

INFORME DE AUDITORIA INTERNA

INFORME DE AUDITORIA AL SERVIDOR DVWA CON BASE A LA NORMA ISO 27001

OCTUBRE 25 DE 2024

4GEEKS ACADEMY

1 INTRODUCCIÓN

1.1 Objeto de la auditoría

Identificar la seguridad proporcionada por el servidor DVWA ante un ataque de SQL injection.

1.2 Alcance de auditoría

El alcance de la auditoría está definido a todo lo relacionado del servidor DVWA y sus posibles configuraciones para un ataque SQL injection.

1.3 Fecha de la auditoría

Las actividades de auditoría fueron ejecutadas el día 24 de octubre del 2024.

1.4 Lugar

Las actividades de auditoría tomaron lugar en la academia 4geeks.

1.5 Áreas auditadas

Se auditaron todas las áreas relacionadas con el servidor DVWA.

1.6 Equipo auditor

La auditoría fue ejecutada por el auditor Mauricio Piscitelli

DESCRIPCIÓN DEL INCIDENTE

Se nos ha informado que existen fugas de información a través del servidor DVWA en el que se mantiene la base de datos de los clientes de forma confidencial. El incidente ocurre al ejecutar código malicioso inyectado a través del SQL.

REPRODUCCIÓN DEL INCIDENTE

Se configuró un servidor DVWA en un ambiente controlado virtual con el backup realizado del original. Se probaron varios métodos para vulnerarlo, sin embargo, solo el SQL injection fue efectivo. En la barra de búsqueda de ID se colocó la expresión **1' OR '1'='1** lo que ocasionó un retorno de la tabla de SQL con todos los datos de los clientes y del administrador.

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

IMPACTO DEL INCIDENTE

El impacto es crítico y muy elevado, debido a que el atacante tiene acceso a toda la información de la base de datos y se podría ocasionar el robo de identidad o de información con fin malicioso. Además de violar la CIA del servidor.

RECOMENDACIONES

Se recomienda para prevenir futuros ataques de SQL injection:

- ❖ Restringir los procedimientos y código de la base de datos.
- ❖ Validar y sanear las entradas de base de datos.
- ❖ Implementar el acceso con menos privilegios.

Estas recomendaciones se presentan para realizarlas con orden inmediata debido al elevado impacto de la vulnerabilidad.

CONCLUSIÓN

Se concluye que el servidor DVWA de 4geeks sufre una vulnerabilidad de impacto elevado y crítico (SQL injection). Se deben tomar medidas inmediatas para evitar la ruptura del CIA de la información, estas medidas se describen en las recomendaciones.