

Challenge

53 solves

×

## "Basic" RSA

### 30

There is a basic implementation of RSA. This is not as secure as seems like. Can you find a way to decrypt the encrypted message?

Unlock Hint for 10 points

 ciphertex...

 public\_ke...

Flag

Submit

Basic rsa

Challenge


8 Solves




## Buggy RSA

58

We have a buggy way of implementing RSA.  
Can you exploit the bug to break the  
encryption and retrieve the secret  
message that was encrypted?

 encrypt.py

 output.txt

Submit

buggy rsa

Challenge 2 Solves





## Crypto Training Caesar IV

70

Caesar has used ECC scheme to encrypt his messages. The source code that he used for encryption and the encrypted message is attached here (of course with the plaintext and the secret being edited out).

**Find and submit the decrypted ciphertext.** Enclose it within esCTF{}

 enc.txt

 qn.py

0/15 attempts

Crypto Training Caesar IV


Challenge 3 solves




# Break a log

80

We were learning about the difficulty to break discrete log. We came up with an implementation for the same, which we think is secure. Can you break it?

 output.txt

 qn.py

Submit

Break a log

challenge

24 solves



## Neo's Forensics Training

30

Neo found a lot of money deposited in a bank, he chances upon an unsupervised ATM, and tries to maliciously withdraw money. With his limited tools and time he is only able to capture a dump of the ATM machine.

Can you help Neo discover some hidden secrets from this dump?

[https://drive.google.com/file/d/1LH\\_BFrg0-k57fBBgvJ5WrrfSrIuvdi0f/view?usp=sharing](https://drive.google.com/file/d/1LH_BFrg0-k57fBBgvJ5WrrfSrIuvdi0f/view?usp=sharing)

Unlock Hint for 10 points

 bank\_at...

Neo's Forensics Training

challenge

13 solves



## Pandora's Box

50

Go on the journey looking into the Pandora's box to find the hidden treasure, make sure you remember the path that you took to reach back home safely.

Find and submit the flag in the hidden treasure.

 file.7z

0/15 attempts

Pandora's Box

challenge

31 solves


×

Magically protected

30

You found a locker, but it seems to have a strange lock protecting it? Can you figure out a way to break in the locker?

nc 0.cloud.chals.io 28941

 locker

5/15 attempts

Flag

Submit

Magically protected

challenge

20 solves



## (not so) Free Flag

44

guessy

You are given a free flag  
"6dab1eeb8f9e9dca1d8a783e8acfad85efb06  
b2fada3e75e72875e" but it is not  
directly usable. Can you extract the  
flag out of it? Submit the extracted  
message within esCTF{ }.

5/50 attempts

"6dab1eeb8f9e9dca1d8a783e8acfad85efb06b2fada3e75e72875e"



Challenge

13 solves




# Device check

56

We developed a password checker to validate the authenticity of a device and then remember it. But unfortunately the code was written on the last day, so there might be few bugs to bypass the check. Can you exploit those to retrieve the flag?

nc 34.100.187.70 1111

 main

nc 34.100.187.70 1111

Device check

Challenge

11 Solves



## Dumped

57

After Kingpin's vault got breached, it auto dumped everything contained in it in a mysterious dumpster. Kingpin's treasure might still have something valuable in it. This interactive dumpster is user friendly but might be vulnerable. Can you find something of interest in this dumpster?

nc 34.100.187.70 4444



dumped

nc 34.100.187.70 4444

Dumped

Challenge

10 solves



## Got2win

57

We found a flag was with Daenerys Targaryen. With the help of the Night Watch you have to infiltrate her city walls and retrieve it.

nc 34.100.187.70 5555

Unlock Hint for 10 points

 got2win

Flag

Submit

```
nc 34.100.187.70 5555
```

Got2win

Challenge

3 solves

×

Notes

89

Use this free app to takes notes about your CTF findings. You can add/delete or see all notes. We tried our level best to make it free from double free. Can you find a way to exploit it and retrieve a flag?

```
nc 34.100.187.70 7777
```

Unlock Hint for 20 points

notes

libc.so.6

Flag

Submit

```
nc 34.100.187.70 7777
```

Notes

Challenge


6 Solves



# I have the Power

60

Prince Adam quite stealthily acquired the power traces of a device running a 128-bit AES encryption with 32-bit input. He utilizes this by providing some plaintexts and getting the corresponding ciphertext. Can you help him figure out the Key with the help of the collected trace. Submit the **key** enclosed within esCTF{ }.

 traces.ta...

I have the Power

Challenge

3 Solves



# KingPin 2.0

60

Kingpin upgrades his security system for the vault after the previous Heist. But unfortunately the upgrade just hides the previous vulnerability rather than fixing it. Can you find a way to break the vault?



kingpin

KingPin 2.0

Challenge


0 Solves




## Fault in our \*\*\*\*\*

70

Darwin got access to a device that encrypts messages using AES 256 before sending them. He uses it to inject single byte faults in the AES encryption during the 8th round before MixColumn and generate faulty ciphertexts. He has a list of 4 ciphertext and faulty ciphertext pairs with him, generated from the same key. He also has a super secret cipher present with him encrypted using the same key. Can you help him figure out the key used in the encryptions and decipher the secret cipher?

 faults.txt

 super\_se...

Fault in our

Challenge 10 Solves



# Welcome to Cinque Terre

56

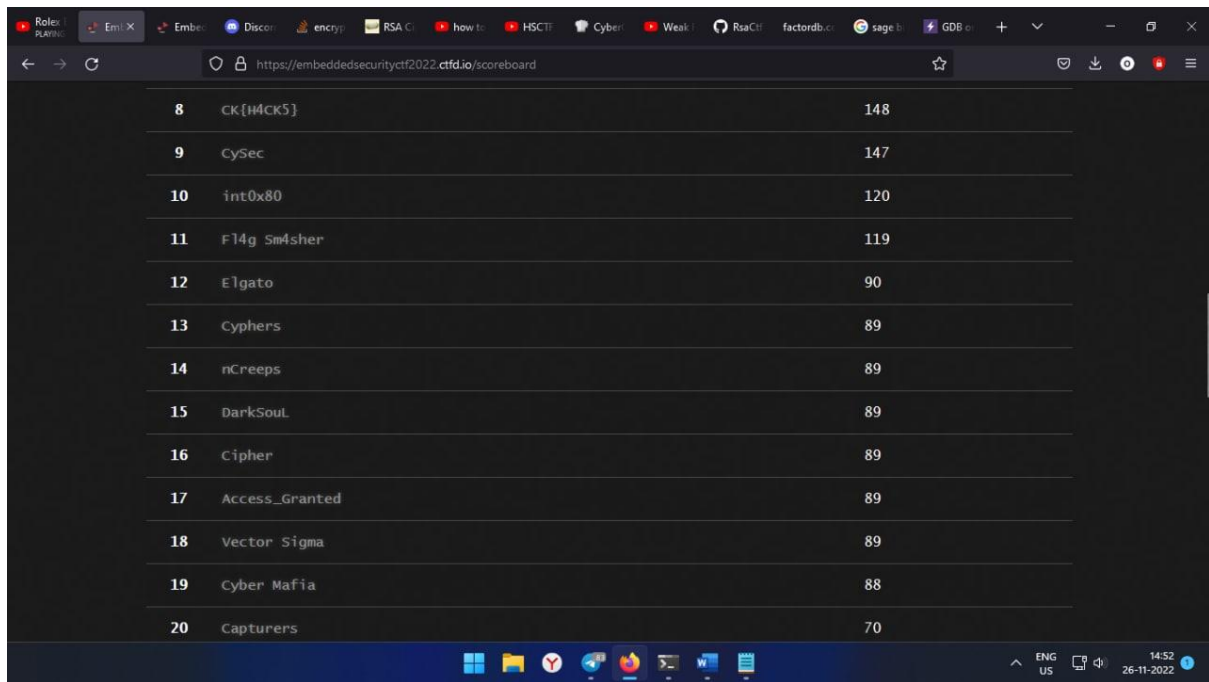
Welcome to Cinque Terre! We would love  
to host you in our lovely villages.  
Explore coastal Italy with us.

[embeddedsecurityctf2022-hostme.chals.io](https://embeddedsecurityctf2022-hostme.chals.io)

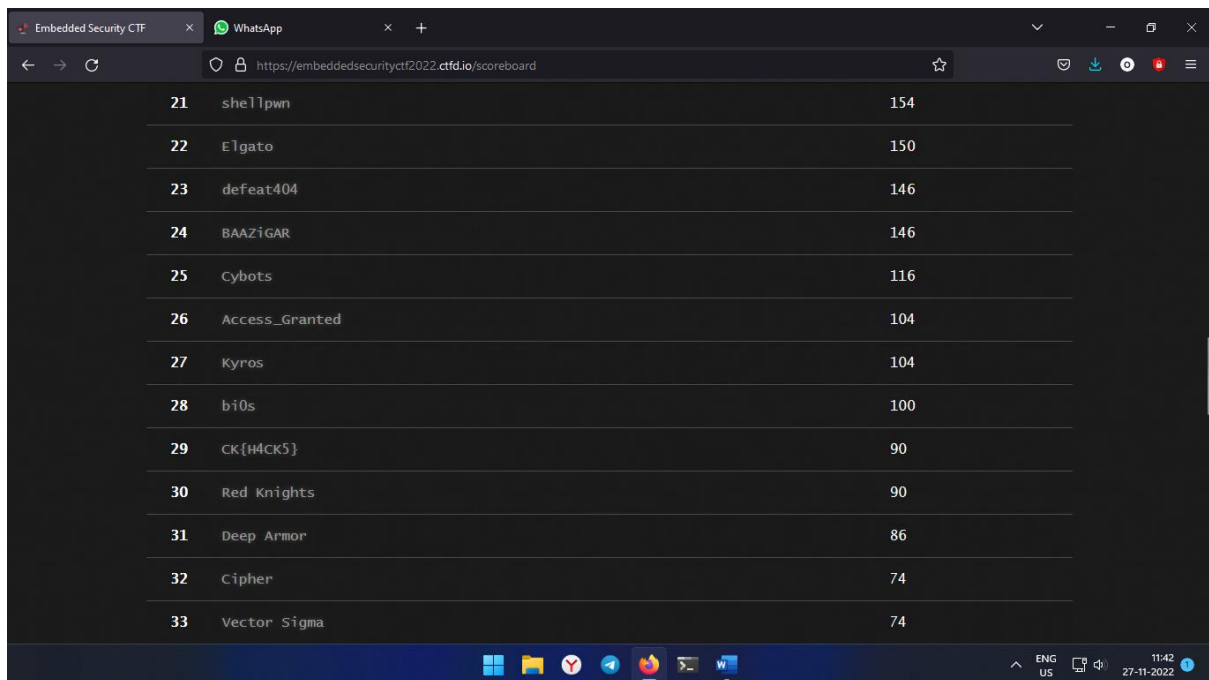
`embeddedsecurityctf2022-hostme.chals.io`

website





8	CK{H4CK5}	148
9	CySec	147
10	int0x80	120
11	F14g Sm4sher	119
12	Elgato	90
13	Cyphers	89
14	nCreeps	89
15	DarkSoul	89
16	Cipher	89
17	Access_Granted	89
18	Vector Sigma	89
19	Cyber Mafia	88
20	Capturers	70



21	shellpwn	154
22	Elgato	150
23	defeat404	146
24	BAAZiGAR	146
25	Cybots	116
26	Access_Granted	104
27	Kyros	104
28	bi0s	100
29	CK{H4CK5}	90
30	Red Knights	90
31	Deep Armor	86
32	Cipher	74
33	Vector Sigma	74

## 60

You are given a free flag  
**"6dab1eeb8f9e9dca1d8a783e8acfad85efb06b2fada3e75e72875e"** but it is not directly usable. Can you extract the flag out of it? Submit the extracted message within esCTF{ }.

**Correct**

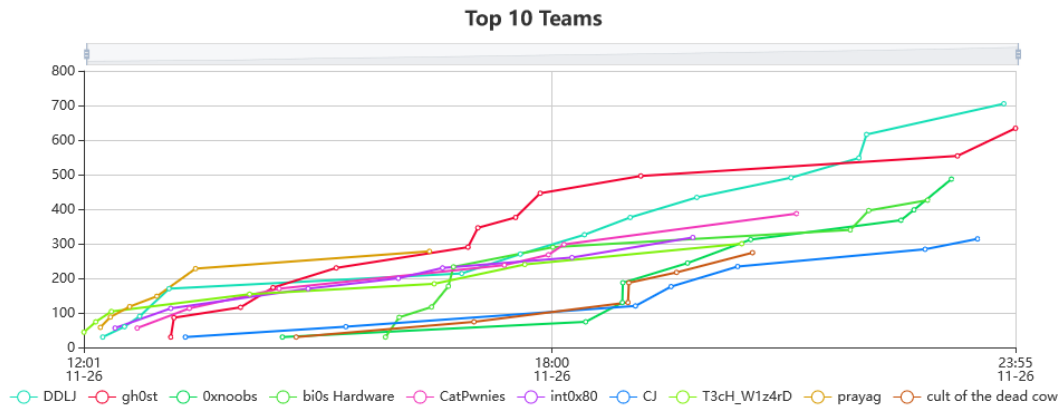
Submit

```
obsidian@Sigma:~$ ./locker
SyntaxError: Non-UTF-8 code starting with '\x83' in file /home/obsidian/binary on line 4, but no encoding declared; see https://python.org/dev/peps/pep-0263/ for details
obsidian@Sigma:~$ cat binary
cat: binary: No such file or directory
obsidian@Sigma:~$
```

1

```
obsidian@Sigma:~$ ./locker
./locker: line 5: python3.7: command not found
```

```
rm binary
```



## Crypto

- "Basic" RSA (30)
- Buggy RSA (58)
- Crypto Training Caesar IV (69)
- Break a log (80)

## Forensics

- Neo's Forensics Training (30)
- Pandora's Box (50)

## Misc

- Magically protected (30)
- (not so) Free Flag (44)

## PWN

- Device check (56)
- Dumped (57)
- Got2win (57)
- Notes (89)

## Side Channel

- I have the Power (60)
- KingPin 2.0 (60)
- Fault in our \*\*\*\*\* (70)

## Web

- Welcome to Cinque Terre (56)

Challenge27 Solved

"Basic" RSA

30

There is a basic implementation of RSA. This is not as secure as seems like. Can you find a way to decrypt the encrypted message?

Unlock Hint for 10 points

ciphertex...

public\_ke...

Correct

ong\_base\_leads\_to\_weak\_enc}

Submit

Last build: 16 hours agoOptionsAbout / Support ?

Recipe

From Hex

Delimiter  
Auto

To Base64

Alphabet  
A-Za-z0-9+/=

Input

length: 54  
lines: 1

6dab1eeb8f9e9dca1d8a783e8acfad85efb06b2fada3e75e72875e

Output

start: 0  
end: 36  
length: 36

time: 0ms  
length: 36  
lines: 1

base64+encoding+is+the+way+to+decode

STEP

BAKE!

Auto Bake

```
obsidian@Sigma:~$ nc 0.cloud.chals.io 28941
Enter the passcode :
alohamora!
Spells are not allowed.
```

## Members

User Name	Score
Obsidian <span>Captain</span>	75
Fazlur rehman	0
Ayush Gupta	0
Shaurya Singh	0

## Solves

Challenge	Value	Time
(not so) Free Flag	45	November 26th, 2:04:35 PM
"Basic" RSA	30	November 26th, 2:52:06 PM