Reto 1 - Vulnerabilidad SQL Injection (SQLi)

Proyectos II - Ciberseguridad

2022 - 2023

Descripción

Se muestran a continuación las preguntas a las que hay que dar respuesta, así como las acciones que deberán ser realizadas.

- ¿Qué es un SQL Injection y qué tipos hay? ¿Qué es una inyección 'ciega'?
- ¿Cuáles son los pasos para explotar una inyección basada en errores?
- ¿Qué tipo de filtros se suelen poner en las aplicaciones para evitar los SQLi?
- ¿Cómo sería posible evadir filtros? Indicar un par de ejemplos
- ¿Es posible ejecutar comandos sobre una máquina o leer ficheros con un SQLi?

- Explotar una inyección SQL en DVWA y extraer información de la base de datos
- Explotar una inyección SQL y evadir los filtros de Web for Pentester
- Explotar una inyección SQL mediante la herramienta SQLmap
- Identificar una máquina vulnerable en Vulnhub e intentar resolverla

Aspectos destacados

Se muestran a continuación los aspectos a tener en cuenta durante el desarrollo del presente reto propuesto:

- Intentar entender todos los integrantes del grupo de forma conjunta la vulnerabilidad y plantearos posibles dudas.
- Repartid las tareas entre los integrantes del equipo una vez entendida la vulnerabilidad, así como que exista comunicación.
- No será necesario identificar una máquina virtual vulnerable.