CTF

Swapnilshrestha.com.np

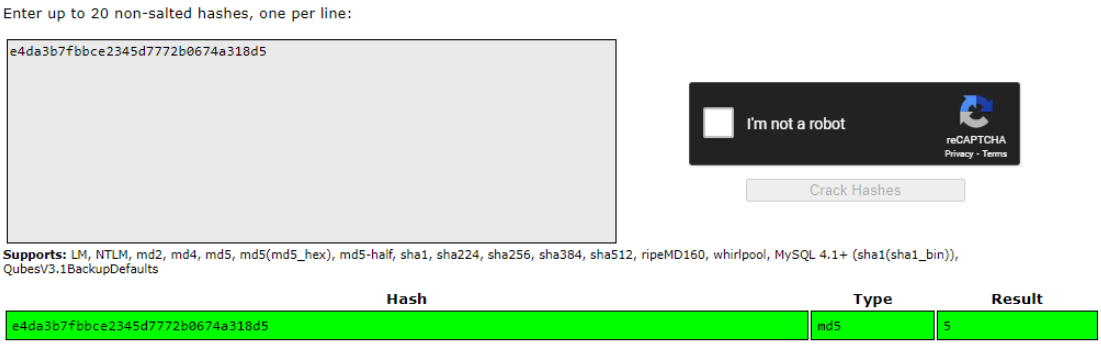
Step1:

Right click and go to view source code

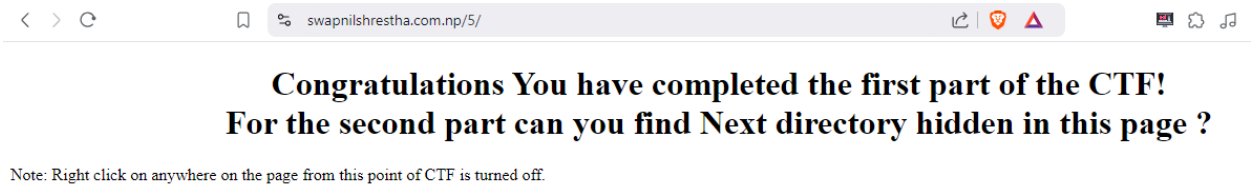
There are many hash key in comment

```
<!-- This website may help: https://crackstation.net/

The md5hash are :
c4ca4238a0b923820dcc509a6f75849b
c81e728d9d4c2f636f067f89cc14862c
eccbc87e4b5ce2fe28308fd9f2a7baf3
a87ff679a2f3e71d9181a67b7542122c
e4da3b7fbbce2345d7772b0674a318d5

-->
```

Crack hash key with crackstation website



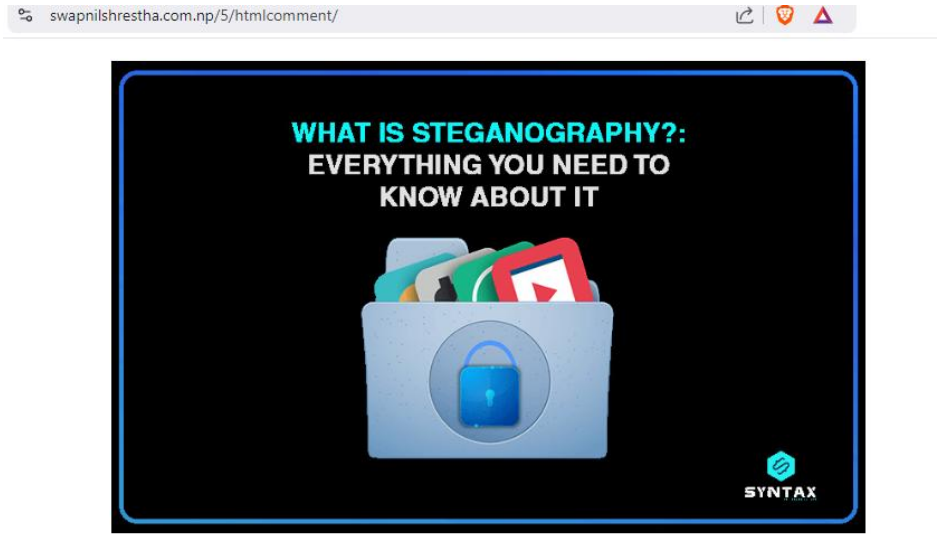
Now the for next directory enter all result one by one until get right result.



After find out next directory, because of right click is turn off on page then we use shortcut key for view source code (ctrl + u).

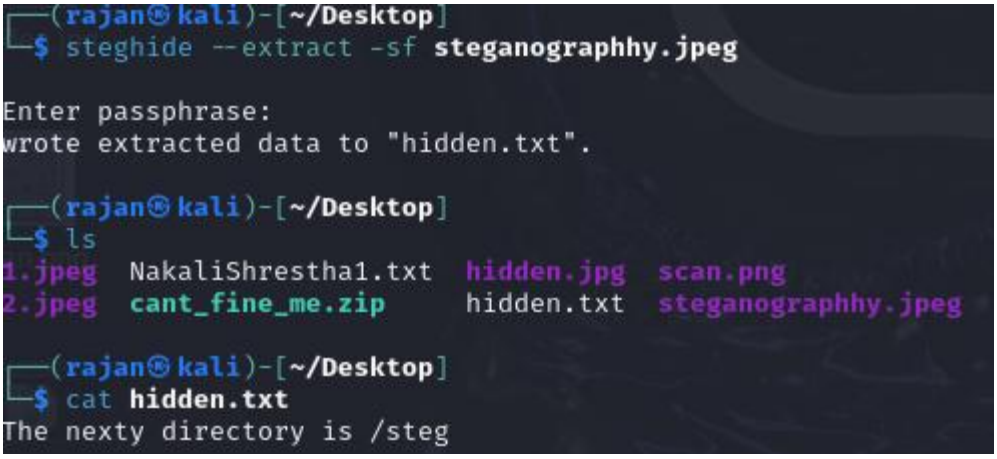
```
<p> Note: Right click on anywhere on the page from this point of CTF is turned off. </p>
<!-- Next directory is /htmlcomment -->
</body>
</html>
```

There is another hint for next directory. (/htmlcomment) now enter this on browser and get in next directory.

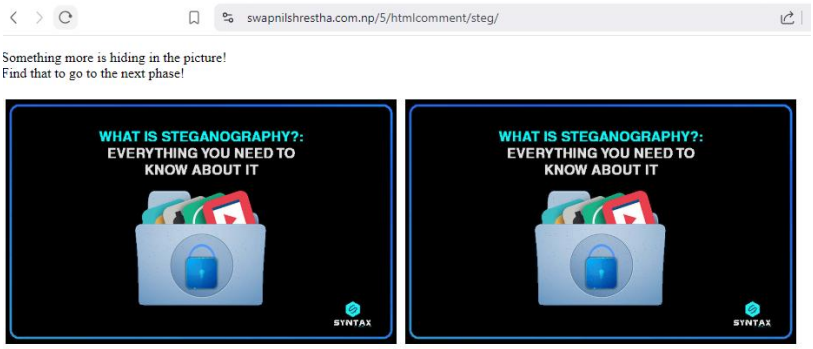


There is another encryption method steganography. And the image steganography is used to hide next directory hint (text).

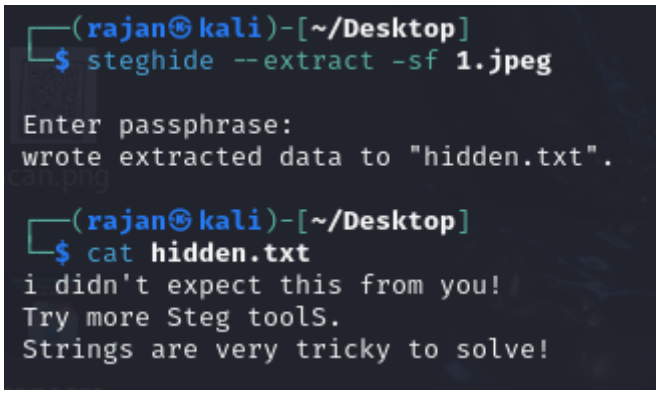
Now we are going to decrypt this image with another tools steghide.



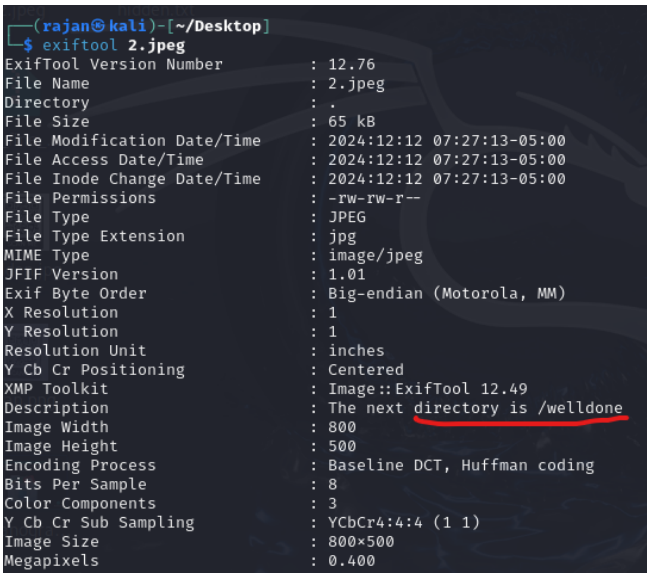
Here we get another hint for next directory (/steg).



Here is another steganography to hide text for next directory. First we download both image from source code on desktop. Then again we used steghide command tools. If steghide command not work for this images, then we will try another command.

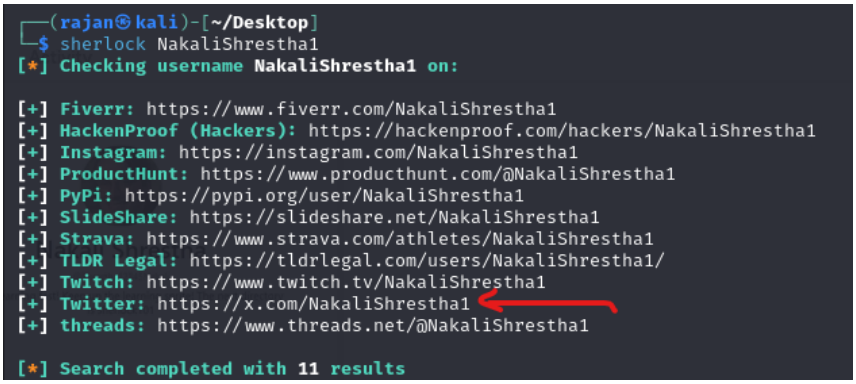


Here when we try steghide command for image1 there is information about use more steg tools for crack image 2.

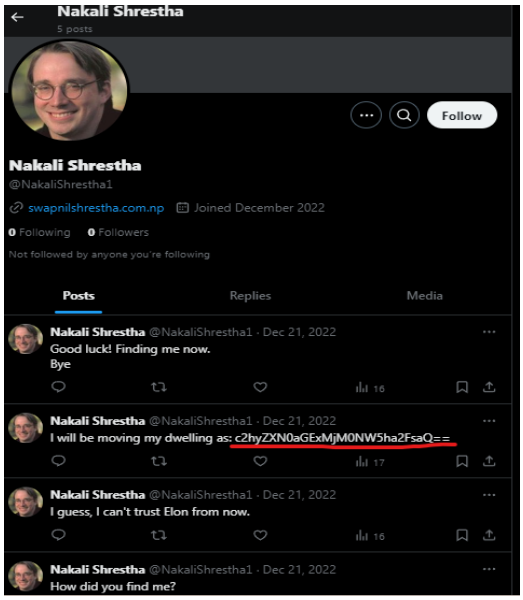


Here we used another steg tools (exiftool) and get another directory on description.

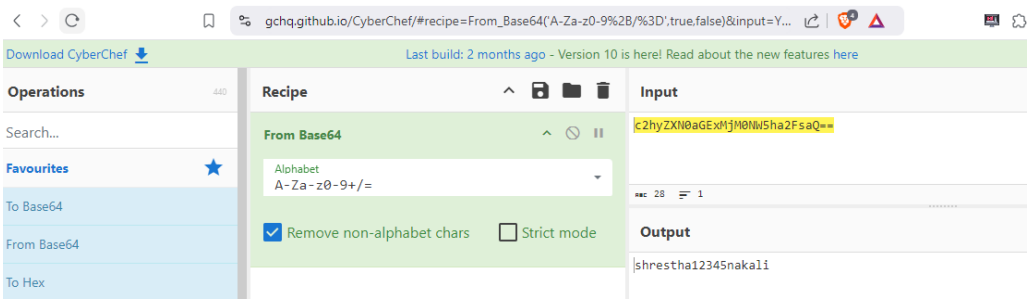
We get another CTF and hint like follow Nakkalishrestha1. This means we are going to use another tools Sherlock which help us to find out this user name on different social media.



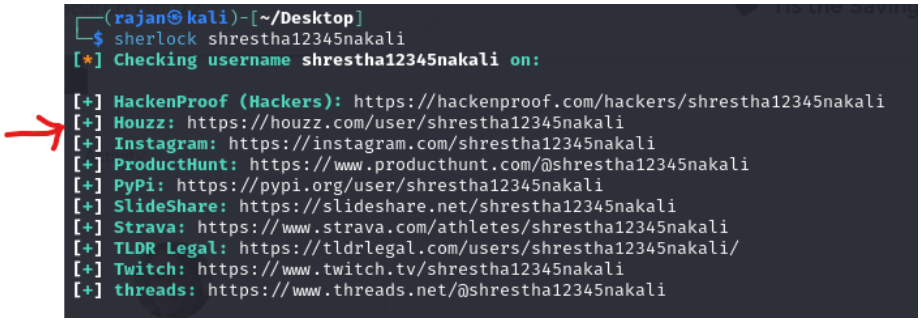
Here we search twitter link of Nakali Shrestha then we get another encoded key for next hint or directory



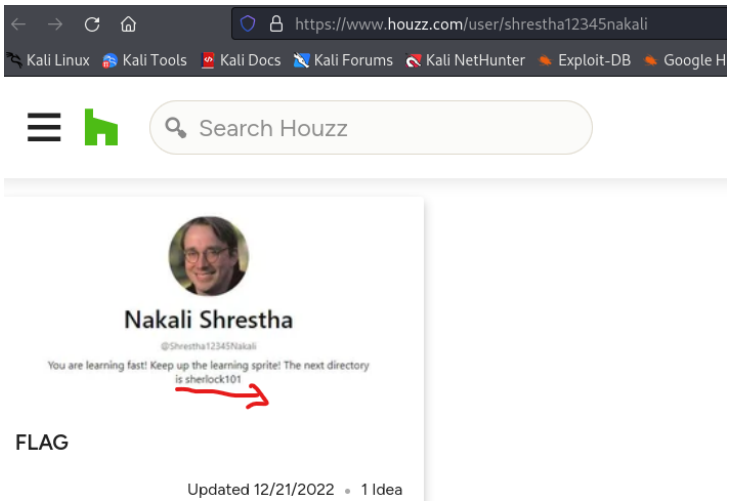
Now we use cyber chef tools to decode this key as this coded in Base64, a common encoding format.



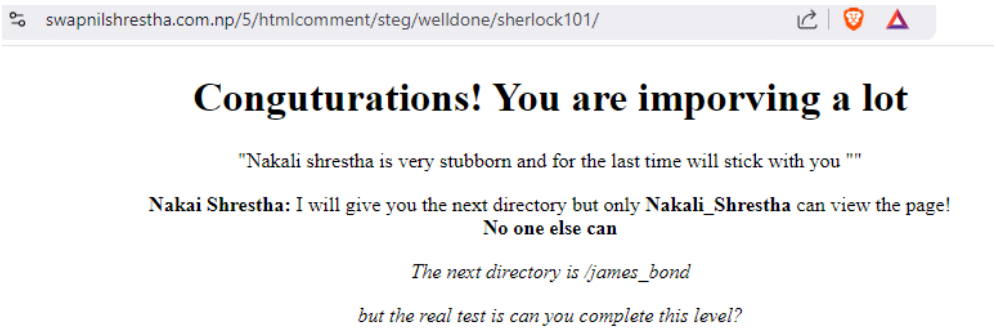
Here is another Username shrestha12345nakali is find out as a result. Now again we used Sherlock to find out related different social media by this username.



Again we try to open all link one by one until get another hints.

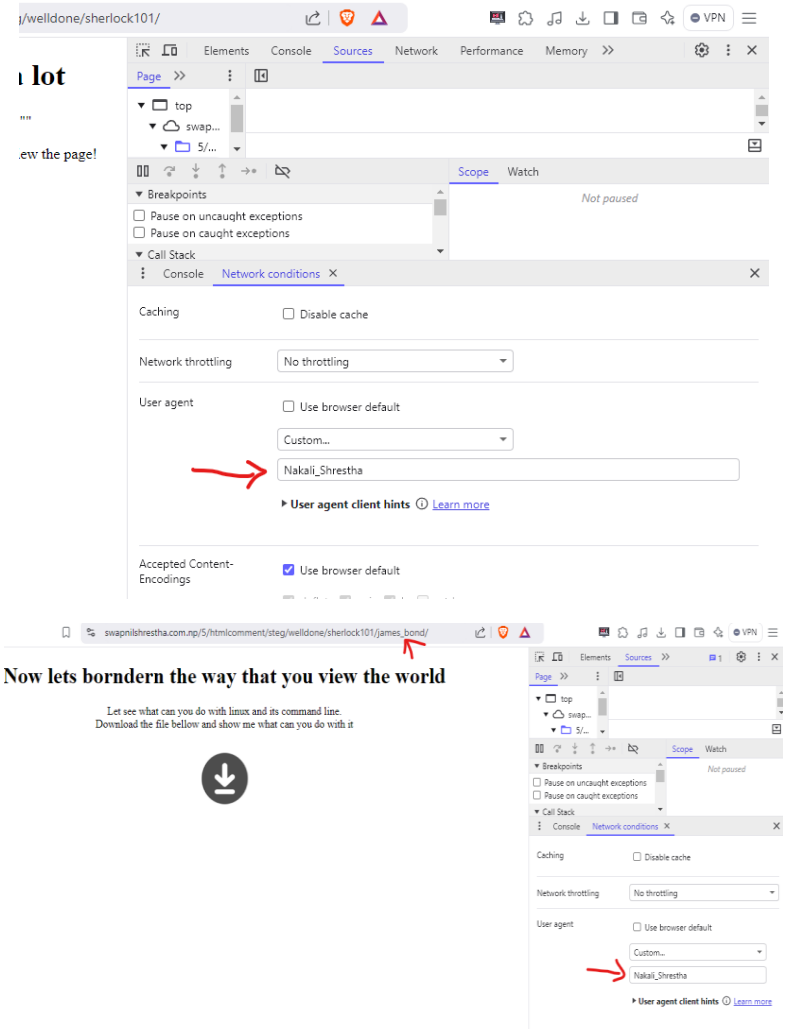


We get another directory (sherlock101) on website houzz.com



We get another page and another hints about next directory (james_bond) but this only work nakali_shrestha.

By pressing shortcut key ctrl + shift + I to inspect page. We are going to change user agent on network condition as nakali Shrestha only work next directory hints(james_bond)



The next directory James_bond is work after change user agent. Download given file on page

After download that file unzip folder

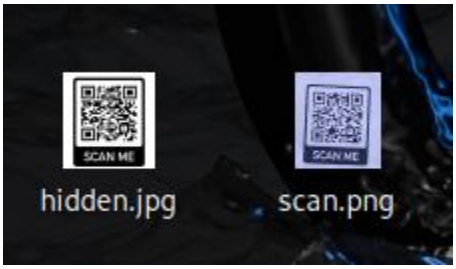
```
┌──(rajan㉿kali)-[~/Desktop]
└─$ unzip -Z cant_fine_me.zip
Archive:  cant_fine_me.zip
Zip file size: 16032 bytes, number of entries: 1
-rw-a--     6.3 fat    18642 bx defN 23-Feb-02 13:55 .hidden.txt
1 file, 18642 bytes uncompressed, 15876 bytes compressed:  14.8%
```

```
┌──(rajan㉿kali)-[~/Desktop]
└─$ ls -la
total 428
drwxr-xr-x  2 rajan rajan   4096 Dec 13 04:54 .
drwx------ 20 rajan rajan   4096 Dec 13 02:58 ..
-rw-rw-r--  1 rajan rajan  18642 Feb  2  2023 .hidden.txt
-rw-rw-r--  1 rajan rajan  81812 Dec 12 07:27 1.jpeg
-rw-rw-r--  1 rajan rajan  64769 Dec 12 07:27 2.jpeg
-rw-rw-r--  1 rajan rajan    490 Dec 13 04:11 NakaliShrestha1.txt
-rw-rw-r--  1 rajan rajan    429 Dec 13 03:37 NakkaliShrestha1.txt
-rwxrw-rw-  1 rajan rajan  16032 Dec 12 08:00 cant_fine_me.zip
-rw-rw-r--  1 rajan rajan  18642 Feb  2  2023 hidden.jpg
-rw-rw-r--  1 rajan rajan     87 Dec 13 03:19 hidden.txt
-rw-------  1 rajan rajan  43887 Dec 12 08:13 scan.png
-rw-rw-r--  1 rajan rajan    500 Dec 13 04:04 shrestha12345nakali.txt
-rw-------  1 rajan rajan 163478 Dec  5 08:32 steganographhy.jpeg
```

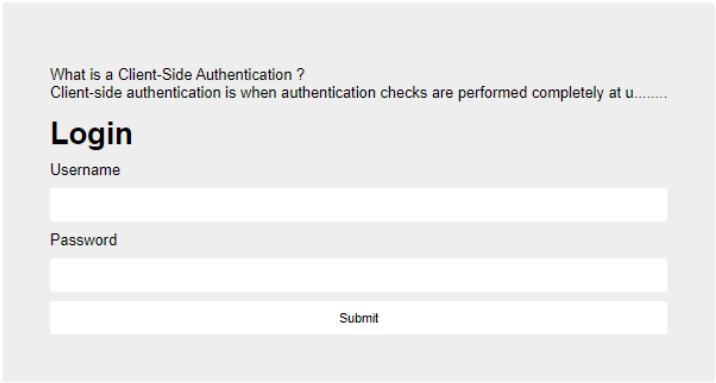
Now hidden.txt file translate into hidden.jpg file

```
┌──(rajan㉿kali)-[~/Desktop]
└─$ mv nohidden.txt hidden.jpg
```

After change into jpg format there is scan file create, after scanning that file another scan image is showed with google map link.

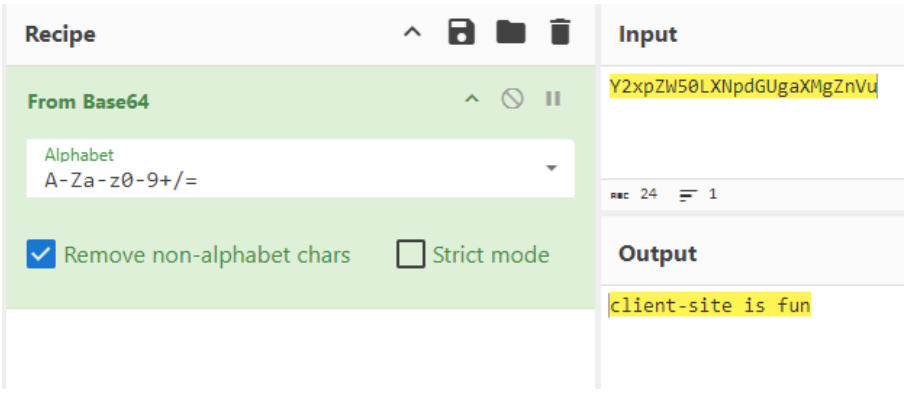


After scanning another scan file its show next directory (glocation) and get next stage of ctf.

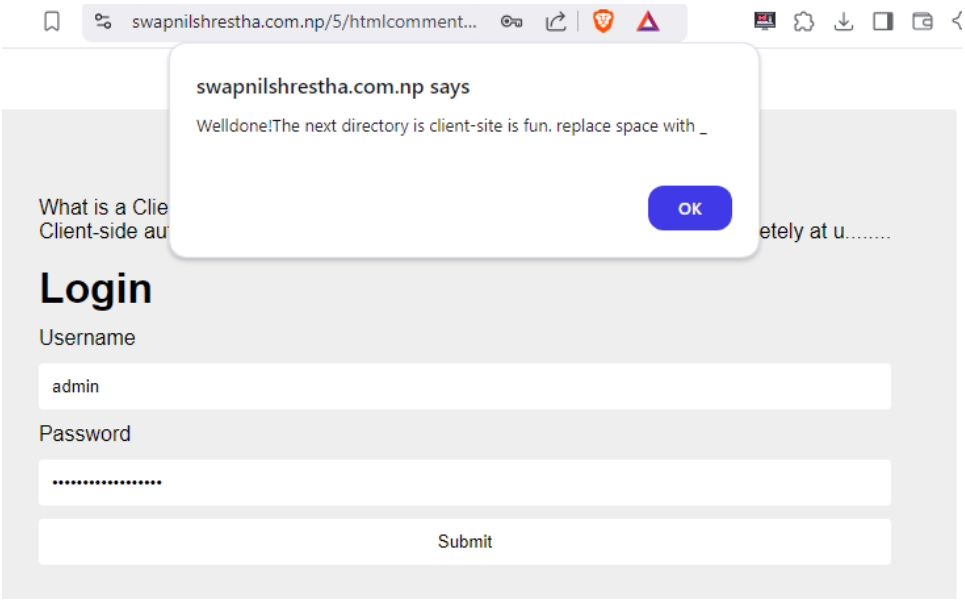


Client side authentication check by inspecting java script file of page.

In java script here is encode key as a password. Then by help of cyber chef we decode the encrypt password.

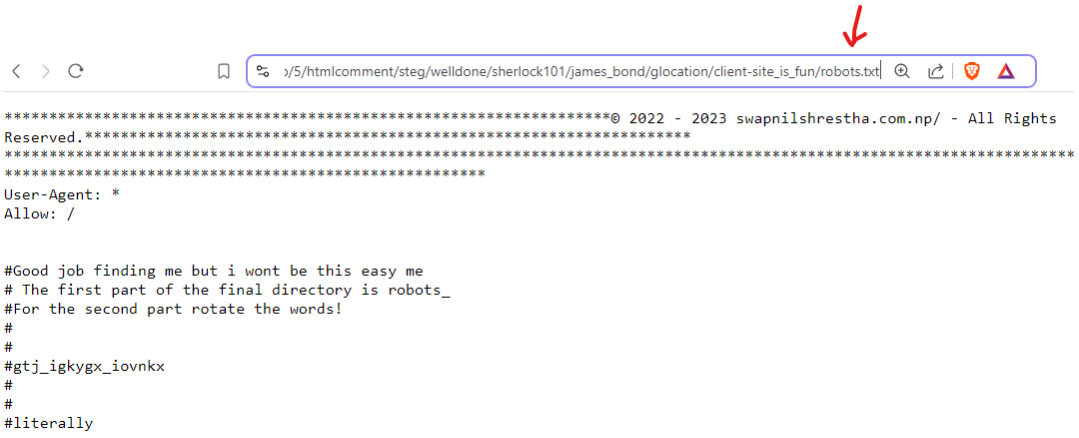


After get password we get next directory for next stage of CTF.



In 1994, a protocol called REP (Robots Exclusion Standard Protocol) was published. This protocol stipulates that all search engine crawlers (user-agents) must first search for that file in the root directory of your site and read the instructions it contains. Only then, robots can start indexing your web page. The file must be located directly in the root directory of your domain and must be written in lower case because bots read that file and its instructions case-sensitive. Unfortunately, not all search engine robots follow these rules.
At least the file works with the most important search engines like Bing, Yahoo, and Google. Their search robots strictly follow the REP and that instruction. In practice, that can be used for different types of files. If you use it for image files, it prevents these files from appearing in the Google search results. Unimportant resource files, such as script, style, and image files, can also be blocked easily with that. In addition, you can exclude dynamically generated web pages from crawling using appropriate commands.
For example, result pages of an internal search function, pages with session IDs or user actions such as shopping carts can be blocked. You can also control crawler access to other non-image files (web pages) by using the text file. Thereby, you can avoid the following scenarios: search robots crawl lots of similar or unimportant web pages your crawl budget is wasted unnecessarily your server is overloaded by crawlers In this context, however, note that that does not guarantee that your site or individual sub-pages are not indexed. It only controls the crawling of your website, but not the indexation.
If web pages are not to be indexed by search engines, you have to set the following meta tag in the header of your web page.

Used robots.txt on url for next directory. And we get first part of next directory and second part of next directory is in encrypted format.



Here we used https://www.dcode.fr/caesar-cipher tools for decode encrypted key

Here we find another parts of next directory