



TALLER DE FUNDAMENTACION
CURSO AVANZADO DE HACKING ETICO
TECNICAS AVANZADAS DE ATAQUE Y DEFENSA.
TALLER - VULNERABILIDADES WEB

EJERCICIO 1

Una vulnerabilidad SQL Injection se produce por:

- a) Un fallo en la configuración el firewall.
- b) Un fallo en la aplicación que construye las consultas.
- c) Un fallo en la configuración de la base de datos.
- d) Un fallo en el filtrado de los parámetros en el navegador.

EJERCICIO 2

¿En qué consiste un ataque SQL Injection Inboud?

- a) La inyección SQL se produce dentro de una consulta.
- b) Los resultados de la consulta se obtienen de la página HTML de respuesta.
- c) La inyección SQL se realiza de fuera hacia dentro.
- d) El firewall permite realiza la inserción de los resultados en la consulta SQL.

EJERCICIO 3

¿Qué es un ataque a ciegas?

- a) Una inyección en la que el atacante no ve la consulta SQL que se construye.
- b) Un ataque en el que el tiempo de respuesta debe medirse.
- c) Un ataque en el que los resultados son inferidos ya que no se pueden ver.
- d) Una inyección en la que los parámetros están ciegos.

EJERCICIO 4

¿Cómo puede reconocerse una respuesta como True en un ataque a ciegas?

- a) Se producirá un True cuando se extraiga el ID de la base de datos por pantalla.
- b) Por identificador del proceso que genera la consulta.
- c) Por una palabra clave en la página de resultados.
- d) Por el tiempo de respuesta.

EJERCICIO 5

¿Qué es efectivo para evitar una vulnerabilidad de SQL injection?

- a) Filtrar la comilla en todas las consultas.
- b) Filtrar la comilla y el carácter de espacio.
- c) No concatenar cadenas de caracteres de comandos y parámetros.
- d) Usar un Firewall para publicar las aplicaciones web.