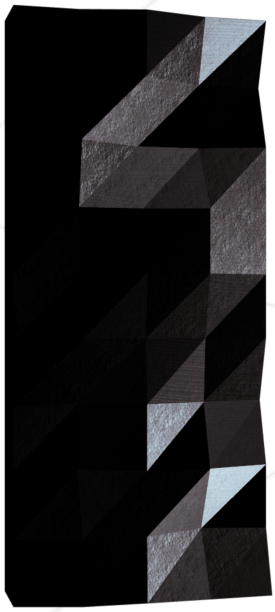

Bootcamp Ciberseguridad | 42 Madrid

Vaccine

Resumen: Inyecciones SQL y otros cuentos de terror.

Versión: 1

Índice general

Capítulo I

Introduction

Todos sabemos lo importante que es una programación segura. En este caso intentarás localizar `errores de filtrado en la entrada de datos`. Se le llama `SQL Injection` a la inyección de comandos SQL para alterar el comportamiento de un programa y ejecutar comandos sobre la base de datos. En este proyecto crearás una herramienta que sea capaz de detectar inyecciones SQL al proporcionar una URL.

Capítulo II

Parte Obligatoria

La herramienta debe tener una batería de pruebas para lanzar contra una URL indicada y, dependiendo de las respuestas, poder detectar inyecciones SQL. Puedes detectar el tipo de motor de base de datos para que las pruebas tengan mayor éxito (2 mínimo). Las pruebas pueden basarse en varios tipos: union, error, booleanas, tiempo e incluso a ciegas (2 mínimo).

En caso de que se confirme una web vulnerable, se pueden obtener:

- Los parámetros vulnerables.
- El payload utilizado
- Nombres de las bases de datos.
- Nombres de las tablas.
- Nombres de las columnas.
- Dump completo de la base de datos.

La herramienta deberá tener algun fichero de almacenamiento de los datos, si no existe se creará en la primera ejecución.

Nombre de función	`vaccine`
Archivos a entregar	`Código fuente del programa, Makefile y documentación en un archivo README.md`
Funciones autorizadas	
Descripción	`Detectar y realizar SQL injection`

El programa `vaccine` permitirá realizar SQL injection proporcionando una url como parámetro. Gestionarás las siguientes opciones del programa:

`./vaccine [-oP] URL`

- Opción `-o` : Archivo de almacenaje, si no se especifica se almacenará en uno por defecto.
- Opción `-X` : Tipo de petición, si no se especifica se usará GET.

Puedes utilizar cualquier lenguaje de programación, no debes usar librerías que automaticen el SQL injection.

Capítulo III

Parte Bonus

La evaluación de los bonus se hará `SI Y SOLO SI` la parte obligatoria es `PERFECTA`. De lo contrario, los bonus serán totalmente `IGNORADOS`.

Puedes mejorar tu proyecto con las siguientes características:

- Mayor rango de motores de base de datos.
- Mayor rango de métodos de inyecciones SQL.
- La herramienta permite editar varios parámetros de la petición, por ejemplo, el User-Agent.

Capítulo IV

Evaluación por pares

Este proyecto será corregido por tus compañeros. Entrega los archivos en el repositorio Git y asegúrate de que todo funciona como se espera.