Reporte de Gestión de Incidentes conforme a ISO 27001 - Vulnerabilidad de Inyección SQL en DVWA

Introducción

Este reporte documenta la identificación y explotación de una vulnerabilidad de inyección SQL en la aplicación web DVWA, probada en un entorno controlado para demostrar su impacto potencial en la seguridad de aplicaciones.

Descripción del Incidente

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

Método de Inyección SQL Usado

Se utilizó el siguiente payload en el campo "User ID":
1' OR '1'='1. Este código explota la vulnerabilidad para modificar la consulta SQL original, obteniendo sin autorización la lista de los usuarios registrados.

Impacto del Incidente

Explotar esta vulnerabilidad podría permitir a un atacante:

- **Confidencialidad**: Acceder y extraer información confidencial de la base de datos, incluyendo credenciales de usuario, datos de carácter confidencial o críticos.
- **Integridad:** Modificar, eliminar o comprometer datos sensibles almacenados en la aplicación.
- **Disponibilidad:** el atacante podría afectar la disponibilidad del sistema se si realiza una modificación extensa en la base de datos o si se eliminan datos esenciales

Recomendaciones

Se sugieren las siguientes medidas correctivas y preventivas:

1. **Validación de Entrada:**
    1. Asegurar que todos los datos ingresados por el usuario sean validados y filtrados para prevenir inyecciones SQL

    2. Utilizar consultas parametrizadas para prevenir modificaciones no autorizadas a las consultas SQL originales

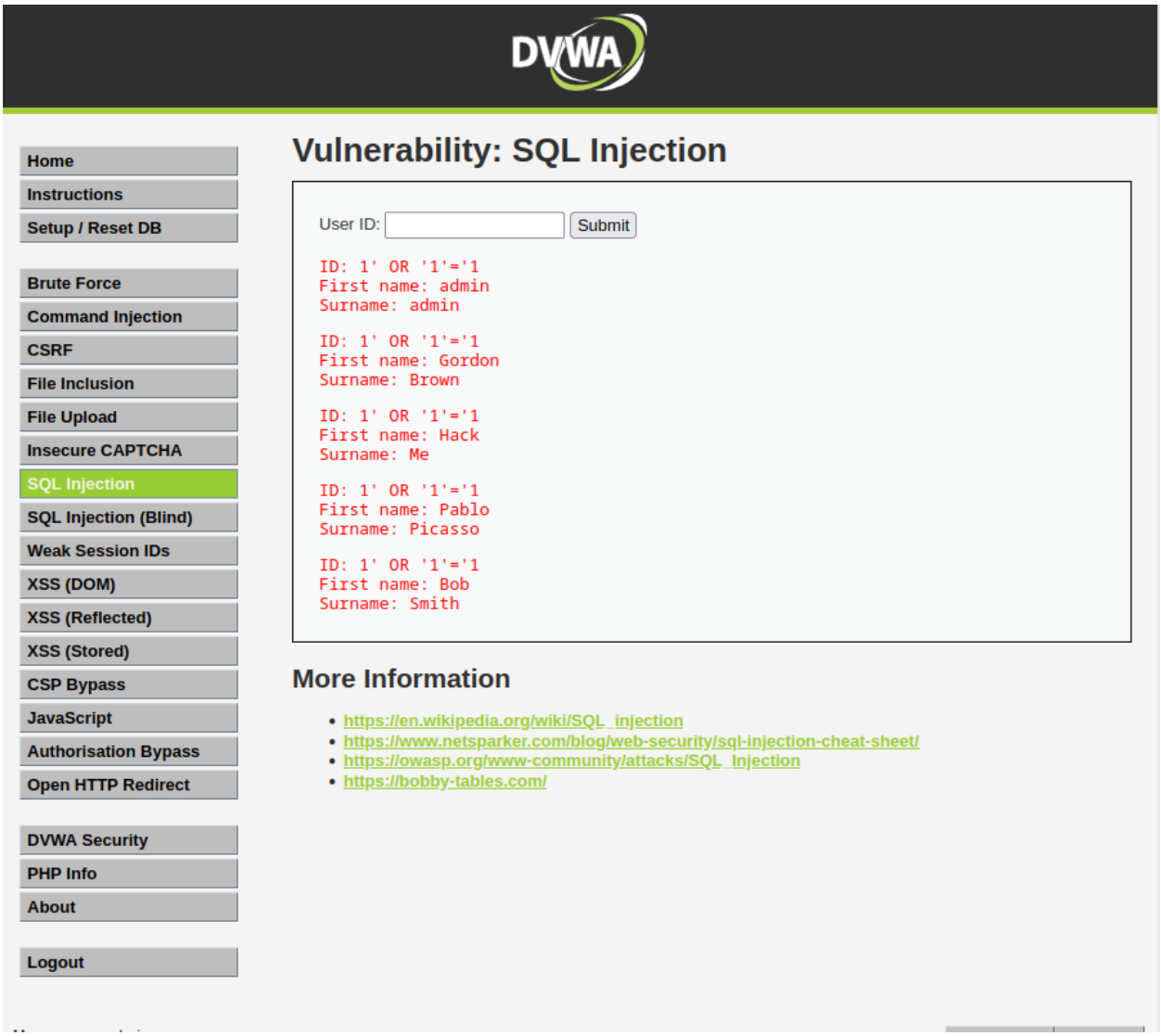
2. **Pruebas de Penetración:** Realizar auditorías regulares para identificar vulnerabilidades potenciales y mitigarlas antes de que puedan ser explotadas
3. **Capacitación y Concienciación:**
    1. Capacitar a desarrolladores y equipo técnico en practicas seguras de desarrollo, con énfasis en la prevención de inyecciones SQL.
    2. Generar concienciación en el personal no técnico sobre los riesgos asociados con la seguridad de la información.

Conclusión

1. La vulnerabilidad de inyección SQL detectada en DVWA destaca la importancia de implementar medidas de seguridad proactivas en aplicaciones web
2. Con la aplicación de controles de seguridad adecuados y la capacitación continu, las organizaciones pueden mitigar los riesgos de seguridad y proteger sus datos críticos, asegurando la continuidad del negocio y la confianza del usuario.

Apendice

Resultados de la prueba controlada en DVWA


DVWA
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
Logout
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/