Assignment 1

Mugdha Thoke

OWASP Vulnerabilities

OWASP stands for Open Web Application Security Project. It is a well-known organization that focuses on enhancing software security. OWASP vulnerabilities are critical security risks that can be faced by web applications or websites or systems.

TOP 10 2021

A01 2021: Broken Access Control

A02 2021: Cryptographic Failures

A03 2021: Injections

A04 2021: Insecure Design

A05 2021: Security Misconfiguration

A06 2021: Vulnerable and Outdated Components

A07 2021: Identification and Authentication Failures

A08 2021: Software and Data Integrity Failures

A09 2021: Security Logging and Monitoring Failures

A10 2021: Server-side Request Forgery

A01 2021: Broken Access Control

List of mapped CWEs

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CWE-23 Relative Path Traversal

CWE-35 Path Traversal: '.../...//'

CWE-59 Improper Link Resolution Before File Access ('Link Following')

CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CWE-201 Exposure of Sensitive Information Through Sent Data

CWE-219 Storage of File with Sensitive Data Under Web Root

CWE-264 Permissions, Privileges, and Access Controls (should no longer be used)

CWE-275 Permission Issues

CWE-276 Incorrect Default Permissions

CWE-284 Improper Access Control

CWE-285 Improper Authorization

CWE-352 Cross-Site Request Forgery (CSRF)

CWE-359 Exposure of Private Personal Information to an Unauthorized Actor

CWE-377 Insecure Temporary File

CWE-402 Transmission of Private Resources into a New Sphere ('Resource Leak')

CWE-425 Direct Request ('Forced Browsing')

CWE-441 Unintended Proxy or Intermediary ('Confused Deputy')

CWE-497 Exposure of Sensitive System Information to an Unauthorized Control Sphere

CWE-538 Insertion of Sensitive Information into Externally-Accessible File or Directory

CWE-540 Inclusion of Sensitive Information in Source Code

CWE-548 Exposure of Information Through Directory Listing

CWE-552 Files or Directories Accessible to External Parties

CWE-566 Authorization Bypass Through User-Controlled SQL Primary Key

CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CWE-639 Authorization Bypass Through User-Controlled Key

CWE-651 Exposure of WSDL File Containing Sensitive Information

CWE-668 Exposure of Resource to Wrong Sphere

CWE-706 Use of Incorrectly-Resolved Name or Reference

CWE-862 Missing Authorization

CWE-863 Incorrect Authorization

CWE-913 Improper Control of Dynamically-Managed Code Resources

CWE-922 Insecure Storage of Sensitive Information

CWE-1275 Sensitive Cookie with Improper SameSite Attribute

CWE-219 Storage of File with Sensitive Data Under Web Root

Description: The product stores sensitive data under the web document root with insufficient access control, which might make it accessible to untrusted parties.

Business Impact: The file where the sensitive data is stored is not secured enough and can be accessed by unauthorized parties. The unauthorized or untrusted adversaries can breach the data and gain access to confidential information. They might modified it and this might impact the customer's trust for the organization. This can lead to unauthorized access, data breach, regulatory compliance violations, loss of intellectual property, impact on customer trust, financial impact, operational disruption, negative publicity, reputational damage, litigation and legal liabilities.

A02 2021: Cryptographic Failures

List of mapped CWEs

CWE-261 Weak Encoding for Password

CWE-296 Improper Following of a Certificate's Chain of Trust

CWE-310 Cryptographic Issues

CWE-319 Cleartext Transmission of Sensitive Information

CWE-321 Use of Hard-coded Cryptographic Key

CWE-322 Key Exchange without Entity Authentication

CWE-323 Reusing a Nonce, Key Pair in Encryption

CWE-324 Use of a Key Past its Expiration Date

CWE-325 Missing Required Cryptographic Step

CWE-326 Inadequate Encryption Strength

CWE-327 Use of a Broken or Risky Cryptographic Algorithm

CWE-328 Reversible One-Way Hash

CWE-329 Not Using a Random IV with CBC Mode

CWE-330 Use of Insufficiently Random Values

CWE-331 Insufficient Entropy

CWE-335 Incorrect Usage of Seeds in Pseudo-Random Number Generator(PRNG)

CWE-336 Same Seed in Pseudo-Random Number Generator (PRNG)

CWE-337 Predictable Seed in Pseudo-Random Number Generator (PRNG)

CWE-338 Use of Cryptographically Weak Pseudo-Random Number Generator(PRNG)

CWE-340 Generation of Predictable Numbers or Identifiers

CWE-347 Improper Verification of Cryptographic Signature

CWE-523 Unprotected Transport of Credentials

CWE-720 OWASP Top Ten 2007 Category A9 - Insecure Communications

CWE-757 Selection of Less-Secure Algorithm During Negotiation('Algorithm Downgrade')

CWE-759 Use of a One-Way Hash without a Salt

CWE-760 Use of a One-Way Hash with a Predictable Salt

CWE-780 Use of RSA Algorithm without OAEP

CWE-818 Insufficient Transport Layer Protection

CWE-916 Use of Password Hash With Insufficient Computational Effort

CWE-319 Cleartext Transmission of Sensitive Information

Description: The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

Business Impact: Password can be easily figured out by the untrusted adversaries as it is in cleartext and not encrypted. It may lead to data exposure and compromise sensitive data. The hacker might use the credential and act as the user to do unethical stuff. This will put the blame on the victim and not the actual perpetrator.

A03 2021: Injections

List of mapped CWEs

CWE-20 Improper Input Validation

CWE-74 Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

CWE-75 Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

CWE-83 Improper Neutralization of Script in Attributes in a Web Page

CWE-87 Improper Neutralization of Alternate XSS Syntax

CWE-88 Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')

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

CWE-90 Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')

CWE-91 XML Injection (aka Blind XPath Injection)

CWE-93 Improper Neutralization of CRLF Sequences ('CRLF Injection')

CWE-94 Improper Control of Generation of Code ('Code Injection')

CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')

CWE-96 Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')

CWE-97 Improper Neutralization of Server-Side Includes (SSI) Within a Web Page

CWE-98 Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

CWE-99 Improper Control of Resource Identifiers ('Resource Injection')

CWE-100 Deprecated: Was catch-all for input validation issues

CWE-113 Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')

CWE-116 Improper Encoding or Escaping of Output

CWE-138 Improper Neutralization of Special Elements

CWE-184 Incomplete List of Disallowed Inputs

CWE-470 Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')

CWE-471 Modification of Assumed-Immutable Data (MAID)

CWE-564 SQL Injection: Hibernate

CWE-610 Externally Controlled Reference to a Resource in Another Sphere

CWE-643 Improper Neutralization of Data within XPath Expressions ('XPath Injection')

CWE-644 Improper Neutralization of HTTP Headers for Scripting Syntax

CWE-652 Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')

CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language 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: The data can be meddled or modified in between by the sql injection and the data that was intended to send to the receiver will not be the original. This can cause misunderstandings between the receiver and sender. If the two parties are reputed organizations, then it will impact on their business relations. It makes prone to man-in-the-middle vulnerability.

A04 2021: Insecure Design

List of mapped CWEs

CWE-73 External Control of File Name or Path

CWE-183 Permissive List of Allowed Inputs

CWE-209 Generation of Error Message Containing Sensitive Information

CWE-213 Exposure of Sensitive Information Due to Incompatible Policies

CWE-235 Improper Handling of Extra Parameters

CWE-256 Unprotected Storage of Credentials

CWE-257 Storing Passwords in a Recoverable Format

CWE-266 Incorrect Privilege Assignment

CWE-269 Improper Privilege Management

CWE-280 Improper Handling of Insufficient Permissions or Privileges

CWE-311 Missing Encryption of Sensitive Data

CWE-312 Cleartext Storage of Sensitive Information

CWE-313 Cleartext Storage in a File or on Disk

CWE-316 Cleartext Storage of Sensitive Information in Memory

CWE-419 Unprotected Primary Channel

CWE-430 Deployment of Wrong Handler

CWE-434 Unrestricted Upload of File with Dangerous Type

CWE-444 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

CWE-451 User Interface (UI) Misrepresentation of Critical Information

CWE-472 External Control of Assumed-Immutable Web Parameter

CWE-501 Trust Boundary Violation

CWE-522 Insufficiently Protected Credentials

CWE-525 Use of Web Browser Cache Containing Sensitive Information

CWE-539 Use of Persistent Cookies Containing Sensitive Information

CWE-579 J2EE Bad Practices: Non-serializable Object Stored in Session

CWE-598 Use of GET Request Method With Sensitive Query Strings

CWE-602 Client-Side Enforcement of Server-Side Security

CWE-642 External Control of Critical State Data

CWE-646 Reliance on File Name or Extension of Externally-Supplied File

CWE-650 Trusting HTTP Permission Methods on the Server Side

CWE-653 Insufficient Compartmentalization

CWE-656 Reliance on Security Through Obscurity

CWE-657 Violation of Secure Design Principles

CWE-799 Improper Control of Interaction Frequency

CWE-807 Reliance on Untrusted Inputs in a Security Decision

CWE-840 Business Logic Errors

CWE-841 Improper Enforcement of Behavioral Workflow

CWE-927 Use of Implicit Intent for Sensitive Communication

CWE-1021 Improper Restriction of Rendered UI Layers or Frames

CWE-1173 Improper Use of Validation Framework

CWE-451 User Interface (UI) Misrepresentation of Critical Information

Description: The user interface (UI) does not properly represent critical information to the user, allowing the information - or its source - to be obscured or spoofed. This is often a component in phishing attacks.

Business Impact: Hackers can exploit the vulnerable holes in the UI and use the victim's data as ransom. They can access the information of the victim through the website's database. This can impact the relation between the customer and organisation. It can lead to , litigation and legal liabilities.

A05 2021: Security Misconfiguration

List of mapped CWEs

CWE-2 7PK - Environment

CWE-11 ASP.NET Misconfiguration: Creating Debug Binary

CWE-13 ASP.NET Misconfiguration: Password in Configuration File

CWE-15 External Control of System or Configuration Setting

CWE-16 Configuration

CWE-260 Password in Configuration File

CWE-315 Cleartext Storage of Sensitive Information in a Cookie

CWE-520 .NET Misconfiguration: Use of Impersonation

CWE-526 Exposure of Sensitive Information Through Environmental Variables

CWE-537 Java Runtime Error Message Containing Sensitive Information

CWE-541 Inclusion of Sensitive Information in an Include File

CWE-547 Use of Hard-coded, Security-relevant Constants

CWE-611 Improper Restriction of XML External Entity Reference

CWE-614 Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

CWE-756 Missing Custom Error Page

CWE-776 Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')

CWE-942 Permissive Cross-domain Policy with Untrusted Domains

CWE-1004 Sensitive Cookie Without 'HttpOnly' Flag

CWE-1032 OWASP Top Ten 2017 Category A6 - Security Misconfiguration

CWE-1174 ASP.NET Misconfiguration: Improper Model Validation

CWE-315 Cleartext Storage of Sensitive Information in a Cookie

Description: The product stores sensitive information in cleartext in a cookie.

Business Impact: Cookies are small text sent by the website to user's browser so as to remember that the user visited the site. If sensitive information gets stored on the cookie then anyone can access it as it is available to everyone through the website. On top of that, if its cleartext then it won't need any decrypting key to read and alter the data. This can damage the user's data and can make them vulnerable to more exploitations.

A06 2021: Vulnerable and Outdated Components

List of mapped CWEs

CWE-937 OWASP Top 10 2013: Using Components with Known Vulnerabilities

CWE-1035 2017 Top 10 A9: Using Components with Known Vulnerabilities

CWE-1104 Use of Unmaintained Third Party Components

CWE-1104 Use of Unmaintained Third Party Components

Description: The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

Business Impact: If the third party components are not maintained, then the third party adversaries can exploit the customer's data and put the blame on the original organisation. This will cause reputational damage of the original organisation but also put the user's data at risk.

A07 2021: Identification and Authentication Failures

List of mapped CWEs

CWE-255 Credentials Management Errors

CWE-259 Use of Hard-coded Password

CWE-287 Improper Authentication

CWE-288 Authentication Bypass Using an Alternate Path or Channel

CWE-290 Authentication Bypass by Spoofing

CWE-294 Authentication Bypass by Capture-replay

CWE-295 Improper Certificate Validation

CWE-297 Improper Validation of Certificate with Host Mismatch

CWE-300 Channel Accessible by Non-Endpoint

CWE-302 Authentication Bypass by Assumed-Immutable Data

CWE-304 Missing Critical Step in Authentication

CWE-306 Missing Authentication for Critical Function

CWE-307 Improper Restriction of Excessive Authentication Attempts

CWE-346 Origin Validation Error

CWE-384 Session Fixation

CWE-521 Weak Password Requirements

CWE-613 Insufficient Session Expiration

CWE-620 Unverified Password Change

CWE-640 Weak Password Recovery Mechanism for Forgotten Password

CWE-798 Use of Hard-coded Credentials

CWE-940 Improper Verification of Source of a Communication Channel

CWE-1216 Lockout Mechanism Errors

A08 2021: Software and Data Integrity Failures

List of mapped CWEs

CWE-345 Insufficient Verification of Data Authenticity

CWE-353 Missing Support for Integrity Check

CWE-426 Untrusted Search Path

CWE-494 Download of Code Without Integrity Check

CWE-502 Deserialization of Untrusted Data

CWE-565 Reliance on Cookies without Validation and Integrity Checking

CWE-784 Reliance on Cookies without Validation and Integrity Checking in a Security Decision

CWE-829 Inclusion of Functionality from Untrusted Control Sphere

CWE-830 Inclusion of Web Functionality from an Untrusted Source

CWE-915 Improperly Controlled Modification of Dynamically-Determined Object Attributes

A09 2021: Security Logging and Monitoring Failures

List of mapped CWEs

CWE-117 Improper Output Neutralization for Logs

CWE-223 Omission of Security-relevant Information

CWE-532 Insertion of Sensitive Information into Log File

CWE-778 Insufficient Logging

A10 2021: Server-side Request Forgery

List of mapped CWEs

CWE-918 Server-Side Request Forgery (SSRF)