Carlos Ordoñez

Reporte de Gestión de Incidentes según ISO 27001

Título: Vulnerabilidad de Inyección SQL en Damn Vulnerable Web Application (DVWA)

Introducción

Este reporte documenta la identificación y explotación de una vulnerabilidad de inyección SQL en la aplicación web Damn Vulnerable Web Application (DVWA). La prueba se realizó en un entorno controlado con el propósito de demostrar cómo una vulnerabilidad común puede comprometer la seguridad de una aplicación y el impacto potencial sobre la integridad y confidencialidad de los datos almacenados.

Descripción del Incidente

Durante una evaluación de seguridad realizada en el módulo "SQL Injection" de DVWA, se identificó una vulnerabilidad que permite a un atacante inyectar consultas SQL maliciosas a través de los campos de entrada de la aplicación web. Esta vulnerabilidad compromete la integridad de las consultas ejecutadas en la base de datos y expone datos confidenciales almacenados en la misma.

Proceso de Reproducción

Para demostrar la vulnerabilidad, se utilizó el siguiente payload SQL en el campo User ID de DVWA:

```
1' OR '1'='1
```

Este payload modifica la consulta SQL original, lo que permite recuperar todos los registros de la tabla users en lugar de solo el usuario especificado por el campo User ID. Al ejecutar este ataque, DVWA mostró una lista de todos los usuarios almacenados en la base de datos, lo que confirma que la vulnerabilidad es explotable.

Resultados observados:

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

Carlos Ordoñez

Surname: Me

ID: 1' OR '1'='1

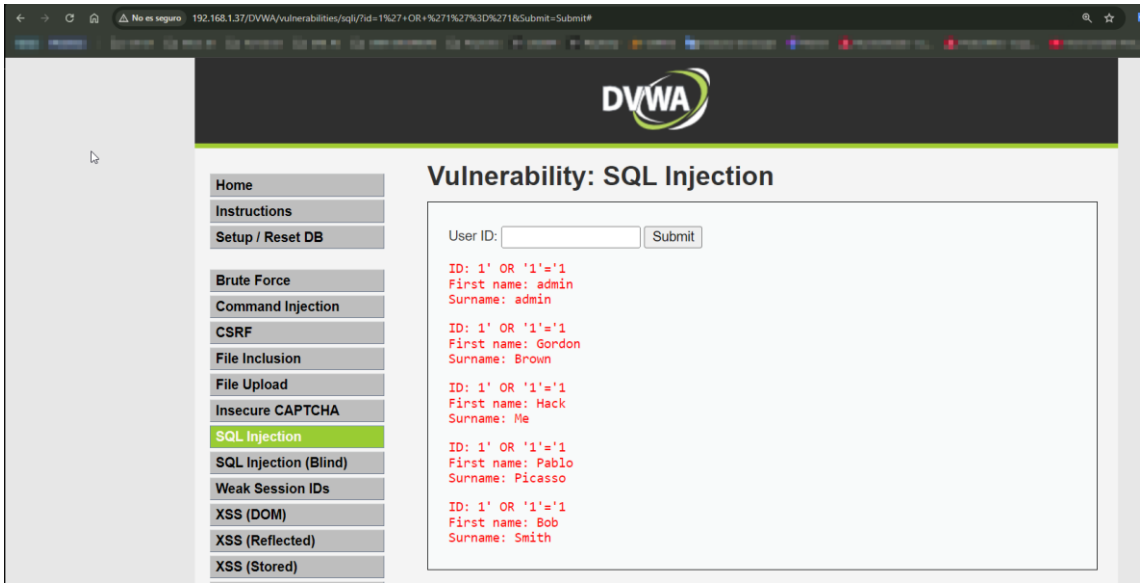
First name: Pablo

Surname: Picasso

ID: 1' OR '1'='1

First name: Bob

Surname: Smith



Esto confirma que la inyección SQL permite acceder a toda la información almacenada en la tabla users sin autorización.

Impacto del Incidente

Explotar esta vulnerabilidad de inyección SQL podría permitir a un atacante:

Acceder a información confidencial: Extraer datos sensibles, incluyendo credenciales de usuarios.

Modificar o eliminar datos: Comprometer la integridad de los datos almacenados.

Escalar privilegios: Utilizar credenciales obtenidas para acceder a funciones restringidas o realizar más ataques.

Esto representa un riesgo crítico para la confidencialidad, integridad y disponibilidad de la información y los servicios ofrecidos por DVWA.

Recomendaciones

Con base en los hallazgos de esta evaluación, se recomiendan las siguientes medidas preventivas y correctivas:

Validación de Entradas:

Implementar validaciones estrictas para todos los datos proporcionados por los usuarios.

Utilizar consultas SQL parametrizadas para evitar la inyección SQL.

Pruebas de Penetración:

Realizar auditorías de seguridad periódicas, incluyendo pruebas de penetración, para identificar y mitigar vulnerabilidades antes de que sean explotadas.

Educación y Concienciación:

Capacitar al personal técnico en prácticas de desarrollo seguro.

Sensibilizar a los empleados sobre los riesgos asociados a las vulnerabilidades de seguridad.

Monitoreo y Detección:

Implementar herramientas de monitoreo para detectar intentos de inyección SQL y responder rápidamente ante incidentes.

Conclusión

La identificación y explotación de esta vulnerabilidad de inyección SQL en DVWA destaca la importancia de implementar controles de seguridad proactivos en el desarrollo y mantenimiento de aplicaciones web. Adoptar mejores prácticas de ciberseguridad, como la validación de entradas y el uso de consultas parametrizadas, es esencial para proteger los activos críticos y garantizar la continuidad del negocio.