CTFs Learning Path: Hacking Web

Sesión 1

SQL INJECTION

David Ramírez Acero
Carlos Freire Caballero

7 de marzo de 2023

Aula de
Ciber seguridad
y Redes

El Aula de Ciberseguridad y Redes presenta

CTFs Learning Path Hacking Web

David Ramírez Acero

Carlos Freire Caballero

Prepárate para hacer frente a todo tipo de CTFs sobre Hacking Web a través de **5 sesiones independientes** en las que ofreceremos los **conceptos clave** de esta categoría mientras resolvemos **multitud de CTFs** entre todos.

Sesión 1
SQL Injection
07/03

Sesión 2
XSS Injection
14/03

Sesión 3
Directory traversal, RFI y LFI
21/03

Sesión 4
CSRF y SSRF
28/03

Sesión 5
Repaso y ejercicios finales
11/04

Aula de Ciberseguridad y Redes

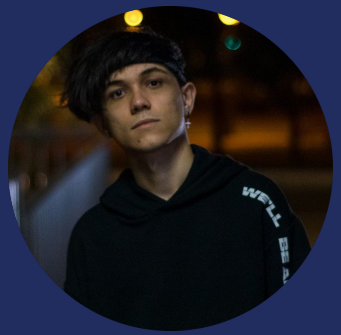
Todas las sesiones se realizarán a las **18:00** en el **aula B1 del Da Vinci**.

EL CONTENIDO DE ESTE TALLER SE IMPARTE ÚNICAMENTE CON

FINES EDUCATIVOS

HACED USO DE ESTE CONOCIMIENTO DE MANERA RESPONSABLE

QUIÉNES SOMOS



DAVID RAMÍREZ ACERO

CARLOS FREIRE CABALLERO

AULA

Aula de
Ciber seguridad
y Redes

¿Qué voy a necesitar?

- Ordenador (preferible Kali Linux).
- Estar conectado al wifi de uconet.

- Conocimientos básicos de SQL.
- Conocimientos básicos de páginas web.

¿Qué vamos a hacer?

Ataques:

- Inyección básica: obtención de datos ocultos y bypass de credenciales.
- UNION: obtención de estructura e información de varias tablas.
- Inyección a ciegas: obtención de información sin poder ver las respuestas del servidor.

¿Qué vamos a utilizar?

- La academia de PortSwigger.
- Otras plataformas CTF.

- Plataforma CTFd para las flags.

Introducción a SQL

Lenguaje de manipulación de datos de una base de datos.

Es el más usado en las bases de datos relacionales.

SQLQuery1.sql - (local)\...\shady...54))*

```
SELECT  *
FROM    Sales.SalesTerritory
```

Results | Messages

	TerritoryID	Name	CountryRegionCode	Group	SalesYTD	SalesLastYear	CostYTD	CostLastYear
1	1	Northwest	US	North America	5767341.9752	3298694.4938	0.00	0.00
2	2	Northeast	US	North America	3857163.6331	3607148.9371	0.00	0.00
3	3	Central	US	North America	4677108.269	3205014.0767	0.00	0.00
4	4	Southwest	US	North America	8351296.7411	5366575.7098	0.00	0.00
5	5	Southeast	US	North America	2851419.0435	3925071.4318	0.00	0.00
6	6	Canada	CA	North America	6917270.8842	5693988.86	0.00	0.00
7	7	France	FR	Europe	3899045.694	2396539.7601	0.00	0.00
8	8	Germany	DE	Europe	2481039.1786	1307949.7917	0.00	0.00
9	9	Australia	AU	Pacific	1977474.8096	2278548.9776	0.00	0.00
10	10	United Kingdom	GB	Europe	3514865.9051	1635823.3967	0.00	0.00

¿Por qué puede ser vulnerable?

Lenguajes de propósito general (Java, C, PHP…) formando peticiones.

Mala sanitización:

- Concatenación directa a la petición de datos de entrada por el usuario.

```
SELECT * FROM users WHERE username = 'wiener' AND password = 'bluecheese'
```

```
SELECT * FROM users WHERE username = 'administrator'--' AND password = ''
```

Revisar SQL Injection Prevention CheatSheet de OWASP.

Datos relevantes antes de empezar a atacar

- Leed la teoría de la academia de PortSwigger y preguntad lo que necesitéis.

- Empezaremos trabajando con servidores web que dan respuesta a nuestras inyecciones. En entornos reales no suele ser así.
- En los ataques a ciegas (Blind SQL) no darán respuestas explícitas.

CTF PortSwigger 1: Bypass de un login

Este ejercicio se realiza de manera guiada.

Pasos:

1. Crearos una cuenta en PortSwigger.
2. Crearos una cuenta en la plataforma CTFd: http://150.214.112.164/
3. Entrad en: https://portswigger.net/web-security/sql-injection/lab-login-bypass
4. Cuando tengáis la inyección realizada acceded a CTFd e introducidla como flag.

UNION

Obtener información de varias tablas.

Con inyecciones, permite hacer reconocimiento de las tablas.

Permite conocer el número de columnas y tipos de datos de cada una.

Blind SQL Injection

Ya no obtenemos respuestas visibles.

Formas de obtener información:

- Comprobando condicionales.
- Forzando errores de ejecución.
- Retrasos en los tiempos de carga.

Ejercicios para hacer

- PortSwigger 1: Bypass de un login. (100 puntos)
- PortSwigger 2: Inyección desde parámetro en URL. (100 puntos)
- PortSwigger 3: UNION número de columnas y tipos de datos. (100 puntos)
- PortSwigger 4: UNION obtención de la contraseña. (150 puntos)
- PortSwigger 5: Blind SQL con respuestas condicionales. (250 puntos)

- RootMe. Web - Server. SQL Injection - Authentication. (200 puntos)
- RootMe. Web - Server. SQL Injection - String. (500 puntos)
- RootMe. Web - Server. SQL Injection - Time Based. (1000 puntos)