

Informe de gestión de incidentes conforme a la norma ISO 27001: vulnerabilidad de inyección SQL

Introducción

-Este informe expone una vulnerabilidad encontrada en la web Damn Vulnerable Web Application (DVWA), en la que se detecta y explota una vulnerabilidad de inyección SQL. Esta prueba se ha realizado en un entorno seguro para demostrar dicha vulnerabilidad y su posible impacto en la seguridad de la aplicación.

Descripción del incidentes


-Durante la evaluación de seguridad de DVWA, se descubrió una vulnerabilidad de inyección SQL en el módulo "Inyección SQL". Esta vulnerabilidad permite a un atacante inyectar consultas SQL maliciosas a través de los campos de entrada de la aplicación web, comprometiendo así la integridad y confidencialidad de los datos almacenados en la base de datos.

Proceso de reproducción

-Para replicar y demostrar la vulnerabilidad, se accedió a la sección SQL Injection, y en el campo de User ID se cargo lo siguiente:

`1' OR '1'='1`

-Esta carga aprovecha la vulnerabilidad para ver la lista de todos los usuarios extraídos de la base de datos, indicando una inyección SQL exitosa como se aprecia en la siguiente imagen.



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Vulnerability: SQL Injection

User ID:

ID: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: Me

ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1
First name: Bob
Surname: Smith

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

Impacto del incidentes

-Esta vulnerabilidad podría permitir a un atacante:

-Acceder y extraer información confidencial de la base de datos, incluidas las credenciales de usuario.

-Modificar, eliminar o comprometer datos confidenciales almacenados en la aplicación.

-Esto representa un riesgo significativo para la confidencialidad, integridad y disponibilidad de los datos y servicios proporcionados por DVWA.

Recomendaciones

-En base a los resultados obtenidos en esta evaluación de seguridad, se recomiendan las siguientes medidas correctivas y preventivas:

1. Validación de entrada: Implementar validaciones de entrada estrictas para todos los datos proporcionados por el usuario, utilizando parámetros seguros en las consultas SQL para evitar la inyección de SQL.

2. Pruebas de penetración: Realizar auditorías de seguridad periódicas, incluyendo pruebas de penetración, para identificar y mitigar las vulnerabilidades de seguridad antes de que sean explotadas por atacantes.

3. Formación y concienciación: Capacitar al personal técnico y no técnico en prácticas seguras de desarrollo de aplicaciones y concientizar sobre los riesgos asociados a las vulnerabilidades de seguridad.

Conclusión

-Gracias a la identificación de la vulnerabilidad de inyección SQL en DVWA, nos reafirma la importancia de la seguridad proactiva en el desarrollo y mantenimiento de aplicaciones web. Al implementar controles de seguridad robustos y seguir las mejores prácticas de ciberseguridad, nos ayuda a la correcta protección de activos críticos y garantiza la continuidad del negocio.