

Informe de gestión de incidentes ISO 27001

Introducción

Este reporte detalla la vulneración y la explotación del servidor DVWA usando el metodo de la inyección SQL.

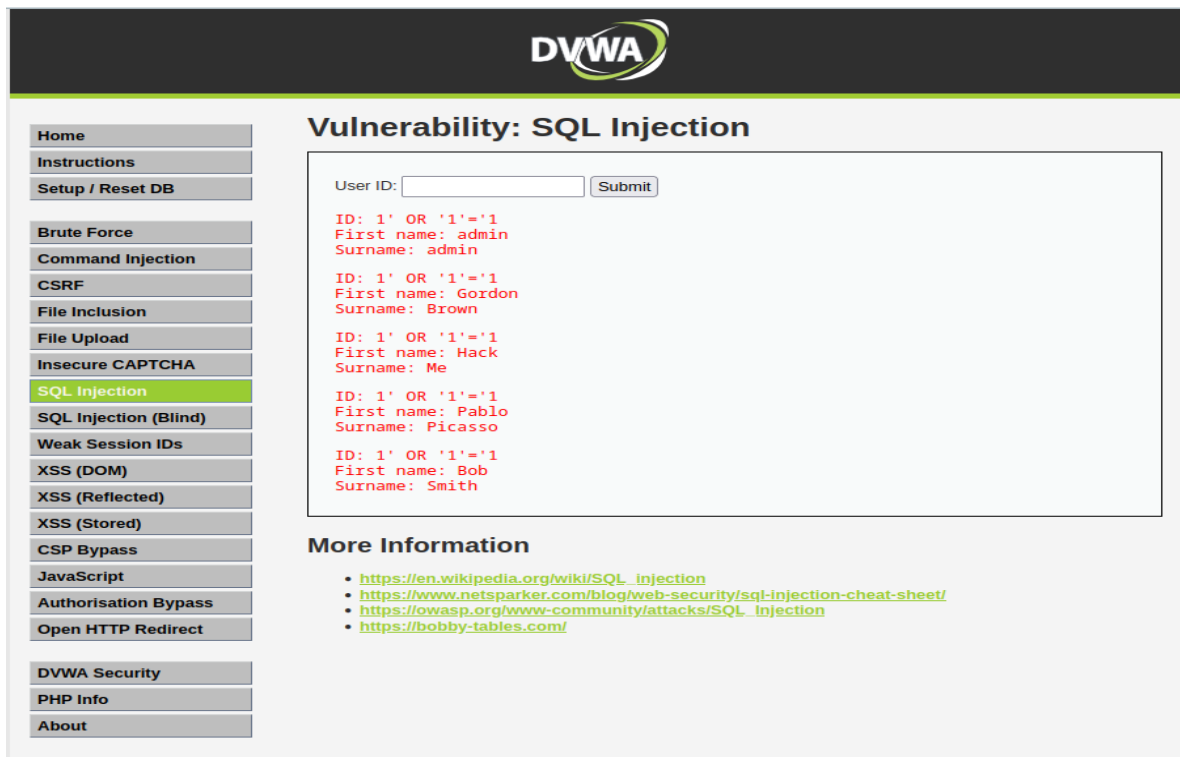
Descripción del incidente

Durante la evaluación se descubrió que un metodo de inyección SQL fue utilizado para vulnerar el servidor, la cual es una técnica de inyección de codigo malicioso.

Proceso de Reproducción

Para replicar la vulnerabilidad se utilizó el siguiente comando:

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



Este comando simple hace que DVWA procese la solicitud y muestre información de la base de datos.

Impacto del incidente

Esta inyección de código malicioso puede permitirle al hacker modificar, eliminar o incluso tomar control total del servidor.

Recomendaciones

Se debe modificar el código para se validen los input (entradas de datos) para que los usuarios no puedan ingresar una entrada incorrecta como "1' OR '1'='1" que en este caso fue utilizada de forma maliciosa para obtener información privada. También se debe aumentar el nivel de seguridad del servidor en la pestaña de Seguridad DVWA.

Conclusión

La identificación de esta explotación SQL demuestra la importancia de validar los input en el servidor e implementar medidas de seguridad mas estrictas para proteger el servidor, también demuestra la importancia de capacitar al personal en contra de estos ataques.