PUESTA EN PRODUCCIÓN SEGURA

Práctica OWASP Top 10 Web

Parte 4 del Proyecto

(19-04-2024)

Rubén de la Viuda Redondo

Ciberseguridad

Índice

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.

2. 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')
- 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

3. 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.

4. Busca 5 ejemplos CVE

CVE que sufren de esta vulnerabilidad son:

- CVE-2024-22234: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-22234
- CVE-2023-47327: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47327
- CVE-2023-47325: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47325
- CVE-2023-47320: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-47320
- CVE-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. Esto 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 tratando.

2. Indica todas las categorías CWE incluye:

Incluye un total de 29 categorías CWE. Estas son:

- 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

3. 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.

4. Busca 5 ejemplos CVE

Algunos CVE que sufren de esta vulnerabilidad 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-2021-4239
- CVE-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-2021-32032
- CVE-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/:

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.

2. Indica todas las categorías CWE incluye:

Incluye un total de 33 categorías CWE. Estas son:

- 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')

3. 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.

4. Busca 5 ejemplos CVE

CVE que sufren de esta vulnerabilidad son:

- CVE-2024-27515 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-27515
- CVE-2024-26470 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26470
- CVE-2024-26260 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-26260
- CVE-2024-25928 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-25928
- CVE-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:

El diseño inseguro se basa en una mal diseño base de una aplicación, produciendo problemas de arreglo de errores, dificultades de securización y problemas de seguridad. No es la razón de la existencia del resto de vulnerabilidades, ay que no es lo mismo un diseño inseguro qué una implementación segura.

2. Indica todas las categorías CWE incluye:

Incluye un total de 40 categorías CWE. Estas son:

- 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

3. Indica cómo se puede mitigar:

Para mitigarlo es importante concienciar de la seguridad a los desarrolladores, además de facilitar su implementación añadiendo cosas como un ciclo de vida del desarrollo, dónde se analicen las necesidades, la implementación, el método de desarrollo, la estructura, etc...

4. Busca 5 ejemplos CVE

CVE que sufren de esta vulnerabilidad son:

- CVE-2019-6260
- CVE-2007-5277
- CVE-2006-7142
- CVE-2007-0408
- CVE-2021-43076

PARTE 5: Security Misconfiguration (configuración errónea de seguridad) https://owasp.org/Top10/A05_2021-Security_Misconfiguration/:

1. Explica con tus palabras qué consecuencias tiene esta vulnerabilidad:

Esta vulnerabilidad se basa en el aprovechamiento de errores de configuración, permisos, servicios en la aplicación o funcionalidades innecesarias en la aplicación. Las vulnerabilidades más comunes de este tipo son:
Uso de usuario y contraseñas por defecto, errores que muestran partes del código o demasiado informativos, falta de directivas seguras en servidores, software desactualizado y funciones innecesarias.

2. Indica todas las categorías CWE incluye:

Incluye un total de 20 categorías CWE. Estas son:

- 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

3. Indica cómo se puede mitigar:

Crear un proceso seguro de desarrollo repetible, de forma que al producir un sistema de forma segura, el resto sea un “clonado” de la configuración, siendo imposible que se nos olvide algún ajuste, crear una plataforma mínima de funcionalidades, para evitar agujeros de seguridad innecesarios, y crear una aplicación segmentada, separando las distintas funciones de la aplicación.

4. Busca 5 ejemplos CVE

CVE que sufren de esta vulnerabilidad son:

- CVE-2023-25768
- CVE-2023-25767
- CVE-2023-25766
- CVE-2023-25765
- CVE-2023-25764

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:

Esta vulnerabilidad consiste en tener componente inseguros en tu aplicación debido a problemas de seguridad en versiones desactualizadas de los mismos, haciendo que un aplicación seguro tenga agujeros por el uso de componentes con vulnerabilidades zero-day o de otro tipo.

2. Indica todas las categorías CWE incluye:

Incluye un total de 3 categorías CWE. Estas son:

- 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

3. Indica cómo se puede mitigar:

Para mitigarlo es importante tener un listado de dependencias y versiones usados por la aplicación, optención de los componentes de sitios oficiales para evitar vulnerabilidades y monitorizar componentes para saber si tienen alguna vulnerabilidad nueva y saber si aquellos no mantenidos son seguros el día de mañana.

4. Busca 5 ejemplos CVE

CVE que sufren de esta vulnerabilidad son:

- CVE-2022-21476
- CVE-2022-2900
- CVE-2022-35914
- CVE-2018-17890
- CVE-2021-44228

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:

Esta vulnerabilidad puede tener una serie de consecuencias graves como el acceso no autorizado, el robo de identidad, la fuga de información confidencial, daño a la reputación o incumplimiento normativo no deseado. En resumen, estas vulnerabilidades tienen un impacto en la seguridad de la aplicación y también puede afectar a la confianza de los usuarios en la misma.

2. Indica todas las categorías CWE incluye:

Incluye un total de 22 categorías CWE. Estas son:

- CWE-255
- CWE-259
- CWE-287
- CWE-288
- CWE-290
- CWE-294
- CWE-295
- CWE-297
- CWE-300
- CWE-302
- CWE-304
- CWE-306
- CWE-307
- CWE-346
- CWE-384
- CWE-521
- CWE-613
- CWE-620
- CWE-640
- CWE-798
- CWE-940
- CWE-1216

3. Indica cómo se puede mitigar:

Se puede mitigar mediante métodos de autenticación seguros como contraseñas robustas y autenticación de dos factores, además de proteger contra fuerza bruta y diccionarios. Aparte se deben gestionar de manera correcta las sesiones de usuario, educar a los usuarios sobre prácticas seguras y realizar pruebas de seguridad regulares.

4. Busca 5 ejemplos CVE

CVE que sufren de esta vulnerabilidad son:

- CVE-2019-11510
- CVE-2020-1472
- CVE-2020-10189
- CVE-2021-3156
- CVE-2021-3449

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/:

1. Explica con tus palabras qué consecuencias tiene esta vulnerabilidad:

Las consecuencias que tiene esta vulnerabilidad pueden ser: pérdida o corrupción de datos, ejecución de código malicioso, alteración de la funcionalidad, pérdida de confianza o incumplimiento normativo.

2. Indica todas las categorías CWE incluye:

Incluye un total de 10 categorías CWE. Estas son:

- CWE-345
- CWE-353
- CWE-426
- CWE-494
- CWE-502
- CWE-565
- CWE-784
- CWE-829
- CWE-830
- CWE-915

3. Indica cómo se puede mitigar:

Se puede mitigar aplicando varias medidas: validación de entrada de datos, control de acceso adecuado, firmas digitales y hashes, actualizaciones y parches, monitoreo y detección de intrusiones, copias de seguridad regulares.

4. Busca 5 ejemplos CVE

CVE que sufren de esta vulnerabilidad son:

- CVE-2017-0143
- CVE-2018-11776
- CVE-2019-0708
- CVE-2020-0601
- CVE-2021-34527

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:

Puede tener consecuencias significativas en la capacidad de detectar y responder amenazas de seguridad, aparte de otras como la detección inadecuada de ataques, dificultad para realizar investigaciones forenses, retrasos en la respuesta a incidentes, incapacidad para cumplir con requisitos regulatorios y pérdida en la confianza del cliente.

2. Indica todas las categorías CWE incluye:

Incluye un total de 4 categorías CWE. Estas son:

- CWE-117
- CWE-223
- CWE-532
- CWE-778

3. Indica cómo se puede mitigar:

Para mitigar estas vulnerabilidades hay que implementar una estrategia integral que incluya la generación de registros de seguridad y el uso de herramientas avanzadas de monitorización, establecer políticas claras de recopilación y la implementación de soluciones tecnológicas como detección de intrusiones y gestión de evento de seguridad.

4. Busca 5 ejemplos CVE

CVE que sufren de esta vulnerabilidad son:

- CVE-2019-11510
- CVE-2020-1472
- CVE-2019-0725
- CVE-2019-8917
- CVE-2020-6287

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:

Las consecuencias de esta vulnerabilidad son graves ya que se pueden enviar solicitudes desde el servidor a recursos internos o externos de la red, alguna consecuencia sería el acceso no autorizado a recursos internos, ataques contra servicios internos, exposición de datos sensibles y credenciales, exfiltración de datos y escalada de privilegios.

2. Indica todas las categorías CWE incluye:

Solo incluye una categoría CWE. Esta es:

- CWE-918

3. Indica cómo se puede mitigar:

Implementando una estricta validación de entradas de usuario, filtrar URLs mediante listas blancas, imitar los recursos y protocolos accesibles desde el servidor, utilizar firewalls o proxies para controlar el trafico.

4. Busca 5 ejemplos CVE

CVE que sufren de esta vulnerabilidad son:

- CVE-2019-0232
- CVE-2019-10092
- CVE-2020-1967
- CVE-2021-26084
- CVE-2021-21972