Capture The Flag Workshop

How to CTF

Lars Palinckx

16 November 2022

Table of contents

INFORMATICA GROEP

Introduction to our CTF

About the CTF — Practical

Make sure to register at `https://ctf.infogroep.be`

- Max 4 players per team
- Challenges will be made available at 18h15
- Until 21h30
- Have fun!

INFORMATICA GROEP

About the CTF — What do you need?

- Laptop
  - Linux will make your life easier
  - Kali Linux best for CTFs
  - VirtualBox[1]
- Brainpower

[1] https://www.virtualbox.org/

INFORMATICA GROEP

About the CTF — General workflow

- Read the description of the challenge, there could be hints towards a possible solution
- Writing scripts: **Don't worry about ugly code**
- Use a language you are comfortable with
  - Python, Scheme, JavaScript, ...

INFORMATICA GROEP

About the CTF — Rules

Breaking any rule will result in disqualification

- Attendance is mandatory
- Do not attack the infrastructure of the CTF
  - Do not brute-force the platform!
  - If there is a brute-force challenge, we provide the file that way you can brute-force locally
- Do not attack the network
  - e.g. port scanners unless explicitly mentioned
- No cross teaming
- Have fun!

[1] `https://ctf.infogroep.be/rules`

INFORMATICA GROEP

Categories

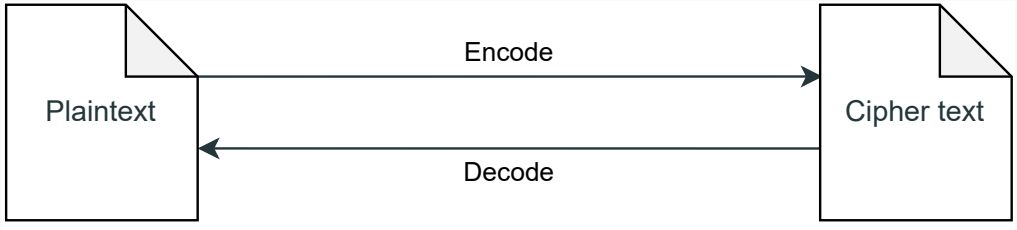
- Cryptography
  - Decoding and decrypting messages
  - Reverse engineer algorithms
- Web
  - SQL injection
  - Exploiting the network
  - Cross-site scripting
- Forensics
  - Steganography
  - Memory dumps
  - PCAP files
- Reverse engineering
  - Decompilation of machine code
- Exploitation
  - Manipulating memory
  - Stack / Buffer overflows

INFORMATICA GROEP

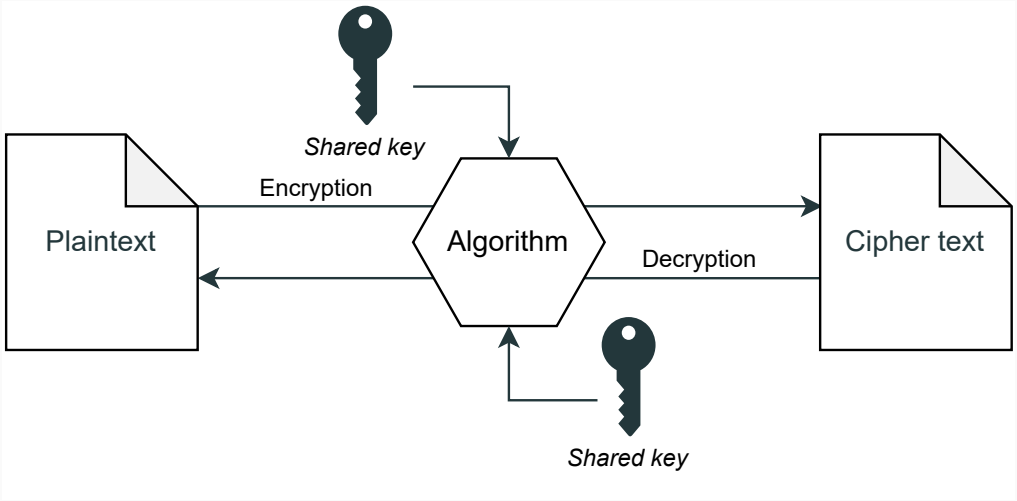
Cryptography

Cryptography — Concepts

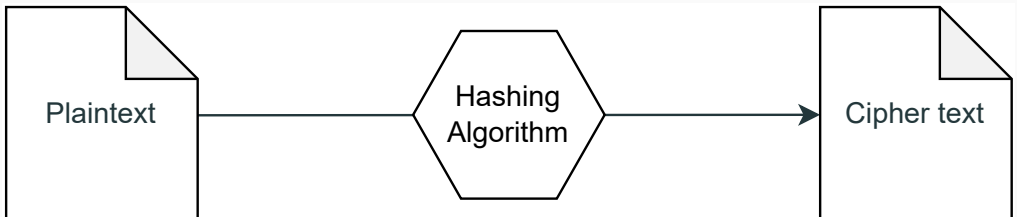
- Encoding (e.g. base64)



- Encryption (e.g. AES)



- Hashing (e.g. MD5)



INFORMATICA GROEP

Cryptography — Concepts

- Encoding (e.g. base64)

```
## Encoding
$ echo -n "IGCTF{S0meSampleFl4g}" | base64
>>> SUdDVEZ7UzBtZVNhbXBsZUZsNGd9
## Decoding
$ echo -n "SUdDVEZ7UzBtZVNhbXBsZUZsNGd9" | base64 -d
>>> IGCTF{S0meSampleFl4g}
```

- Other encodings: base2 (binary), base8 (octal), base16 (hexadecimal)
- XOR
- Character representations
  - ASCII, Unicode, Morse, ...

INFORMATICA GROEP

Cryptography — Concepts

- Encryption (e.g. AES)

```
## Encrypt
$ echo -n "IGCTF{S3curedF14g}" | openssl enc -aes256
↪  -pbkdf2 -a > encrypted.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
## Decrypt
$ openssl aes-256-cbc -d -pbkdf2 -a < encrypted.enc
enter aes-256-cbc decryption password:
>>> IGCTF{S3curedF14g}
```

- Other encryption algorithms: RSA, ROT(13), DES

INFORMATICA GROEP

Cryptography — Concepts

- Hashing (e.g. MD5)

```
## Hash
$ echo -n "IGCTF{H4shThisPlease}" | md5sum
>>> a1913c52dc78a3321d046a82643de00c
```

INFORMATICA GROEP

Cryptography

- Check for broken algorithms/hashes
- Reverse engineer a given algorithm
- Do not brute-force the platform!

INFORMATICA GROEP

Tool — CyberChef

`https://gchq.github.io/CyberChef/`

- *The Cyber Swiss Army Knife*
- Many different encoders/decoders, encryptors/decryptors, ...

INFORMATICA GROEP

Web

Web — Concepts

Client contacts web server using **HTTP/HTTPS** requests

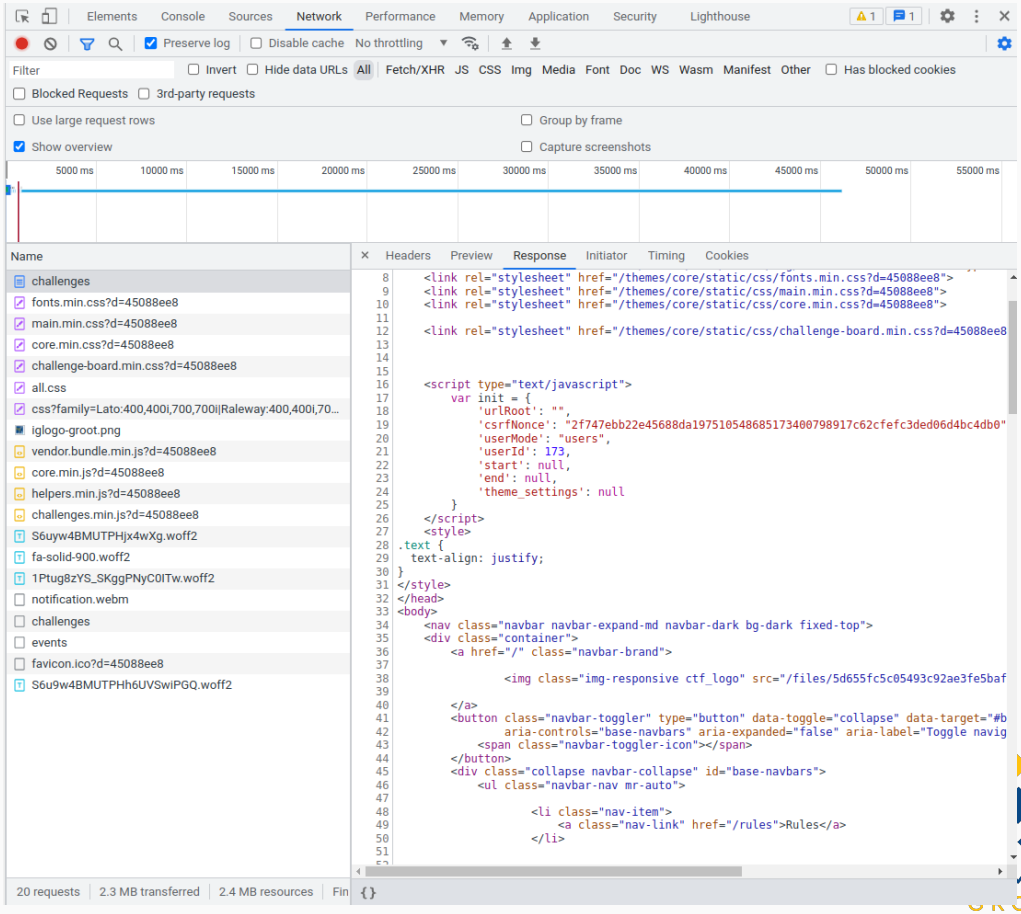
- GET: Request data from the server, e.g. HTML page
- POST: Submit data to the server, e.g. creating an account
- PUT: Edit submitted data, e.g. changing your password
- DELETE: Remove submitted data, e.g. delete your account

INFORMATICA GROEP

Web — Developer console

Open with F12

- Get HTML pages
- JavaScript console
- Analyse network traffic
- Cookies



Web — Common vulnerabilities

- Headers and cookies
  - Sensitive information
- SQL Injections
  - Input SQL queries into forms
- Cross-site scripting (XSS)
  - JavaScript code as HTML text can be exploited

INFORMATICA GROEP

Steganography

Steganography — Concepts

Hide information in files

- Wide range of possibilites
  - Audios, videos, images
- Often requires some creativity

Example

- Hiding text, possibly with LSB
- Hiding files into other files

INFORMATICA GROEP

Steganography — Tools

- `strings`
  - Extract strings from a file

```
$ strings -n6 <file>
```

- `grep`
  - Search for strings, use in combination with `strings`

```
$ grep "IGCTF" <file>
$ strings -n6 <file> | grep "IGCTF"
```

INFORMATICA GROEP

Steganography — Tools

- `file`
  - Determine file type

```
$ file <file>
```

- `binwalk`
  - Extracts files hidden in other files

```
$ binwalk -Me <file>
```

INFORMATICA GROEP

Steganography — Tools

- `exiftool`
  - Print metadata files

```
$ exiftool <file>
```

- `xxd`
  - Inspect (or create) hexdump

```
$ xxd file | less
```

INFORMATICA GROEP

Reverse engineering

Reverse engineering — Concepts

Programs written in C, C++ or Rust-like languages are first fed to compiler, which generates a binary file.

- Machine code
- Unreadable for humans
- Decompilation possible until certain extent

INFORMATICA GROEP

Reverse engineering — Tools

Ghidra

- Open-source
- Alternatives
  - Cutter
  - IDA Pro
  - JADX

[1] https://ghidra-sre.org/

INFORMATICA GROEP

Exploitation

Exploitation — Setup

You receive:

- IP and port
- Possibly a file

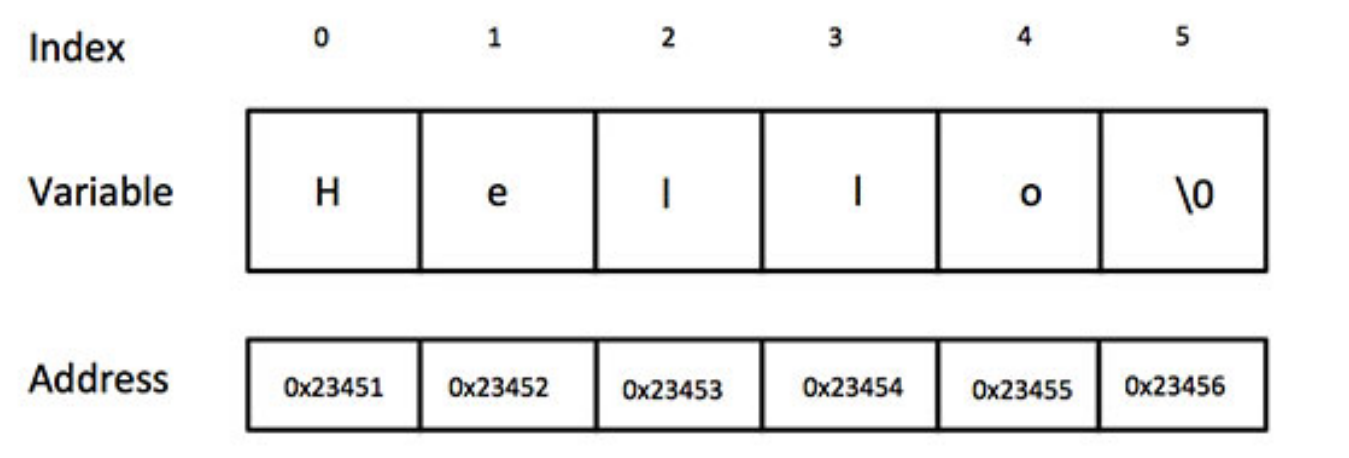
```
$ nc <ip> <port>
```

INFORMATICA GROEP

Exploitation — Concepts

C Strings

- Strings a null-terminated
- Overwriting the null-byte can let you print out what comes after the string!



INFORMATICA GROEP

Exploitation — PwnTools

PwnTools: Python library for CTF Exploits

```
from pwn import *
offset_buffer = 32
offset_ebp = 8
r = process('./call_me_maybe')
```

INFORMATICA GROEP

Exploitation — PwnTools

```
print(r.recvuntil("Pointer to printflag is "))
addr = int(r.recvuntil("\n"), 16)
print(addr)
print(r.recvline())
offset = "A"*offset_buffer + "B"*offset_ebp
r.send(offset)
r.sendline(p64(addr))
r.interactive()
```

INFORMATICA GROEP

Summary

Tools

- CyberChef
  - https://gchq.github.io/CyberChef/
- Write-ups of past years CTFs
  - https://git.infogroep.be/ig/write-ups-challenges-2021-2022
- PwnTools
  - https://docs.pwntools.com/en/stable/install.html
- Kali VM setup
  - https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/
- Google
  - https://www.google.com/

INFORMATICA GROEP

Tools

- Learn.Ctf
  - `https://learn.ctf.infogroep.be`
- Ghidra
  - `https://ghidra-sre.org/`

INFORMATICA GROEP

Questions?