

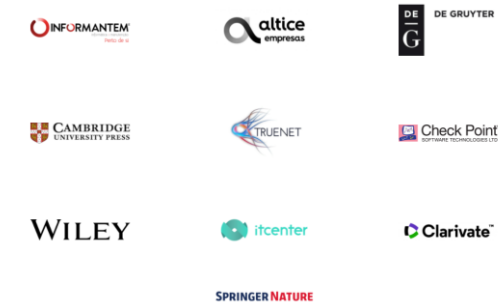
# {CAPTURE THE FLAG}

João Machado  
2021/10/21

## Patrocinadores Platina



## Patrocinadores Ouro



## Patrocinadores Prata

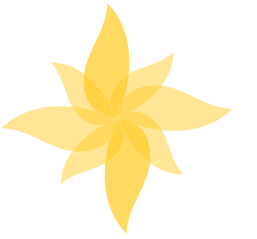


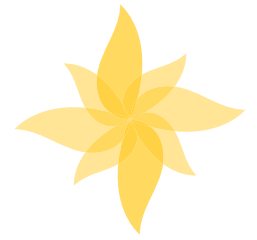
## Apoios



# AGENDA

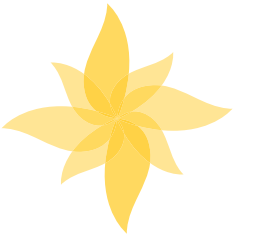
- O que é um CTF?
- Como criar um CTF?
- Exemplos de Exercícios





# O QUE É UM CTF?

# O QUE É UM CTF?

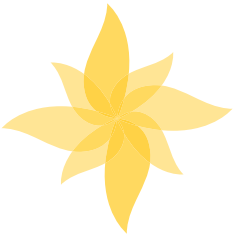


- É uma competição de Ciber-Segurança.
- Podem durar entre horas a vários dias.
- Atraem estudantes, entusiastas ou mesmo profissionais.
- Pontos são atribuídos com base em submissões de flags.

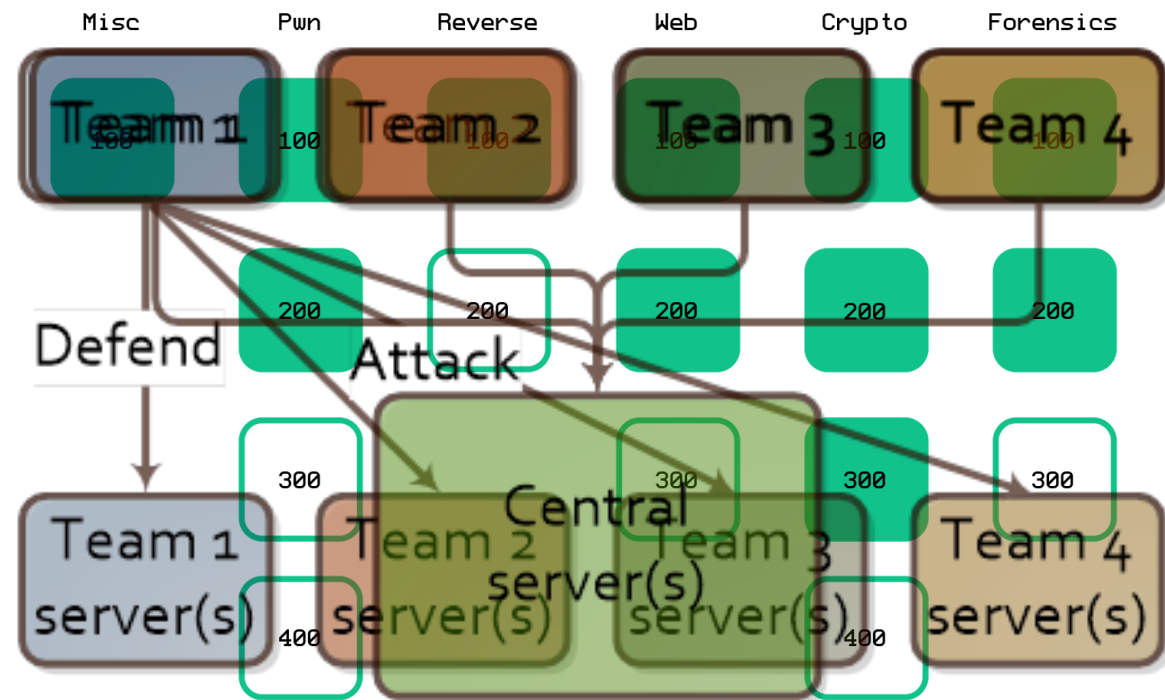


**Flag{Th1s\_1s\_4\_Fl4G}**

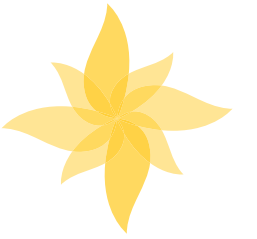
# TIPOS DE CTF



- Jeopardy
- Attack & Defense
- King of the Hill



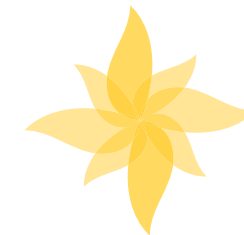
# QUAL O PROPÓSITO DE UM CTF?



- Ferramenta para treino.
- Team building e Soft Skills.
- Entender vulnerabilidades e respetivas correções.

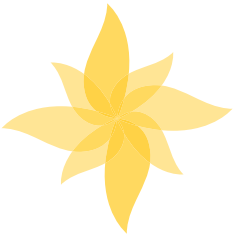


# PLATADORMAS DE CTF CONHECIDAS



- picoCTF (<https://www.picoctf.org>)
- Hack This site (<https://www.hackthissite.org>)
- HackTheBox (<https://www.hackthebox.eu>)
- VulnHub (<https://www.vulnhub.com>)
- TryHackMe (<https://tryhackme.com>)
- HackerOne (<https://ctf.hacker101.com>)
- Entre outros...

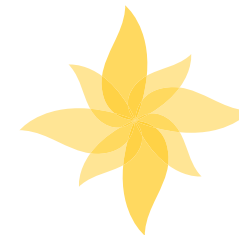
# INFORMAÇÕES SOBRE CTFS



- Resultados de competições
- Informações sobre competições a nível mundial
- Calendários e próximos eventos
- Resoluções de exercícios de CTF anteriores
- Acessível em <https://ctftime.org/>

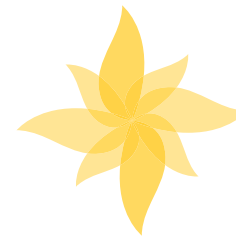






# COMO CRIAR UM CTF?

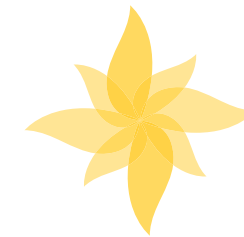
# COMO COMEÇAR?



- Participar frequentemente em desafios de CTF
- Ler Write-ups de exercícios e entender as vulnerabilidades
- Começar a criar exercícios!
- Usar frameworks para criar um CTF com os exercícios criados



# FERRAMENTAS

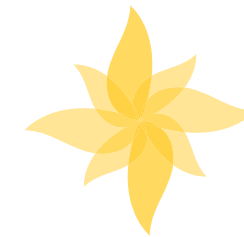


## Treino

- OWASP Juice Shop (<https://owasp.org/www-project-juice-shop>)
- Damn Vulnerable Web Application (DVWA) (<https://dvwa.co.uk>)
- picoCTF (<https://github.com/picoCTF/picoCTF>)



# FERRAMENTAS

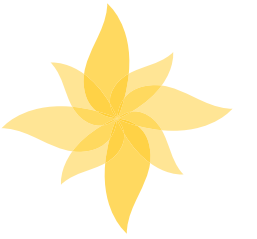


## Criação de CTFs

- Facebook's CTF Framework (<https://github.com/facebookarchive/fbctf>)
- picoCTF (<https://github.com/picoCTF/picoCTF>)
- SecGen (<https://github.com/cliffe/SecGen>)
- CTFd (<https://ctfd.io>)

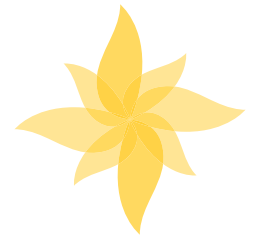


# CUIDADOS A TER



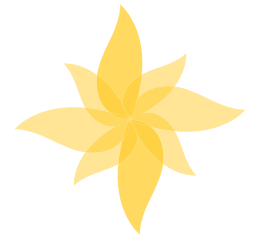
- Regras específicas em ambientes Cloud
- Evitar colocar sistemas vulneráveis expostos à internet
- Definir sempre o contexto e as regras específicas do CTF.



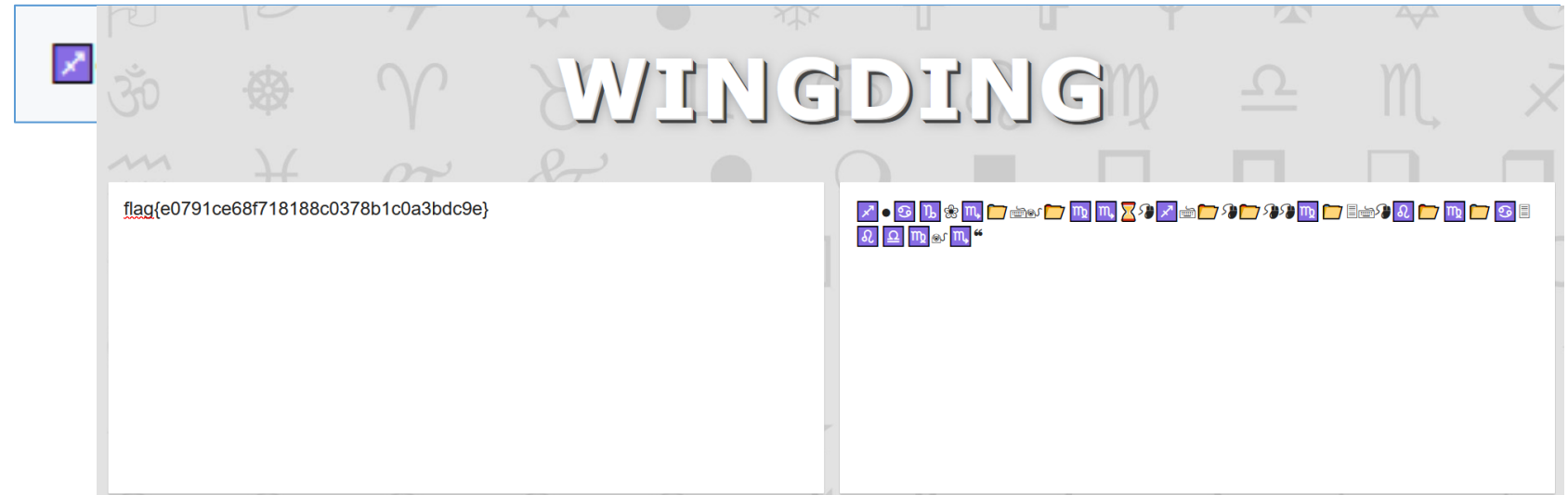


# EXEMPLOS DE EXERCÍCIOS

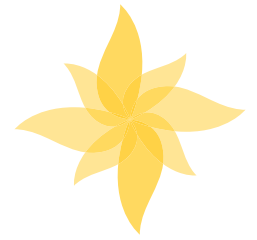
# EXERCÍCIOS



- Nahamcon2021 – ChickenWings (Cryptography)



# EXERCÍCIOS



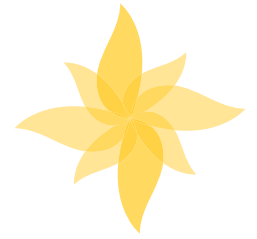
- Cyber Apocalypse 2021 – Nintendo Base64 (Cryptography)

```
Input                                     length: 1005
                                         lines: 9
Vm                                     0w                                     eE5GbFdWW                               GhT                               V0d4VVYwZ
G9                                     XV                                     mx                                     ywk   ZOV                               1JteD                               BaV   WRH
                                         YW                                     xa                                     c1                                     Nswl dS   M1   JQ   WV                               d4
S2RHVkljRm   Rp   UjJoMlZrZH   plRmRHV   m5WaVJtU1   hUVEZLZVZk   V1VrZFpWmu   pHVDFaV1Z   tSkdXazlXYW   twdl   Yx   Wm   Fj   bHBFVwxwTlZ
Xdz   Bwa   2M   xVT   FSc   1d   uT1   hi   R2h   XWw   taS   1dG   VXh   Xbu   ZTT   VdS   eLYy   cz   FWM   ky2VmtwV2
JU   RX   dZ   ak   Zr   U0   Z0c2JGwmlS   a3   BY   V1   d0   YV   lV   MH   hj   RVpYY1VaVFRWW   mF   lV   mt   3V
lR   GV   01   ER   kh   Zak   5rVj   JFe   VR   Ya   Fdha   3BIV   mpGU   2NtR   kdX   bWx   oT   TB   KW   VYxW   lNSM
Wx   XW   kV   kV   mJ   GWlRZ   bXmXy2xWc   1V   sZ   FRiR1J5VjJ   0a1YySkdj   RVpwWmxKV   1V   GRTlQUT09

Output                                     time: 13ms
                                         length: 38
                                         lines: 1
CHTB{3nc0d1ng_n0t_3qu4l_t0_3ncrypt10n}
```



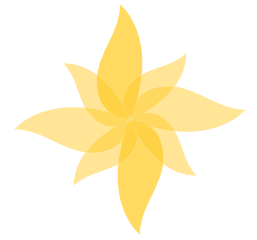
# EXERCÍCIOS



- Summer 2020 RCTS CERT CTF – Stega 300 (Forensics)



# EXERCÍCIOS



- Cyber Apocalypse 2021 – Passphrase (Reverse)

The screenshot displays a debugger interface with several panels. The top-left panel shows a 'Program Trees' view with a tree structure for 'passphrase1' containing sub-items like '.bss', '.data', '.got', '.dynamic', '.fini\_array', and '.init\_array'. The top-right panel shows a 'Listing' window with the following Python code:

```
hex_string = [0x78, 0x74, 0x72, 0x34, 0x74, 0x33, 0x72, 0x52, 0x33, 0x73, 0x74, 0x52, 0x31, 0x34, 0x4c, 0x35, 0x5f, 0x56, 0x53, 0x5f, 0x68, 0x75, 0x6d, 0x34, 0x6e, 0x35]
out = []

for item in hex_string:
    out.append(chr(item))
```

The main console window shows the execution of the program:

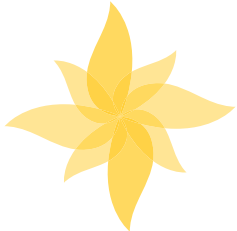
```
./passphrase
Halt!
You do not look familiar..
Tell me the secret passphrase: 3xtr4t3rR3stR14L5_VS_hum4n5
Sorry for suspecting you, please transfer this important message to the chief: CHTB{3xtr4t3rR3stR14L5_VS_hum4n5}
```

The bottom panel shows a disassembler view with instructions and their addresses:

00100b34	74 05	JZ	LAB_00100b3b	25	undefined local_47;
00100b36	e8 a5 fc	CALL	__stack_chk_fail	26	undefined local_46;
	ff ff			27	undefined local_45;
				28	undefined local_44;

Below the disassembler, there is a note: "-- Flow Override: CALL RETURN (CALL TERMINATOR)".

# EXERCÍCIOS



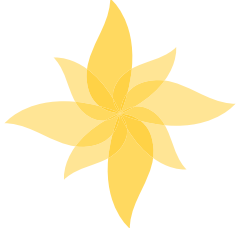
- RCTS\_CERT CTF 2021 - Well Hello there (Pwn)

```
(jmachado@kali) - [~/Desktop/RCTS_CERT_CTF_2021]
$ ./program
Hello there! What is your name?
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
flag{buff3r_0v3rfl0w_r0cks}
```

```
loc_11E1:
mov     edi, 0Ah
call   _putchar
mov     eax, 0
add     rsp, 58h
retn
```

```
call   _gets
mov     eax, [rsp+58h+var_C]
test    eax, eax
jnz     short loc_11E1
```

# EXERCÍCIOS



- TMUCTF 2021 - Foreign Student (OSINT)

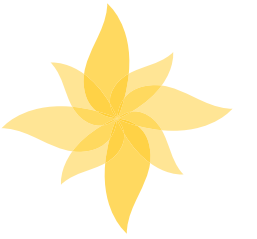
```
└─$ curl https://raw.githubusercontent.com/ZedZini/secretkey/main/0xEB0B6528-pub.asc | gpg --import
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total      Spent    Left    Speed
  0     0     0     0     0     0     0     0  0  0  0  0  0  0  0  0  0  0  0  0  0
  0     0  19488     0  ---:---:---  ---:---:---  ---:---:---  19427
gpg: key 586DD615EB0B6528: public key "Zedmondo Zaberini (Nothing to say...) <Z3dm0nd0_Z4b3r1n5k1_15_My_R34l_N4m3@zaberini.com>" imported
gpg: Total number processed: 1
gpg:          imported: 1
```

```
flag{Z3dm0nd0_Z4b3r1n5k1_15_My_R34l_N4m3@zaberini.com}
8P447Zr0G5kDPP9a5sA MyT834LSN4M3@zaberini.com
SzChR0Jt3vI7BjA3WV1xQp94XTqRqFrjtJkS2I3n03I94jhLu0AwfoiskKzyl+tQ
lexhE31arP/MEYV9VfPSxqR23rm+shIdeKP+9G9XR3Z1rp00+1P78o7uvRG/7oPR
P0w6CAh0eXLpM3P18irvjnH3VekS0g9a/d/7hhyVkrtsH4vAd8038Z3Q82dWws5J
... cut ...
=oo5F
-----END PGP PUBLIC KEY BLOCK-----
```

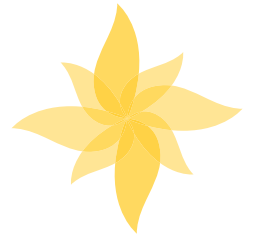
**Dummy-Repo** Public  
Will be used later, or perhaps never...  
Updated on Feb 15 ☆ Star

**secretkey** Public  
It is a public key. Not really a secret, right?  
Updated on Feb 15 ☆ Star

# EM RESUMO



- ✓ Os desafios CTF podem ser usados para treino.
- ✓ A criação de um CTF pode ser usado para demonstrar vulnerabilidades.
- ✓ Podem ser usadas como ferramentas de team building e de melhoria de soft e hard skills.



Obrigado