Titulo del Report: SQL injection

Intodrucción:

El ataque de SQL explota la falta de validación de entradas en una consulta SQL. Este ataque funciona 1 OR 1 = 1 siempre se evalúa como verdadero, lo que permite al atacante acceder a datos no autorizados o incluso no comprometer la base de datos.

Descripción del incidente:

Tipo de ataque: SQL injection.

Payload: 1 OR 1 =1.

Objetivo: Bypass de autenticación o extracción de datos.

Processo de Reproducción:

1- Accede a la pagina de inicio de sesión

2- En el campo de nombre de ususario, ingresa admin.

3- En el campo contraseña ingresa 1 OR 1 = 1

4- Haz clic en botón de iniciar sesión.

5- Observa que el sistema permite el acceso sin validar correctamente las credenciales.

Impacto del incidente:

Acceso no autorizado a cuentas

Posible exposición de datos sensibles

Recomendaciones:

Usar firewall de aplicaciones web(WAF).

Implementar consultas parametrizadas.

Validar y sanitizar las entradas del usuario.

Conclusión:

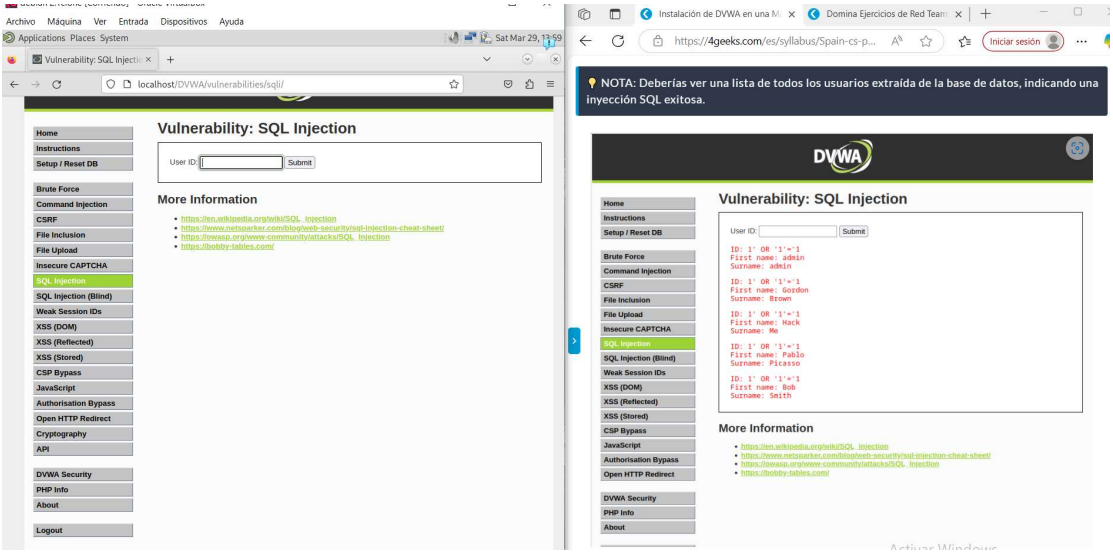
The identification and successful exploitation of the SQL injection vulnerability in DVWA underscores

the importance of proactive security in the development and maintenance of web applications.

Implementing robust security controls and following best cybersecurity practices are essential to

protect critical assets and ensure business continuity.

Implementar medidas robustas de controle de seguridad y seguir buenas practicas y mantenimiento de sanitización del desarrollo WEB son esenciales para la seguridad.


Archivo Máquina Ver Entrada Dispositivos Ayuda
Applications Places System
Sat Mar 29, 13:59
Vulnerability: SQL Injectic
localhost/DVWA/vulnerabilities/sqli/
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
Cryptography
API
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
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/
Instalación de DVWA en una M
Domina Ejercicios de Red Team
https://4geeks.com/es/syllabus/Spain-cs-p...
Iniciar sesión
NOTA: Deberías ver una lista de todos los usuarios extraída de la base de datos, indicando una inyección SQL exitosa.
DVWA
Vulnerability: SQL Injection
User ID:
Submit
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/