# CDAC Capture The Flag (CTF) Manual

## Introduction

Capture the Flag (CTF) in computer security is an exercise in which "flags" are secretly hidden in purposefully-vulnerable programs or websites. Competitors steal flags either from other competitors (attack/defence-style CTFs) or from the organizers (jeopardy-style challenges). Several variations exist, including hiding flags in hardware devices. Competitions exist both online and in-person, and can be advanced or entry-level.

Security CTFs are usually designed to serve as an educational exercise to give participants experience in securing a machine, as well as conducting and reacting to the sort of attacks found in the real world.

Classic CTF activities include reverse-engineering, packet sniffing, protocol analysis, system administration, programming, cryptoanalysis, and writing exploits, among others. In an attack/defence style competition, each team is given a machine (or a small network) to defend—typically on an isolated competition network. Teams are scored on both their success in defending their assigned machine(s) and on their success in attacking the other team's machines. A variation from classic flag-stealing is to "plant" own flags on opponent's machines.

Hardware challenges usually involve getting an unknown piece of hardware and having to figure out how to bypass part of the security measures, e.g., using debugging ports or using a side-channel attack. Jeopardy-style competitions are closer to programming competitions: teams do not directly attack each other, but rather solve challenges posed by the organizers.

## Prerequisite Skills

In order to be successful in playing/solving **CTF** competitions, there are certain skills that you are expected to already have hands-on. These prerequisites skills are Programming, Networking, Linux-distro Basics, Windows basics, Cryptography, Exploitation, Digital forensics, and Reverse engineering.

### Programming

Programming is the first and foremost most important skill that's required to solve CTF, it's used in creating and understanding various exploits and can be used to automate things instead of doing manually. As a beginner, you must have a basic understanding of how to read syntax/program, understand how a program works and also you must know how to reverse engineer a program.

### Linux Distributions

As a pentester, you need to have an understanding of Linux Distribution and also experience with terminal and CLI (command-line interface) environments. Also, Linux comes with many advantages as open-source code, high customization, and the availability of lots of community support.

In Linux, there're many types of variations of Distros. As we're looking for a pen-testing aspect, OS like Kali Linux and Parrot Security are widely used.

## Cryptography

For cryptography, you need to have a basic idea behind the Fundamentals of cryptography like Hash functions, Symmetric-key algorithms, Asymmetric-key algorithms, Symmetric-Key Algorithms for Encryption/Decryption, etc you have to decipher texts and encrypt/decrypt texts and you need to have a good understanding of salting (passwords).

## Exploitation Techniques

**Exploitation**: A process of gaining unauthorized access by exploiting a software vulnerability or security flaw that's present in the system/application by using a chunk of data or sequence of code.

Exploits can be of various types such as binary exploitation, Web exploitation, Network exploitation, Software exploitation, etc

**Binary exploitation**: Commonly known as memory corruption, it's the process of exploiting a compiled application such that it violates some trust boundary and gives you root access in a way that is advantageous to you, the attacker.

**Web-Based Exploitation**: In web-based exploitations, there're many methods to exploit a web server. The commonly known are Cross-Site Scripting, Code Injections such as SQL Injections, CSRF attacks, XML External Entities (XEE), etc. I recommend checking out OWASP Top 10 to learn more about them.

**Network-Based Exploitation**: These are the types of Attacks used against the big organizations in an attempt to get unauthorized access or to infect their system with worms or to force their system to malfunction. Common types of Network-Based attacks are DDoS attacks, self-propagating virus, malware, spyware, worms, etc.

## Digital Forensics

Digital Forensics: A process of identifying, processing, and analysing computer-related data in order to find bugs/issues or network flaws.

To learn forensics, you need to learn how to find certain types of files, how to extract hidden information from a file. For instance, extracting data from an image using a tool called steghide, this's also known as steganography.

# Tools

In order to start in CTF competitions, we have listed some of the basic tools that you can use ordered by different challenges categories.

## WEB

**Burp suite**: Commonly used tool for testing web applications with several features one of them is burp proxy for intercepting HTTP requests.

**Cookie Editor**: useful browser extension for editing cookies.

**Postman:** send and modify API requests.

## Crypto

**rsatool**: tool used to calculate RSA and RSA-CRT parameters.

**CyberChef**: Web app for analysing and decoding data.

**PkCrack**: A tool for Breaking PkZip-encryption.

**QuipQuip**: An online tool for breaking substitution ciphers or vigenere ciphers (without key).

**XORTool**: A tool to analyse multi-byte xor ciphers.

## Digital Forensics

**ExifTool**: used for reading, writing and editing meta information in a wide variety of files (e.g., JPEG, JPG, JPE)

**Wireshark**: Tool for analysing Network traffic and PCAP files.

**Audacity**: Tool for analysing audio files (e.g. .mp3,.wav, etc).

**Foremost**: extracting files based on their headers, footers, and internal data structures.

**Stegsolve**: used for applying different techniques on images

**Volatility**:  To investigate memory dumps

## Reverse

**IDA Pro**: most used Disassembler and Debugger.

## Exploitation

**DLLInjector**: Inject dlls in processes

**libformatstr**: Simplify format string exploitation.

**Metasploit**: Penetration testing software

**one_gadget**: A tool to find the one gadget

**Pwntools**: CTF Framework for writing exploits

**Qira**: QEMU Interactive Runtime Analyser

**ROP Gadget**: Framework for ROP exploitation

**V0lt**: Security CTF Toolkit

## Android Application Analysis

**ADB:** Tool used for the debugging of Android-based devices

**Logcat:** Obtain and analyse android logs

**Genymotion:** Android emulator

**Android Studio:** Develop and Debug Android application

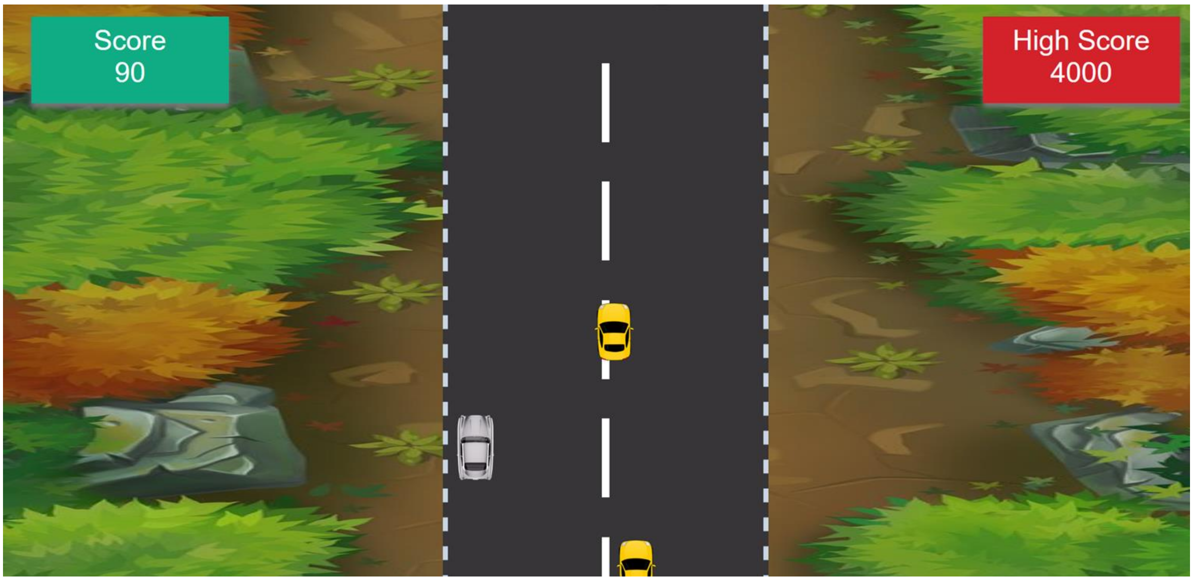
## Sample Question

### Question

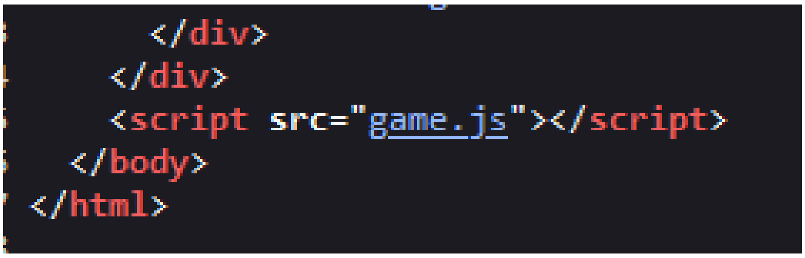
Our organization has intercepted a communication between two anti-national groups. We observed a gaming website which looks suspicious. Your task is to analyse the game and reveal the hidden message. Click Here to access the website.

### Solution

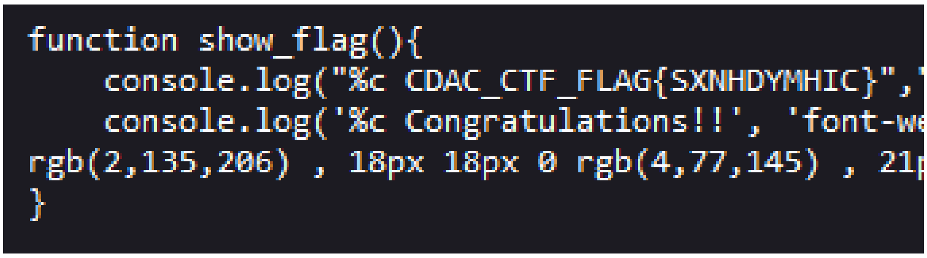
On clicking the link, a page with a car game opens.



If we view the page source there is a js file named “game.js”. On studying the JavaScript file, we get the flag.



```
      </div>
    </div>
    <script src="game.js"></script>
  </body>
</html>
```



```
function show_flag(){
    console.log("%c CDAC_CTF_FLAG{SXNHDYMHIC}",'
    console.log('%c Congratulations!!', 'font-we
rgb(2,135,206) , 18px 18px 0 rgb(4,77,145) , 21p
}
```

Flag: CDAC_CTF_FLAG{SXNHDYMHIC}

You need to submit the flag to complete the challenge.