Capture The Flag: A Cybersecurity Masterclass

Master the art of hacking through competitive security challenges. Learn cryptography, reverse engineering, web exploitation, and more.

Made with GAMMA

What is Capture The Flag?

The Challenge

CTF competitions are cybersecurity challenges where participants solve puzzles and exploit vulnerabilities to capture flags—snippets of code proving successful completion.

Why Participate?

CTFs game-ify security flaws, offering hands-on learning across web exploitation, cryptography, reverse engineering, and forensics. They test real hacking skills in competitive environments.

Flag Format: CTC{F4K3_F14G}

Made with GAMMA

Your Arsenal: Kali Linux

Kali Linux is a specialized operating system designed for penetration testing and digital forensics. It provides comprehensive tools for ethical hackers and security professionals to assess system vulnerabilities and strengthen security postures.

Penetration Testing

Identify weaknesses in security systems

Digital Forensics

Analyze and recover digital evidence

Ethical Hacking

Exploit vulnerabilities responsibly

Made with GAMMA

Core Mission: Your Objectives

1 **Find Vulnerabilities**

Discover weaknesses through penetration testing and security assessments.

2 **Map Attack Surfaces**

Identify areas where sensitive data could be compromised in cyber attacks.

3 **Exploit Responsibly**

Attempt exploitations as attackers would, but within ethical boundaries.

4 **Document Everything**

Submit detailed writeups explaining your attack methodology and findings.

Made with GAMMA

Web Exploitation Fundamentals

Web exploitation involves finding and leveraging vulnerabilities in web applications to gain unauthorized access, steal data, or take control of systems. Attackers can manipulate flaws to compromise entire applications and their users.

01

View Page Source

Inspect HTML, CSS, and JavaScript to find hardcoded secrets and logic flaws.

02

Use Developer Tools

Leverage browser console, network tab, and cookie inspection to analyze requests.

03

Discover Routes

Check /robots.txt, /admin/, /api/ and use dirbuster or gobuster for hidden directories.

04

Test HTTP Requests

Use Burp Suite, Postman, or cURL to craft and analyze request-response patterns.

05

Identify Injection Flaws

Test for SQL injections and common CVEs using automated and manual techniques.

Made with GAMMA

Cryptography: Securing Information

Cryptography uses mathematics and algorithms to convert messages into difficult-to-decode formats, protecting sensitive data from unauthorized access. It ensures privacy, authenticity, and integrity in digital communications.

Symmetric Encryption

Single key for both encryption and decryption. Fast but requires secure key exchange. Examples: DES, AES.

Asymmetric Encryption

Public and private key pairs. Only private key holder decrypts. Even if public key is shared, security remains. Example: RSA.

Hash Functions

No keys used. Generate fixed-length hash values ensuring original data cannot be retrieved. Common for password protection.

Base64 Encoding

Binary-to-text encoding translating data into ASCII characters. Not encryption, but ensures compatibility across text-based channels like email.

Made with GAMMA

Reverse Engineering: Decoding Binaries

What is it?

Disassemble executable files into assembly code to understand program implementation, discover hidden functionality, and analyze how applications work without source code.

When to Use

- Binary files without source code
- Server-side applications
- Malware analysis
- Network protocol analysis

Essential Tools

Ghidra

NSA-developed decompiler with excellent analysis features

Radare2 (r2)

Lightweight disassembler and debugger framework

IDA Pro

Industry-leading interactive disassembler

Made with GAMMA

ELF Files & Reverse Engineering Techniques

What is ELF? Executable Linkable Format (ELF) is the standard format for executable files on Linux. It contains machine code, libraries, symbols, and metadata about how the program should run.

1

Identify ELF Files

Run the `file` command to confirm format. Check file headers—ELF files start with magic bytes `0x7F454C46` (ELF in hex).

2

Read ELF Files

Use `readelf`, `objdump`, and `gdb` to inspect functions, system calls, libraries, and executable structure.

3

Solve Challenges

Use r2 and ghidra to disassemble, perform file recon, analyze function calls, and employ fuzzing techniques for vulnerabilities.

Made with GAMMA

OSINT & Steganography: Hidden Intelligence

OSINT: Playing Private Eye

- Reverse image search (Google Lens, TinEye)
- Check image metadata using strings
- Search internet archives (WayBack Machine)
- Research server registrants using WHOIS
- Hunt usernames with Sherlock

Steganography Essentials

Steganography hides information within files, images, or media. Unlike cryptography, it conceals the existence of data itself. Extract hidden flags by analyzing image layers, metadata, and binary content.

Learn more at GitHub repositories for OSINT tools and techniques.

Made with GAMMA

Your Journey Begins: Next Steps

Register and Start Competing

Visit **isfcr.ctfd.io** to register, login, and attempt challenges. Your first flag: `isfcr{w3lc0me!}`

Career Opportunities Await

₹7,24,297

Information Security Tester

Design and implement security systems to safeguard networks

₹8,50,000

Network Security Engineer

Protect network infrastructures from evolving threats

$109,020

Security Architect

Design robust security structures and strategies for organizations

Data Exfiltration Successful. Valuable Skills Acquired.

Questions? Ask and we'll do our best to answer!

Made with GAMMA