Capture The Flag

$WHOAMI

Abishekraghav Murugeashan

Chapter Head @ OWASP Namakkal

Independent Security Researcher

Reverse engineer , Exploit Developer.

To win is passion , To loss is death </>

Agenda

- Introduction of solving the CTFs

  - ✓ Cryptography
  - ✓ Steganography
  - ✓ Forensics
  - ✓ Miscellaneous
  - ✓ Open-source intelligence
  - ✓ Reverse engineering
  - ✓ Web exploitation

CRYPTOGRAPHY

- In the case of CTFs, the goal is usually to crack or clone cryptographic objects or algorithms to reach the flag.
- There is not an format for these challenge for hiding the flags.
- It will be encrypted or decrypted too.
- You need to find that for solving the task.
- It will be couples time rotated

STEGANOGRAPHY

- In the case of CTFs, the goal is usually to extract the hidden data from an image or from a text file etc.
- The data could be hidden in any kind of file format.
- But you need understand the task before solving .
- Possible for multiple flags.

FORENSICS

- In the case of CTFs, the goal is usually to find the flags using different digital forensics patterns.
- which includes Hex values, exif data, history of a browser etc...
- You need to be very practical for solving these kinds of challenge.

MISCELLANEOUS

- In the case of CTFs, the goal is usually to find flags using different techniques like……

  => cracking the passwords of locked files

  => searching for a flag inside a file that has a lot of data etc….

- Basically Miscellaneous challenges are a mixture of all the CTF challenges.
- **Misc in CTF** is different from real-life forensics.

OSINT

- In the case of CTFs, the goal is usually to find flag using search engines and public forums etc...
- Basically it depends how good you are in recon (information gathering).
- Flag could be hidden any where on the internet.
- OSINT was the coolest part plays in the CTFs. This was the easiest and hardest part of the CTFs

REVERSE ENGINEERING

- In the case of CTFs, the goal is usually to Reverse the scenario for finding the flags.
- First necessary thing is you need to understand the function of the scenario for finding the flags.
- Mostly in the CTFs, RE plays the necessary part
- You can use the famous tools like **Immunity Debugger , OllyDBG etc…**

WEB EXPLOITATION

- *In the case of CTFs, the goal is usually to find flags using web penetration.*
- *Testing methods like XSS, SQL Injection, Robots.txt files etc.*
- *There is possible for flags anywhere in the websites.*
- *In some times you need to perform privilege escalation for the user to find the flags.*

THANK YOU!

ABISHEKRAGHAV MURUGEASHAN

@arhaxor21