
CTF Code

Writeups

Криптография

21 сентября 2021 г.

Оглавление

Easy		1
1	Based task	1
2	Hashes among us	2

Easy

1 Based task

Достаточно простая задача. Нам дается файл с какими-то иероглифами:



Рис. 1: Китайцы уже близко

Казалось бы, что тут можно придумать, переводчик выдает какую-то дичь. Если заметить название задачи, то можно подумать про какую-то кодировку из base'ов. Немного гуглинга и можно наткнуться на весьма интересную штуку под названием [base65536](#). Прогнав через него натыкаемся на какую-то случайную последовательность эмодзи:



Рис. 2: Кто-то слишком эмоционален

Поуглиив еще немного можно найти **base100**, после извлечения из которого получаем старый-добрый base64:

b3Jlb19jdGZfS2V2aW5EYXZpZE1pdG5pY2shCg==

Рис. 3: То, что знакомо почти всем

И тут два варианта:

- Прогнать обратно ручками
- Написать питоновский скрипт

Чтобы райтап был полным, рассмотрим второй вариант, потому что первый достаточно очевидный и не требует пояснений. Скрипт для расшифровки выглядит примерно следующим образом:

Листинг 1: Дешифровка флага

```
#!/usr/bin/env python3

import base65536
import pybase100 as base100
import base64

with open('flag.enc', 'r') as flag_file:
    flag = flag_file.read()

flag = base65536.decode(flag)
flag = base100.decode(flag)
flag = base64.b64decode(flag)
flag = flag.decode('utf-8')

print(flag)
```

На выходе получаем флаг `oren_ctf_KevinDavidMitnick!`.

2 Hashes among us

Судя по виду зашифрованного флага и названию задачи перед нами какой-то хэш.



```
1775fe677ade895006ac191fc4391761
```

Рис. 4: Слишком много хешков

Если посмотреть длину, то мы увидим, что длина флага ровно 32 символа, что позволяет подумать про MD5. Дальше можно либо брутить локально с помощью HashCat/JhonTheRipper или воспользоваться онлайн-сервисами наподобие [CrackStation](#). После чего получаем строку `RobertMorris`, которую нужно обернуть в `oren_ctf_` и `!`. После чего получаем флаг `oren_ctf_RobertMorris!`.