CTFs Learning Path: Hacking Web

Sesión 3

File Related Vulnerabilities

David Ramírez Acero
Carlos Freire Caballero

21 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

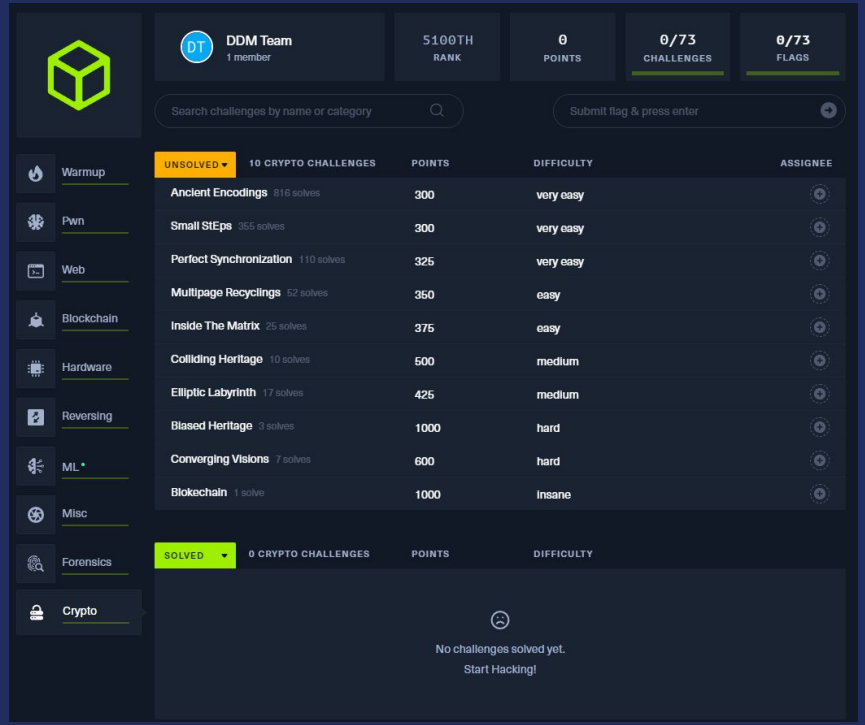
CARLOS FREIRE CABALLERO

AULA

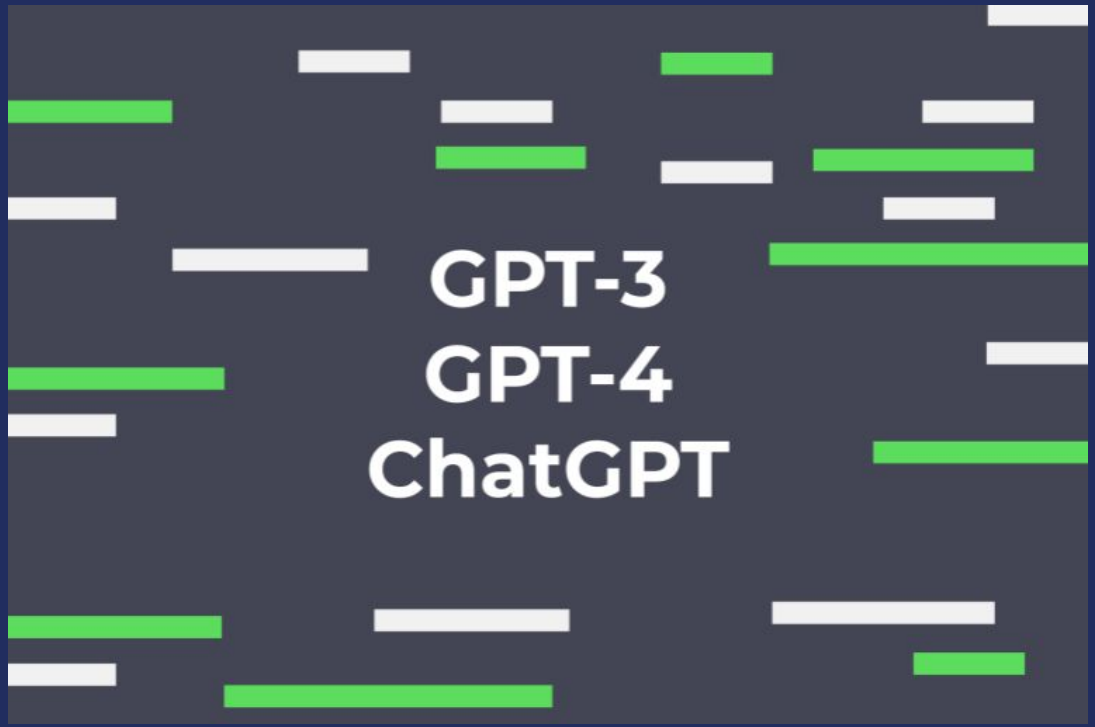
Aula de
Ciber seguridad
y Redes

Noticias

HACKTHEBOX
CYBER APOCALYPSE
THE CURSED MISSION
RESERVE YOUR SPOT
3
Hours
10
Minutes
32
Seconds
CYBER APOCALYPSE CTF 2023
THE CURSED MISSION
18th - 23rd March, 202


DDM Team
1 member
5100TH
RANK
0
POINTS
0/73
CHALLENGES
0/73
FLAGS
Search challenges by name or category
Submit flag & press enter
Warmup
Pwn
Web
Blockchain
Hardware
Reversing
ML*
Misc
Forensics
Crypto
UNSOLVED
10 CRYPTO CHALLENGES
POINTS
DIFFICULTY
ASSIGNEE
Ancient Encodings 816 solves 300 very easy
Small StEps 355 solves 300 very easy
Perfect Synchronization 110 solves 325 very easy
Multipage Recyclings 52 solves 350 easy
Inside The Matrix 25 solves 375 easy
Colliding Heritage 10 solves 500 medium
Elliptic Labyrinth 17 solves 425 medium
Biased Heritage 3 solves 1000 hard
Converging Visions 7 solves 600 hard
Blokechain 1 solve 1000 insane
SOLVED
0 CRYPTO CHALLENGES
POINTS
DIFFICULTY
No challenges solved yet.
Start Hacking!

Noticias



Repaso de las sesiones anteriores

¿Dudas?

Place	User	Score
1	Carlos Marin	2836
2	Alvaro Palacios Criado	1336
3	naibu3	1137
4	i12mocab	638
5	Txrrxs	509
6	serranito	388
7	pablo_dominguez_alcaide	168
8	Miguel Orzáez	168
9	fonti	168
10	JoaquinMateos	168

Tabla de repaso

Client-Side	Server-Side
XSS Injection	SQL Injection
DOM-based	Directory Traversal
	File Related Vulnerabilities (LFI y RFI - RCE)
-	

¿Qué voy a necesitar?

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

- Conocimientos básicos de PHP.
- Conocimientos básicos de páginas web.

¿Qué vamos a hacer?

- Movernos entre directorios y archivos usando Directory Traversal.
- Visualizar y explotar archivos internos del servidor usando LFI.
- Explotar el servidor ejecutando archivos de otro servidor usando RFI.
- Obtener ejecución remota de comandos subiendo archivos PHP.

Ataques:

- Directory Traversal.
- LFI y RFI.
- Subida de archivos para ganar RCE. Web shell.

Directory Traversal

Moverse entre directorios y archivos internos del servidor.

A partir de un parámetro se incluye un archivo que está en alguna ruta del servidor.

Por ejemplo: las imágenes de un servidor se guardan en /var/www/images.

Con ../ podría entrar en el directorio www.

?page=image.png → ?page=../

Local File Inclusion (LFI)

Permite visualizar archivos mal restringidos del servidor.

Suele ocurrir en PHP en las funciones include() y require().

?page=index.php → ?page=../../root.php

Remote File Inclusion (RFI)

Permite visualizar archivos de otros servidores.

Suele ocurrir en PHP en las funciones include() y require(). (Igual que en LFI)

?page=index.php → ?page=https://google.es

Subida de archivos

Abarcan todas las vulnerabilidades relacionadas con la subida de archivos.

Suele ocurrir cuando una página web te permite subir archivos y no filtra el tipo de archivo o la ejecución de las subidas.

Por ejemplo: se sube un archivo PHP y se guarda en una ruta del servidor web. El usuario puede entrar en esa ruta (no lo tiene restringido) y se ejecuta el PHP.

Puede llevar al establecimiento de interfaces **web shell**.

Teoría

Directory Traversal: https://portswigger.net/web-security/file-path-traversal

LFI: https://d00mfist.gitbooks.io/ctf/content/local_file_inclusion.html

RFI: https://d00mfist.gitbooks.io/ctf/content/remote_file_inclusion.html

File upload vulnerabilities: https://portswigger.net/web-security/file-upload

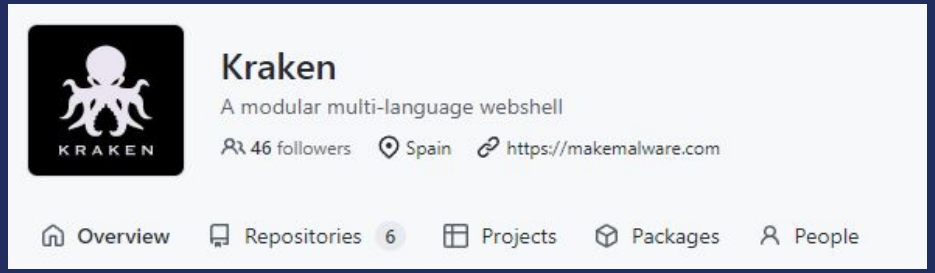
CTF PortSwigger 1: Directory Traversal simple

Este ejercicio se realiza de manera guiada.

Pasos:

1. Acceded a la plataforma CTFd: http://150.214.112.168/
2. Entrad en: https://portswigger.net/web-security/file-path-traversal/lab-simple
3. Responded la pregunta de la plataforma de CTFd.

Ejercicios extra de hoy



http://150.214.112.168:8080/

@secu_x11

Ejercicios para hacer

- PortSwigger 1. Directory Traversal simple.
- PortSwigger 2. Directory Traversal acortado.
- RootMe: LFI - 1
- Rootme: LFI - Doble codificación
- RootMe: RFI - 1
- PortSwigger 1. Ejecución remota de código subiendo archivos.
- PortSwigger 2. Ejecución remota de código vía Directory Traversal.

- Squid Game CTF. Pregunta 1.
- Squid Game CTF. Pregunta 2.