unauthorized access, data breaches, and identity theft.

Vulnerability Path

URL: http://yourpracticewebsite.com/profile

Vulnerability Parameter: http://yourpracticewebsite.com/profile

Steps to Reproduce:

Log in to your user account.

Access the user profile.

Log out.

Attempt to access the profile again without logging in.

**Cross-Site Request Forgery (CSRF)**

CWE: CWE-352

OWASP Category: A8:2017 – Cross-Site Request Forgery (CSRF)

Description: CSRF is an attack that tricks the user into executing unwanted actions on a different website where they are authenticated.

Business Impact: CSRF attacks can lead to unauthorized actions being taken on behalf of the user, potentially compromising their account or data.

Vulnerability Path

URL: http://yourpracticewebsite.com/change\_password

Vulnerability Parameter: http://yourpracticewebsite.com/change\_password

Steps to Reproduce:

Log in to your user account.

Visit a malicious website that contains a CSRF attack.

Observe if unauthorized actions are taken on the practice website.

**XML External Entity (XXE) Injection**

CWE: CWE-611

OWASP Category: A4:2017 – XML External Entity (XXE) Processing

Description: XXE vulnerabilities occur when an application processes XML input from untrusted sources, potentially leading to disclosure of internal files, denial of service, and remote code execution.

Business Impact: XXE vulnerabilities can expose sensitive information, disrupt services, and lead to data breaches.

Vulnerability Path

URL: http://yourpracticewebsite.com/parse-xml

Vulnerability Parameter: http://yourpracticewebsite.com/parse-xml?xml=

Steps to Reproduce:

Access the XML parsing feature on the website.

Submit an XML file with a malicious external entity definition.

Observe if the website processes the XML insecurely.

**Security Misconfiguration**

CWE: CWE-732

OWASP Category: A6:2017 – Security Misconfiguration

Description: Security misconfigurations occur when an application is not securely configured, leading to vulnerabilities such as unauthorized access, data exposure, and other security risks.

Business Impact: Security misconfigurations can result in data breaches, unauthorized access, and financial costs.

Vulnerability Path

URL: http://yourpracticewebsite.com/admin

Vulnerability Parameter: http://yourpracticewebsite.com/admin

Steps to Reproduce:

Access the admin section of the website.

Observe if there are security misconfigurations that allow unauthorized access.

**Missing Function-Level Access Control**

CWE: CWE-284

OWASP Category: A5:2017 – Broken Access Control

Description: Missing function-level access control vulnerabilities occur when an application does not properly check whether a user has access to certain functions or actions.

Business Impact: This can lead to unauthorized access and the execution of restricted functions.

Vulnerability Path

URL: http://yourpracticewebsite.com/change-email

Vulnerability Parameter: http://yourpracticewebsite.com/change-email

Steps to Reproduce:

Log in as a regular user.

Access a privileged function, such as changing another user's email.

Observe if the website enforces proper access control.

**Cross-Origin Resource Sharing (CORS) Misconfiguration**

CWE: CWE-346

OWASP Category: A7:2017 – Cross-Site Scripting (XSS)

Description: CORS misconfigurations can allow unauthorized websites to make requests to your site on behalf of a user, potentially exposing sensitive data.

Business Impact: CORS misconfigurations can lead to data exposure, unauthorized access, and privacy violations.

Vulnerability Path

URL: http://yourpracticewebsite.com/api

Vulnerability Parameter: http://yourpracticewebsite.com/api

Steps to Reproduce:

Access the website's API.

Observe if there are misconfigured CORS settings that allow cross-origin requests.