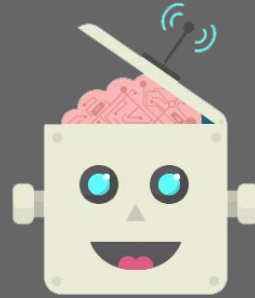JOINT

STUDENT BRANCH UFPB
CHAPTER

IEEE Computational Intelligence Society

IEEE computer society

CTF

But wait... Diabé CTF?

- Competição de Segurança da Informação
- **Jeopardy**, Attack-Defense
- Achar flags pra ganhar pontos

CTF

- Como é um desafio?

Not(e) accessible 55

Solves: 130

We love notes. They make our lifes more structured and easier to manage! In 2018 everything has to be digital, and that's why we built our very own note-taking system using micro services: Not(e) accessible! For security reasons, we generate a random note ID and password for each note.

Recently, we received a report through our responsible disclosure program which claimed that our access control is bypassable...

http://35.207.120.163

Difficulti estimate: Easy-Medium

CTF

- Tipos
  - rev
  - pwn
  - crypto
  - web
  - misc

https://github.com/saurav3199/CTF-writeups/tree/master/HSCTF6
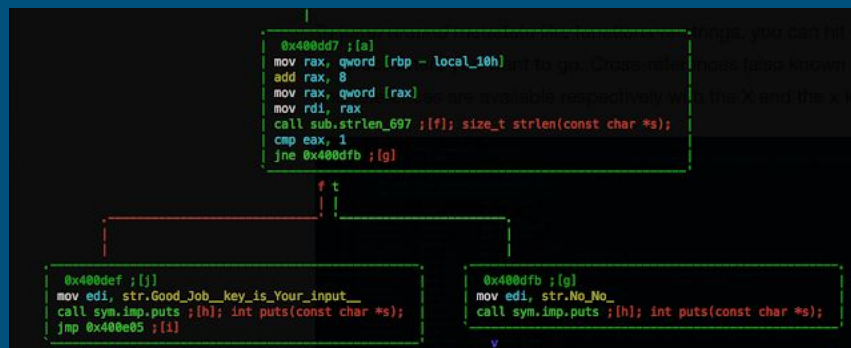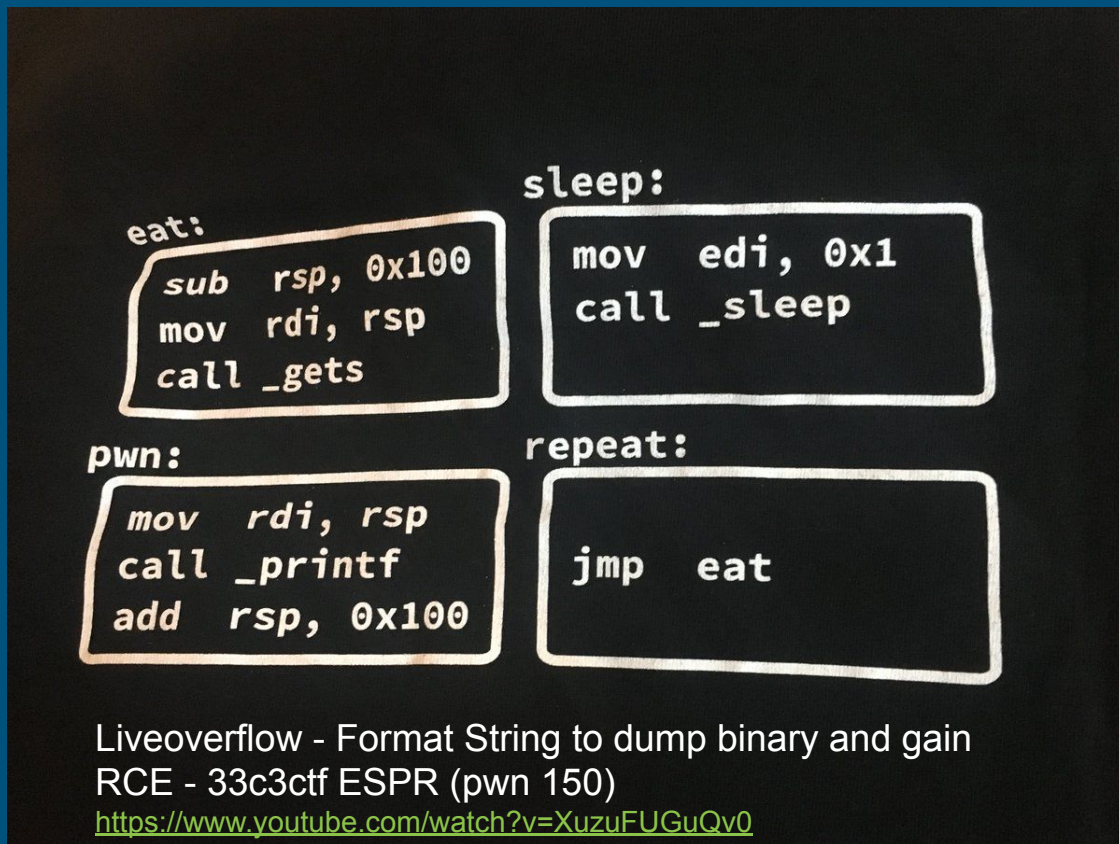
CTF

- Tipos
  - rev
    - Engenharia reversa.
    - Binário (executável)
    - Assembly
    - Objetivo
      - Entender o que o binário faz para conseguir extrair informações dele.

CTF

- Tipos
  - rev
  - pwn
    - Binário (executável)
    - Assembly
    - Binário rodando num servidor
    - Objetivo:
      - Achar uma forma de corromper o binário para conseguir executar código no servidor

Liveoverflow - Format String to dump binary and gain RCE - 33c3ctf ESPR (pwn 150)
https://www.youtube.com/watch?v=XuzuFUGuQv0
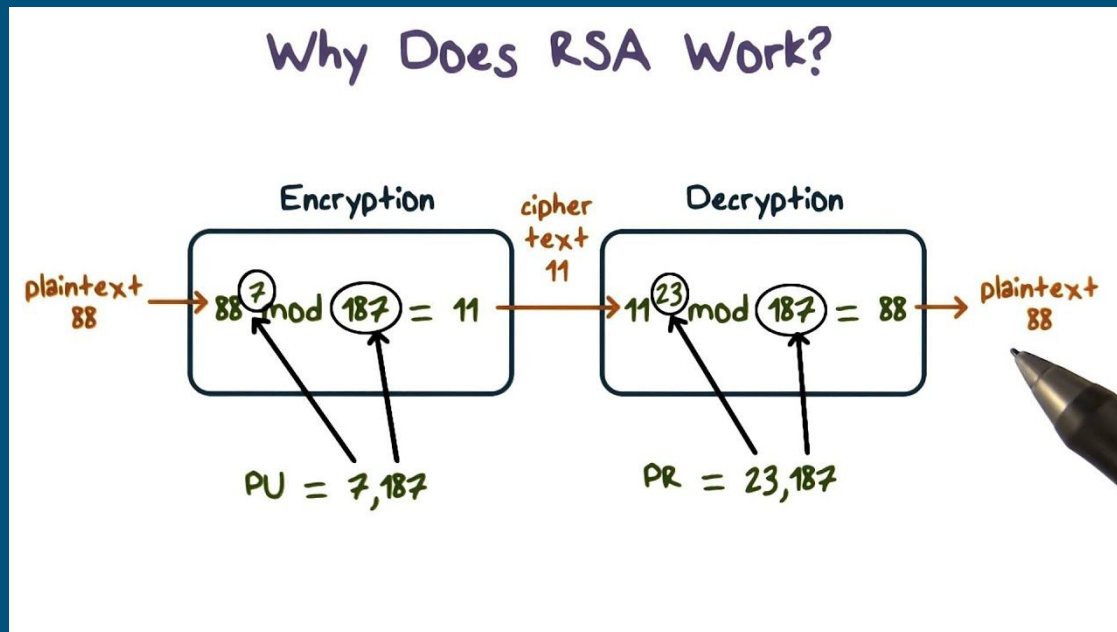
CTF

- Tipos
  - rev
  - pwn
  - crypto
    - Criptografia
    - Mais matemático
    - Objetivo:
      - Encontrar uma chave ou quebrar alguma cifra.

John Hammond - b00t2root CTF: cuz rsa is lub [RSA Cryptography]
https://www.youtube.com/watch?v=_Ig2AEqRTjg

CTF

- Tipos
  - rev
  - pwn
  - crypto
  - web
    - Um site;
    - Uma vulnerabilidade: SQLi, auth bypass, XSS, CSRF, etc
    - Objetivo:
      - Acessar a uma página sem permissão ou o servidor do site

```php
<?php
$flag = file_get_contents("/flag");

if (!isset($_GET["md4"]))
{
    highlight_file(__FILE__);
    die();
}

if ($_GET["md4"] == hash("md4", $_GET["md4"]))
{
    echo $flag;
}
else
{
    echo "bad";
}
?>
```
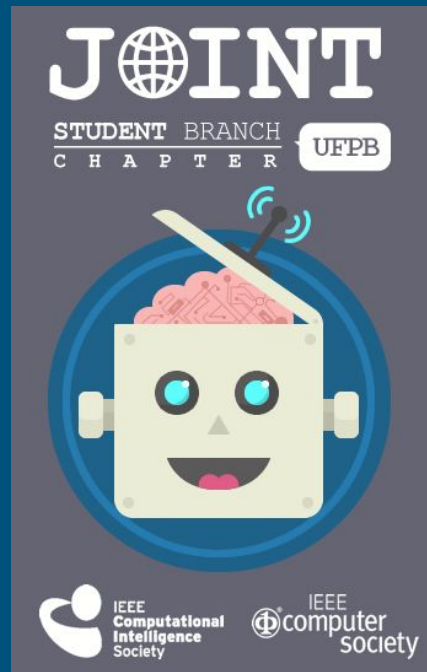
https://github.com/saurav3199/CTF-writeups/tree/master/HSCTF6#md5---

CTF

- Tipos
  - rev
  - pwn
  - crypto
  - web
  - misc
    - Forense
    - Pesquisa
    - Estenografia
    - Desafio de programação
    - Demais...

https://github.com/cscisufpb/CTF/tree/master/Chall%20Joint%20Logo

Onde encontrar?

https://ctftime.org/

Como encontrar um time?

Wargames

- Overthewire - https://overthewire.org/wargames/
- Cryptopals - https://cryptopals.com/
- Pwnable.kr - http://pwnable.kr/
- Hacking-lab - https://www.hacking-lab.com/index.html
- HackTheBox - https://www.hackthebox.eu/
- Many more...
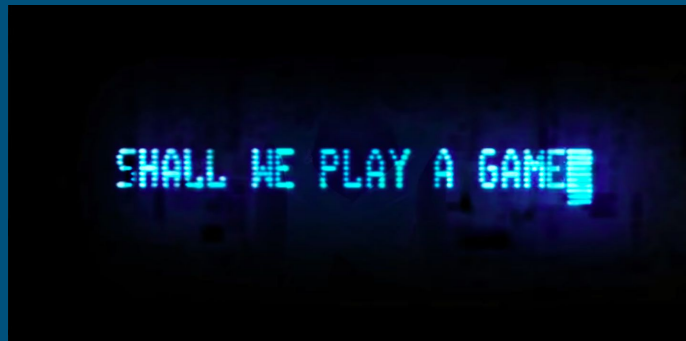
Lembrando!

Você vai errar MUITO!!!

F.A.I.L

First Attempt In Learning

O que fazer depois que falhar?

WRITE UPS E

COMPETITION CHAT

E sempre...

- Respeitar as regras e as pessoas;
- Não compartilhar flags;
- HAVE FUN!

Dúvidas?

Ou vamos ver alguns desafios?