|  |
| --- |
| **CONTEXTO Y DESCRIPCION DE LA PRACTICA** |
| * **Toda aplicación/sistema puede tener fallos que pueden ser explotados, pero detectar y corregir esos errores/fallos no es tarea simple.** * **Existen diferentes organismos/empresas que se dedican a detectar y plantear soluciones a las vulnerabilidades que se van detectando** * **Las Vulnerabilidades y exposiciones comunes ( Common Vulnerabilities and Exposures, siglas CVE), es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene:**   + **Un número de identificación CVE-ID (CVE-AÑO-XXXX).**   + **Descripción de la vulnerabilidad.**   + **Que versiones del software están afectadas.**   + **Posible solución al fallo (si existe) o como configurar para mitigar la vulnerabilidad.**   + **Referencias a publicaciones o entradas de foros o blog donde se ha hecho pública la vulnerabilidad o se demuestra su explotación.** * **La corporación Mitre y el instituto SANS, junto con otros expertos mundiales, mantienen el sistema de categorías CWE (Common Weakness Enumeration) que cataloga las diversas vulnerabilidades. Las categorías para CWE van desde todo, como el estándar de codificación SEI CERT Oracle para Java, hasta debilidades sin patrones de fallas de software. Afortunadamente, la taxonomía, la organización y la accesibilidad de las categorías tienen una clasificación muy alta. Ver https://cwe.mitre.org/top25** * **Entre los muchos proyectos que tiene OWASP uno de los más importantes es la divulgación de los 10 riesgos web más importantes en la actualidad. Ver** [**https://owasp.org/www-project-top-ten/**](https://owasp.org/www-project-top-ten/)   **Dicho proyecto pública cada 4 años los 10 riegos web más importantes** |

**PARTE 1: Broken Access Control (Rotura Del Control De Acceso). Ver https://owasp.org/Top10/A01\_2021-Broken\_Access\_Control/**

1. Explica con tus palabras qué consecuencias tiene esta vulnerabilidad

|  |
| --- |
| Esta vulnerabilidad permite a un usuario acceder a un archivo para el cual no debería tener permiso. Esto puede tener consecuencias en la confidencialidad, integridad y disponibilidad del archivo, ya que el usuario podría tener permiso para leer, modificar y borrar el archivo respectivamente. |

1. Indica todas las categorías CWE incluye

|  |
| --- |
| Esta vulnerabilidad está incluida en un total de 34 CWE distintas.  Son las siguientes:  [CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')](https://cwe.mitre.org/data/definitions/22.html)  [CWE-23 Relative Path Traversal](https://cwe.mitre.org/data/definitions/23.html)  [CWE-35 Path Traversal: '.../...//'](https://cwe.mitre.org/data/definitions/35.html)  [CWE-59 Improper Link Resolution Before File Access ('Link Following')](https://cwe.mitre.org/data/definitions/59.html)  [CWE-200 Exposure of Sensitive Information to an Unauthorized Actor](https://cwe.mitre.org/data/definitions/200.html)  [CWE-201 Exposure of Sensitive Information Through Sent Data](https://cwe.mitre.org/data/definitions/201.html)  [CWE-219 Storage of File with Sensitive Data Under Web Root](https://cwe.mitre.org/data/definitions/219.html)  [CWE-264 Permissions, Privileges, and Access Controls (should no longer be used)](https://cwe.mitre.org/data/definitions/264.html)  [CWE-275 Permission Issues](https://cwe.mitre.org/data/definitions/275.html)  [CWE-276 Incorrect Default Permissions](https://cwe.mitre.org/data/definitions/276.html)  [CWE-284 Improper Access Control](https://cwe.mitre.org/data/definitions/284.html)  [CWE-285 Improper Authorization](https://cwe.mitre.org/data/definitions/285.html)  [CWE-352 Cross-Site Request Forgery (CSRF)](https://cwe.mitre.org/data/definitions/352.html)  [CWE-359 Exposure of Private Personal Information to an Unauthorized Actor](https://cwe.mitre.org/data/definitions/359.html)  [CWE-377 Insecure Temporary File](https://cwe.mitre.org/data/definitions/377.html)  [CWE-402 Transmission of Private Resources into a New Sphere ('Resource Leak')](https://cwe.mitre.org/data/definitions/402.html)  [CWE-425 Direct Request ('Forced Browsing')](https://cwe.mitre.org/data/definitions/425.html)  [CWE-441 Unintended Proxy or Intermediary ('Confused Deputy')](https://cwe.mitre.org/data/definitions/441.html)  [CWE-497 Exposure of Sensitive System Information to an Unauthorized Control Sphere](https://cwe.mitre.org/data/definitions/497.html)  [CWE-538 Insertion of Sensitive Information into Externally-Accessible File or Directory](https://cwe.mitre.org/data/definitions/538.html)  [CWE-540 Inclusion of Sensitive Information in Source Code](https://cwe.mitre.org/data/definitions/540.html)  [CWE-548 Exposure of Information Through Directory Listing](https://cwe.mitre.org/data/definitions/548.html)  [CWE-552 Files or Directories Accessible to External Parties](https://cwe.mitre.org/data/definitions/552.html)  [CWE-566 Authorization Bypass Through User-Controlled SQL Primary Key](https://cwe.mitre.org/data/definitions/566.html)  [CWE-601 URL Redirection to Untrusted Site ('Open Redirect')](https://cwe.mitre.org/data/definitions/601.html)  [CWE-639 Authorization Bypass Through User-Controlled Key](https://cwe.mitre.org/data/definitions/639.html)  [CWE-651 Exposure of WSDL File Containing Sensitive Information](https://cwe.mitre.org/data/definitions/651.html)  [CWE-668 Exposure of Resource to Wrong Sphere](https://cwe.mitre.org/data/definitions/668.html)  [CWE-706 Use of Incorrectly-Resolved Name or Reference](https://cwe.mitre.org/data/definitions/706.html)  [CWE-862 Missing Authorization](https://cwe.mitre.org/data/definitions/862.html)  [CWE-863 Incorrect Authorization](https://cwe.mitre.org/data/definitions/863.html)  [CWE-913 Improper Control of Dynamically-Managed Code Resources](https://cwe.mitre.org/data/definitions/913.html)  [CWE-922 Insecure Storage of Sensitive Information](https://cwe.mitre.org/data/definitions/922.html)  [CWE-1275 Sensitive Cookie with Improper SameSite Attribute](https://cwe.mitre.org/data/definitions/1275.html) |

1. Indica cómo se puede mitigar

|  |
| --- |
| Podemos mitigar esta vulnerabilidad con las siguientes reglas:   * Utilizar denegación de acceso por defecto para todos los usuarios excepto para los archivos públicos y para los únicos usuarios requeridos. * Limitar la velocidad de acceso a la API para evitar ataques automatizados. * Deshabilitar el listado de archivos del servidor web. * Eliminar los metadatos de los archivos del servidor web.   Entre otras. |

1. Busca 5 ejemplos CVE

|  |
| --- |
| CVE que sufren de Broken Access Control son: CVE-2024-22234 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22234CVE-2023-47327 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47327CVE-2023-47325 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47325CVE-2023-47320 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47320CVE-2023-38880 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38880 Todos ocurridos en el transcurso del último año. |

**PARTE 2: Crytographic Failures (fallo de cifrado)** **Ver https://owasp.org/Top10/A02\_2021-Cryptographic\_Failures/**

1. Explica con tus palabras qué consecuencias tiene esta vulnerabilidad

|  |
| --- |
| Esta vulnerabilidad permite obtener datos que en principio deberían estar cifrados con criptografía. Estp puede tener consecuencias desastrosas, ya que permitiría descubrir las contraseñas, datos bancarios o datos médicos de los usuarios; hasta secretos de Estado dependiendo de la información que se esté |

1. Indica todas las categorías CWE incluye

|  |
| --- |
| Incluye un total de 29 categorías CWE. Estas son:  [CWE-261 Weak Encoding for Password](https://cwe.mitre.org/data/definitions/261.html)  [CWE-296 Improper Following of a Certificate's Chain of Trust](https://cwe.mitre.org/data/definitions/296.html)  [CWE-310 Cryptographic Issues](https://cwe.mitre.org/data/definitions/310.html)  [CWE-319 Cleartext Transmission of Sensitive Information](https://cwe.mitre.org/data/definitions/319.html)  [CWE-321 Use of Hard-coded Cryptographic Key](https://cwe.mitre.org/data/definitions/321.html)  [CWE-322 Key Exchange without Entity Authentication](https://cwe.mitre.org/data/definitions/322.html)  [CWE-323 Reusing a Nonce, Key Pair in Encryption](https://cwe.mitre.org/data/definitions/323.html)  [CWE-324 Use of a Key Past its Expiration Date](https://cwe.mitre.org/data/definitions/324.html)  [CWE-325 Missing Required Cryptographic Step](https://cwe.mitre.org/data/definitions/325.html)  [CWE-326 Inadequate Encryption Strength](https://cwe.mitre.org/data/definitions/326.html)  [CWE-327 Use of a Broken or Risky Cryptographic Algorithm](https://cwe.mitre.org/data/definitions/327.html)  [CWE-328 Reversible One-Way Hash](https://cwe.mitre.org/data/definitions/328.html)  [CWE-329 Not Using a Random IV with CBC Mode](https://cwe.mitre.org/data/definitions/329.html)  [CWE-330 Use of Insufficiently Random Values](https://cwe.mitre.org/data/definitions/330.html)  [CWE-331 Insufficient Entropy](https://cwe.mitre.org/data/definitions/331.html)  [CWE-335 Incorrect Usage of Seeds in Pseudo-Random Number Generator(PRNG)](https://cwe.mitre.org/data/definitions/335.html)  [CWE-336 Same Seed in Pseudo-Random Number Generator (PRNG)](https://cwe.mitre.org/data/definitions/336.html)  [CWE-337 Predictable Seed in Pseudo-Random Number Generator (PRNG)](https://cwe.mitre.org/data/definitions/337.html)  [CWE-338 Use of Cryptographically Weak Pseudo-Random Number Generator(PRNG)](https://cwe.mitre.org/data/definitions/338.html)  [CWE-340 Generation of Predictable Numbers or Identifiers](https://cwe.mitre.org/data/definitions/340.html)  [CWE-347 Improper Verification of Cryptographic Signature](https://cwe.mitre.org/data/definitions/347.html)  [CWE-523 Unprotected Transport of Credentials](https://cwe.mitre.org/data/definitions/523.html)  [CWE-720 OWASP Top Ten 2007 Category A9 - Insecure Communications](https://cwe.mitre.org/data/definitions/720.html)  [CWE-757 Selection of Less-Secure Algorithm During Negotiation('Algorithm Downgrade')](https://cwe.mitre.org/data/definitions/757.html)  [CWE-759 Use of a One-Way Hash without a Salt](https://cwe.mitre.org/data/definitions/759.html)  [CWE-760 Use of a One-Way Hash with a Predictable Salt](https://cwe.mitre.org/data/definitions/760.html)  [CWE-780 Use of RSA Algorithm without OAEP](https://cwe.mitre.org/data/definitions/780.html)  [CWE-818 Insufficient Transport Layer Protection](https://cwe.mitre.org/data/definitions/818.html)  [CWE-916 Use of Password Hash With Insufficient Computational Effort](https://cwe.mitre.org/data/definitions/916.html) |

1. Indica cómo se puede mitigar

|  |
| --- |
| Podemos mitigar esta vulnerabilidad con las siguientes reglas:   * No utilizar métodos no seguros como HTTP, FTP o SMTP para transportar datos confidenciales. * No almacenar datos confidenciales que no vayamos a utilizar. Los datos de los que no dispongamos no se pueden robar. * Deshabilitar el almacenamiento en caché para respuestas que contengan datos personales. * Almacenar todas las contraseñas utilizando funciones de hash lo más potentes posibles.   Entre otras. |

1. Busca 5 ejemplos CVE

|  |
| --- |
| Algunos CVE que sufren de Cryptographic Failures son: CVE-2022-20866 <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20866>CVE-2021-4239 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4239CVE-2021-20305 <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20305>CVE-2021-32032 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32032CVE-2018-1000808 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000808 |

**PARTE 3: Injection (inyección) https://owasp.org/Top10/A03\_2021-Injection/**

■ Sql Injection

■ Cross-Site scripting (XSS)

1. Explica con tus palabras qué consecuencias tiene esta vulnerabilidad

|  |
| --- |
| Esta vulnerabilidad permite la ejecución de código. Por ejemplo, se puede inyectar código SQL para modificar o leer las bases de datos a las que no se debería poder tener acceso.  Esto puede tener consecuencias en todas las dimensiones de la seguridad, ya que se podría leer, modificar y borrar la información afectada. |

1. Indica todas las categorías CWE incluye

|  |
| --- |
| Incluye un total de 33 categorías CWE. Estas son:  [CWE-20 Improper Input Validation](https://cwe.mitre.org/data/definitions/20.html)  [CWE-74 Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')](https://cwe.mitre.org/data/definitions/74.html)  [CWE-75 Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)](https://cwe.mitre.org/data/definitions/75.html)  [CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')](https://cwe.mitre.org/data/definitions/77.html)  [CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')](https://cwe.mitre.org/data/definitions/78.html)  [CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')](https://cwe.mitre.org/data/definitions/79.html)  [CWE-80 Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)](https://cwe.mitre.org/data/definitions/80.html)  [CWE-83 Improper Neutralization of Script in Attributes in a Web Page](https://cwe.mitre.org/data/definitions/83.html)  [CWE-87 Improper Neutralization of Alternate XSS Syntax](https://cwe.mitre.org/data/definitions/87.html)  [CWE-88 Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')](https://cwe.mitre.org/data/definitions/88.html)  [CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')](https://cwe.mitre.org/data/definitions/89.html)  [CWE-90 Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')](https://cwe.mitre.org/data/definitions/90.html)  [CWE-91 XML Injection (aka Blind XPath Injection)](https://cwe.mitre.org/data/definitions/91.html)  [CWE-93 Improper Neutralization of CRLF Sequences ('CRLF Injection')](https://cwe.mitre.org/data/definitions/93.html)  [CWE-94 Improper Control of Generation of Code ('Code Injection')](https://cwe.mitre.org/data/definitions/94.html)  [CWE-95 Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')](https://cwe.mitre.org/data/definitions/95.html)  [CWE-96 Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')](https://cwe.mitre.org/data/definitions/96.html)  [CWE-97 Improper Neutralization of Server-Side Includes (SSI) Within a Web Page](https://cwe.mitre.org/data/definitions/97.html)  [CWE-98 Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')](https://cwe.mitre.org/data/definitions/98.html)  [CWE-99 Improper Control of Resource Identifiers ('Resource Injection')](https://cwe.mitre.org/data/definitions/99.html)  [CWE-100 Deprecated: Was catch-all for input validation issues](https://cwe.mitre.org/data/definitions/100.html)  [CWE-113 Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')](https://cwe.mitre.org/data/definitions/113.html)  [CWE-116 Improper Encoding or Escaping of Output](https://cwe.mitre.org/data/definitions/116.html)  [CWE-138 Improper Neutralization of Special Elements](https://cwe.mitre.org/data/definitions/138.html)  [CWE-184 Incomplete List of Disallowed Inputs](https://cwe.mitre.org/data/definitions/184.html)  [CWE-470 Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')](https://cwe.mitre.org/data/definitions/470.html)  [CWE-471 Modification of Assumed-Immutable Data (MAID)](https://cwe.mitre.org/data/definitions/471.html)  [CWE-564 SQL Injection: Hibernate](https://cwe.mitre.org/data/definitions/564.html)  [CWE-610 Externally Controlled Reference to a Resource in Another Sphere](https://cwe.mitre.org/data/definitions/610.html)  [CWE-643 Improper Neutralization of Data within XPath Expressions ('XPath Injection')](https://cwe.mitre.org/data/definitions/643.html)  [CWE-644 Improper Neutralization of HTTP Headers for Scripting Syntax](https://cwe.mitre.org/data/definitions/644.html)  [CWE-652 Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')](https://cwe.mitre.org/data/definitions/652.html)  [CWE-917 Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')](https://cwe.mitre.org/data/definitions/917.html) |

1. Indica cómo se puede mitigar

|  |
| --- |
| Podemos mitigar esta vulnerabilidad con las siguientes reglas:   * Validar la entrada de datos en todas las direcciones para las páginas y aplicaciones que no requieran utilizar caracteres especiales. * Escapar todos los caracteres especiales utilizados es el código. * Utilizar LIMIT y otros controles SQL dentro de las consultas para evitar la divulgación masiva de registros en caso de inyección SQL. * Utilizar APIs seguras en lugar de utilizar un intérprete completo.   Entre otras. |

1. Busca 5 ejemplos CVE

|  |
| --- |
| CVE que sufren de Injection son: CVE-2024-27515 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-27515CVE-2024-26470 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26470CVE-2024-26260 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26260CVE-2024-25928 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-25928CVE-2024-25722 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-25722 Todos ellos ocurridos en el transcurso de 2024. |

**PARTE 4: Insecure Design (diseño inseguro) https://owasp.org/Top10/A04\_2021-Insecure\_Design/**

1. Explica con tus palabras qué consecuencias tiene esta vulnerabilidad

|  |
| --- |
|  |

1. Indica todas las categorías CWE incluye

|  |
| --- |
|  |

1. Indica cómo se puede mitigar

|  |
| --- |
|  |

1. Busca 5 ejemplos CVE

|  |
| --- |
|  |

**PARTE 5: Security Misconfiguration (configuración errónea de seguridad) https://owasp.org/Top10/A05\_2021-Security\_Misconfiguration/**

■ XML External Entities (XXE)

1. Explica con tus palabras qué consecuencias tiene esta vulnerabilidad

|  |
| --- |
|  |

1. Indica todas las categorías CWE incluye

|  |
| --- |
|  |

1. Indica cómo se puede mitigar

|  |
| --- |
|  |

1. Busca 5 ejemplos CVE

|  |
| --- |
|  |

**PARTE 6: Vulnerable and Outdated Components (componentes vulnerables o desactualizados) https://owasp.org/Top10/A06\_2021-Vulnerable\_and\_Outdated\_Components/**

1. Explica con tus palabras qué consecuencias tiene esta vulnerabilidad

|  |
| --- |
|  |

1. Indica todas las categorías CWE incluye

|  |
| --- |
|  |

1. Indica cómo se puede mitigar

|  |
| --- |
|  |

1. Busca 5 ejemplos CVE

|  |
| --- |
|  |

**PARTE 7: Identification and Authentication Failures (Broken Authentication): fallos de identificación y autorización https://owasp.org/Top10/A07\_2021-Identification\_and\_Authentication\_Failures/**

1. Explica con tus palabras qué consecuencias tiene esta vulnerabilidad

|  |
| --- |
|  |

1. Indica todas las categorías CWE incluye

|  |
| --- |
|  |

1. Indica cómo se puede mitigar

|  |
| --- |
|  |

1. Busca 5 ejemplos CVE

|  |
| --- |
|  |

**PARTE 8: Software and Data Integrity Failures (fallos de integridad de software y de datos) https://owasp.org/Top10/A08\_2021-Software\_and\_Data\_Integrity\_Failures/**

■ Insecure Deserialization

1. Explica con tus palabras qué consecuencias tiene esta vulnerabilidad

|  |
| --- |
|  |

1. Indica todas las categorías CWE incluye

|  |
| --- |
|  |

1. Indica cómo se puede mitigar

|  |
| --- |
|  |

1. Busca 5 ejemplos CVE

|  |
| --- |
| Ejemplo CVE-2010-0467 |

**PARTE 9: Security Logging and Monitoring Failures (fallos de seguridad de monitorización y log) https://owasp.org/Top10/A09\_2021-Security\_Logging\_and\_Monitoring\_Failures/**

1. Explica con tus palabras qué consecuencias tiene esta vulnerabilidad

|  |
| --- |
|  |

1. Indica todas las categorías CWE incluye

|  |
| --- |
|  |

1. Indica cómo se puede mitigar

|  |
| --- |
|  |

1. Busca 5 ejemplos CVE

|  |
| --- |
|  |

**PARTE 10: Server-Side Request Forgery (falsificación de solicitudes del lado del servidor). https://owasp.org/Top10/A10\_2021-Server-Side\_Request\_Forgery\_%28SSRF%29/**

1. Explica con tus palabras qué consecuencias tiene esta vulnerabilidad

|  |
| --- |
|  |

1. Indica todas las categorías CWE incluye

|  |
| --- |
|  |

1. Indica cómo se puede mitigar

|  |
| --- |
|  |

1. Busca 5 ejemplos CVE

|  |
| --- |
|  |