Mission : Recovery

Author : Ala Loghmari
Difficulty : Friendly/Easy

Description

Your machine has been compromised and all of your data has been encrypted, you found the hacker's personal website and decided to investigate it in order to get the decyption key somehow.

Skills Required

- Web Enumeration

Skills Learned

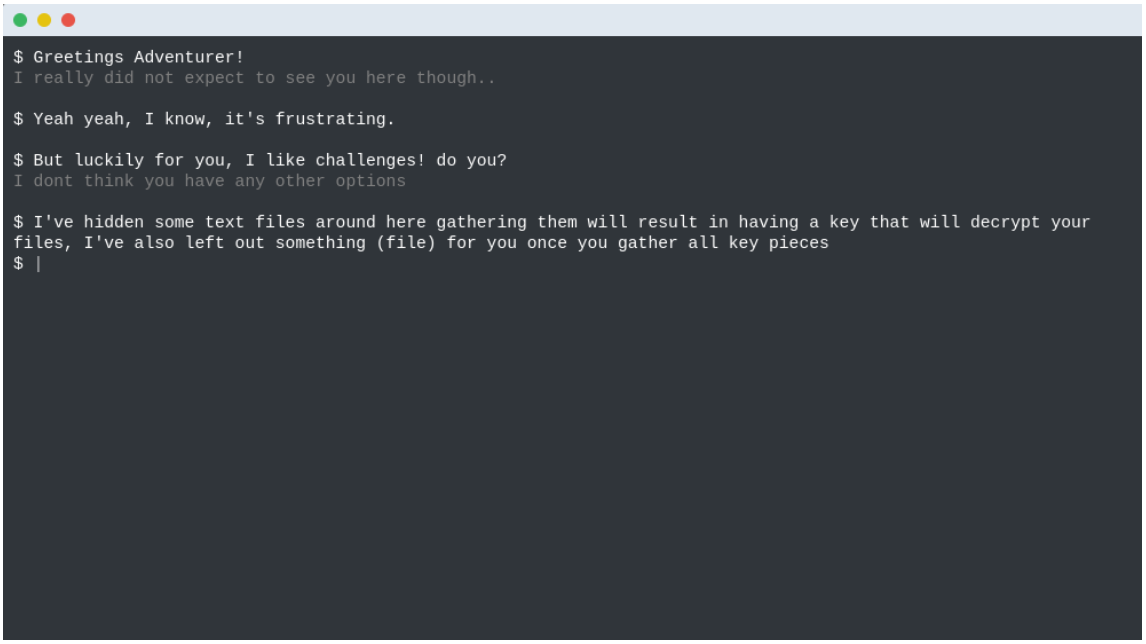
- Web Enumeration & Fuzzing
- Encryption / Decryption

References & Guides

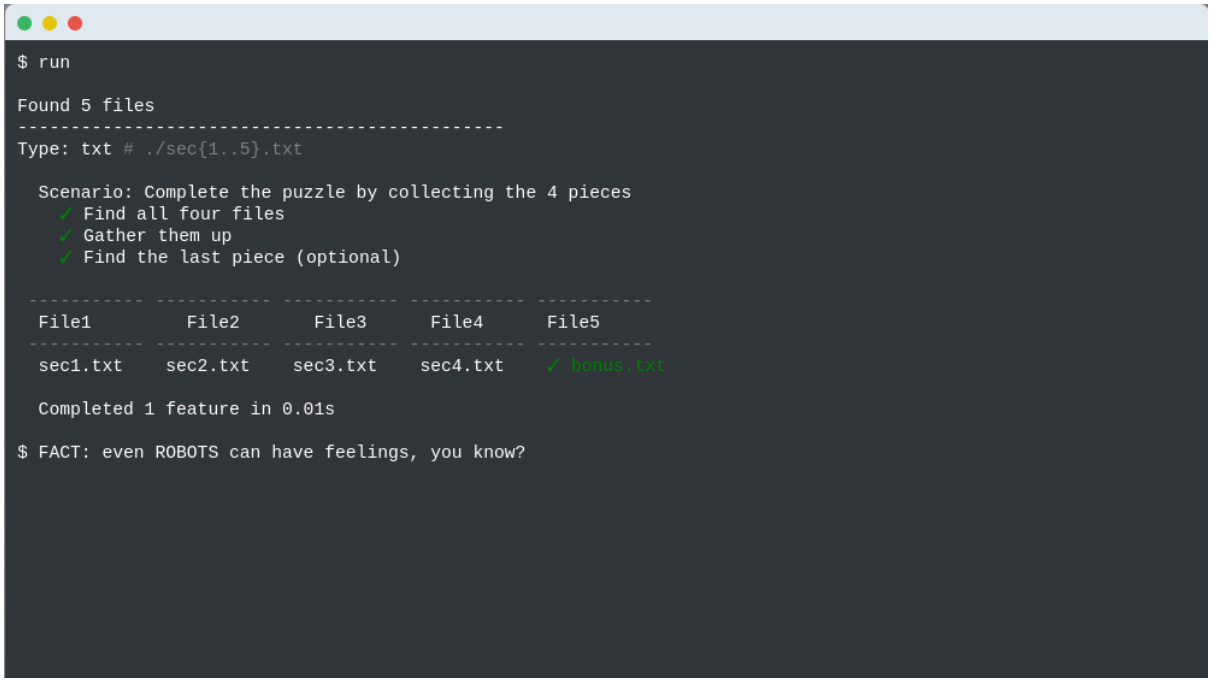
- https://www.cloudflare.com/learning/bots/what-is-robots-txt/ (Robots.txt)
- https://bitcoinwiki.org/wiki/base58 (Base 58)

Reconnaissance

Navigating to the task's website we get a look-a-like terminal interface. Reading through the text that's being written, we figure out that the text is from the threat actor.



So, indeed, this is the personal website of the hacker that encrypted our files and from what it seems we have to gather up some sort of files that will help us getting the key to decrypt the files on our system.



Okey, so, let's sort all of this out, we need to :

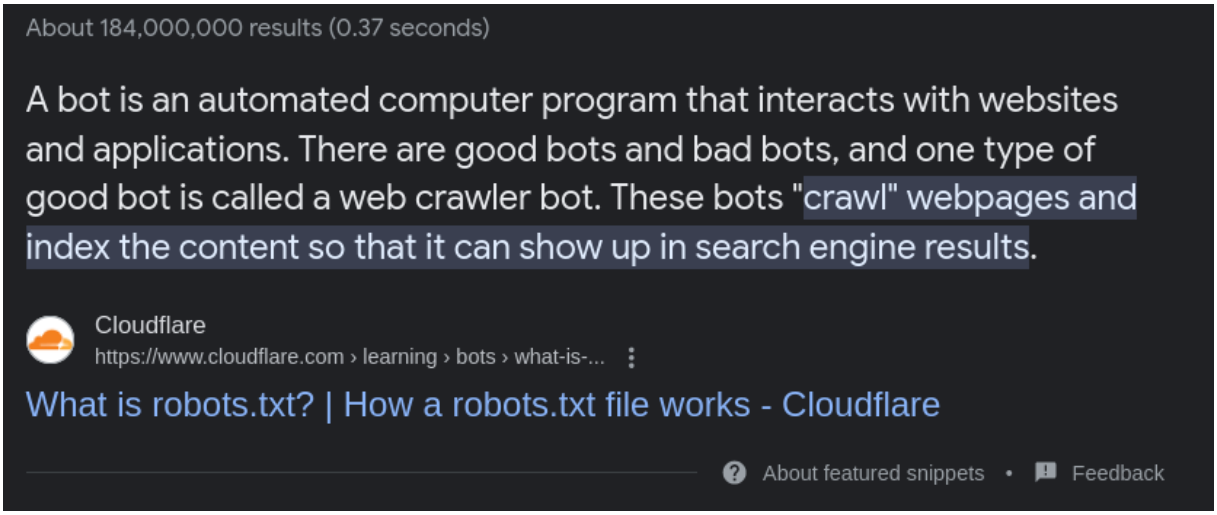
- Gather out the 4 txt files.
- Find a bonus txt file that is not mandatory in the completion of the task.
- Put the 4 pieces found in the txt files together to get our key.

Enumeration

The hacker left a fact for us mentioning robots, at first glance, it doesn't really make sense.
Hitting CTRL U to view the page source code we find out something interesting, a comment left for us.

```
43   <br>
44 </div>
45
46
47
48 <!-- What do robots have to do with web pages? Google it !-->
49
50
51 </body>
52 <footer>
53
```

Googling the "What do robots have to do with web pages?" result in a cloudflare article.

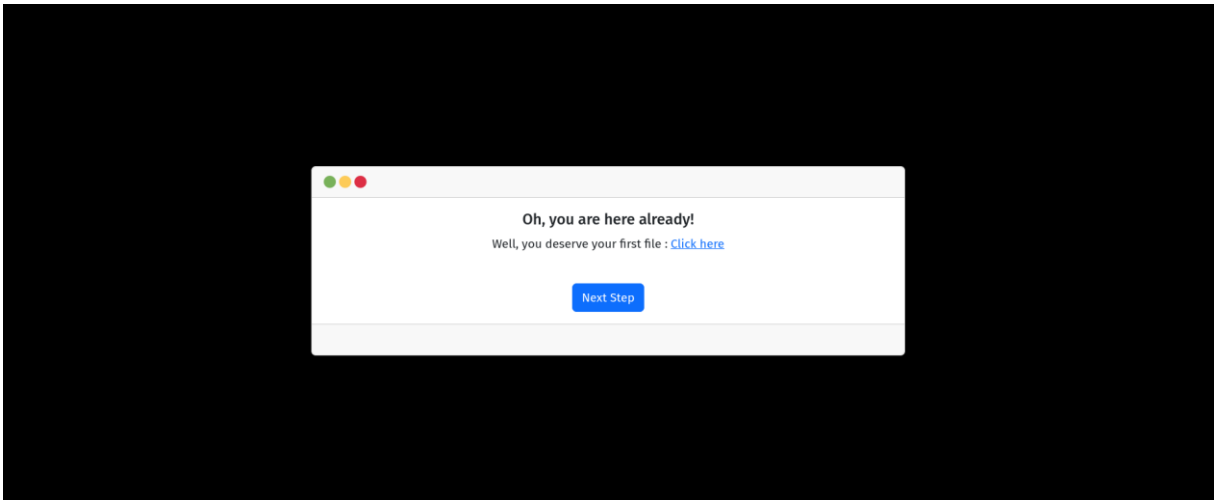


Interesting, so basically a robots.txt is a file that can exist on web servers to tell the search engines what they should and should not show up in a search results.

Checking the /robots.txt, we get a disallowed entry to /h3ll0in7rud3r.

```
User-agent: *

Disallow: /h3ll0in7rud3r
```

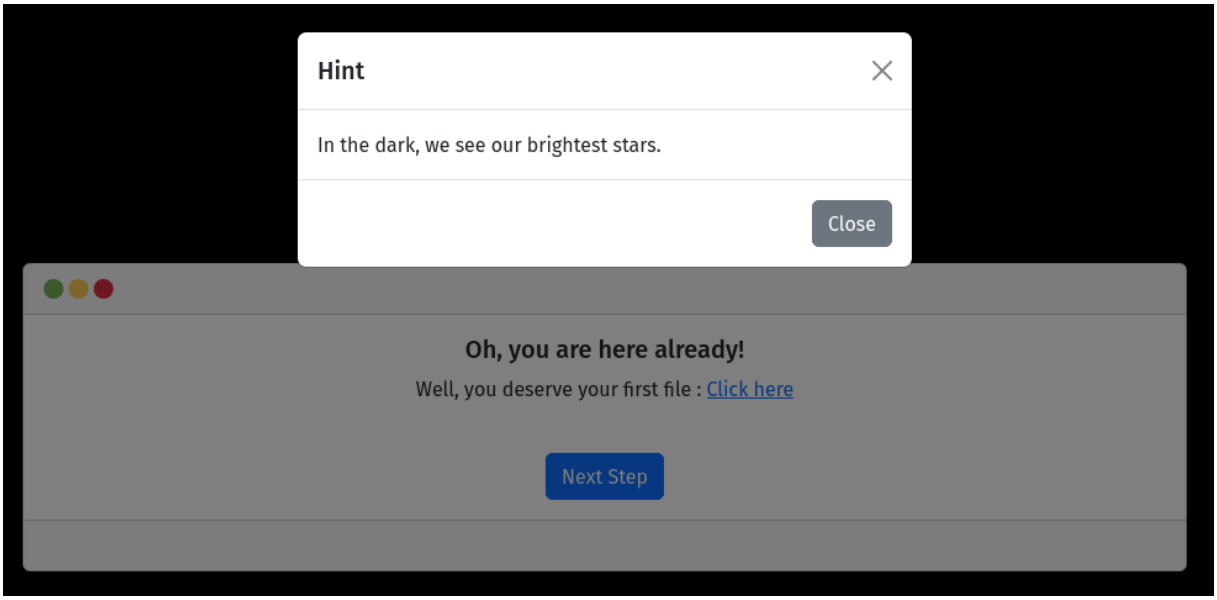
Navigating to the disallowed route.



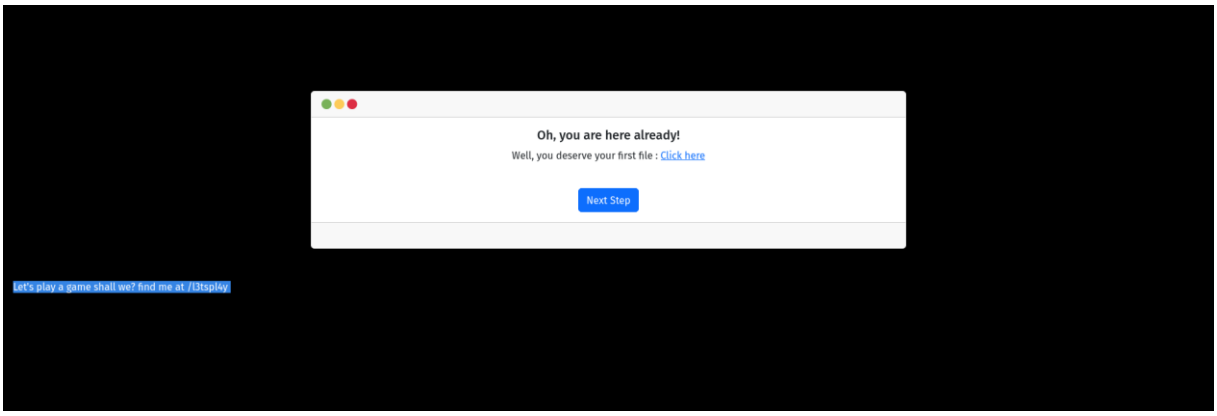
We have our first part of the decryption key !

Sec1.txt content

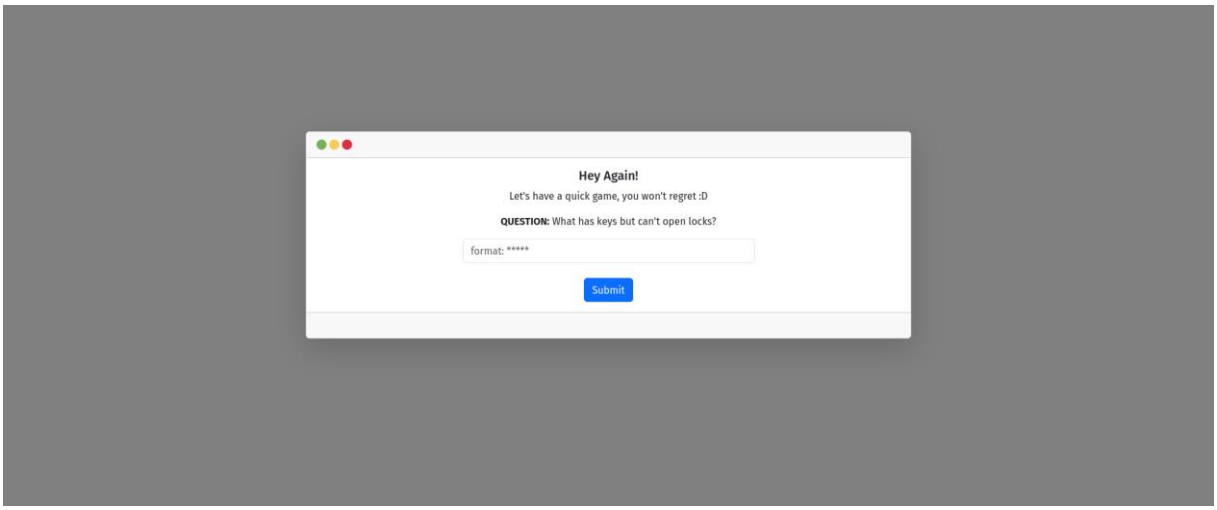
Hiting the « **Next Step** » button, a hint appears.



Something seems to be hidding here from what the hint says as it's mentioning "dark" and we have a black color background.



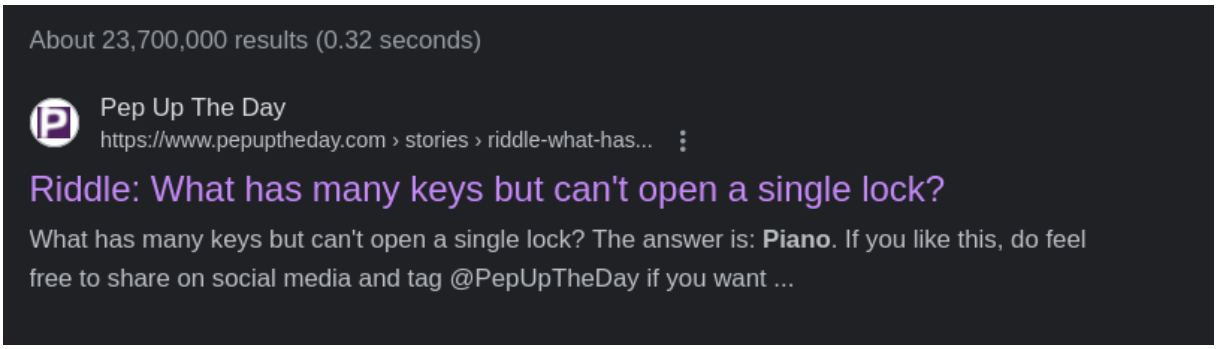
As we thought, a black colored message is hidden, asking us to play a game at /l3tspl4y.



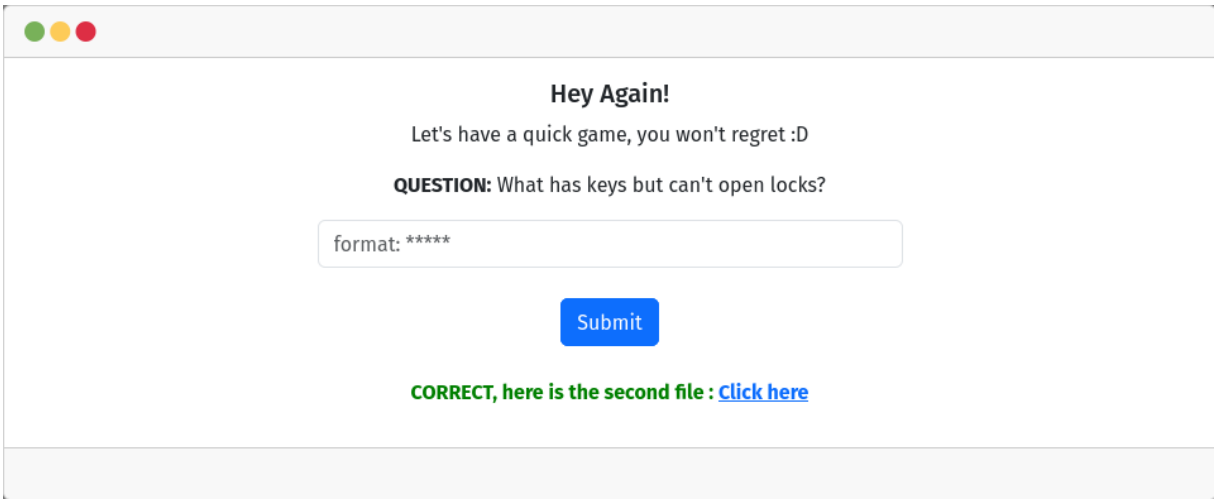
No black backgrounds anymore, nice !

This time, we got a question to answer : “What has keys but can’t open locks?” .

Guessing that would take quite some times why don’t we use the tools that are free and at our disposal? Google, correct !



Well, Piano it is, it wasn’t that hard actually.



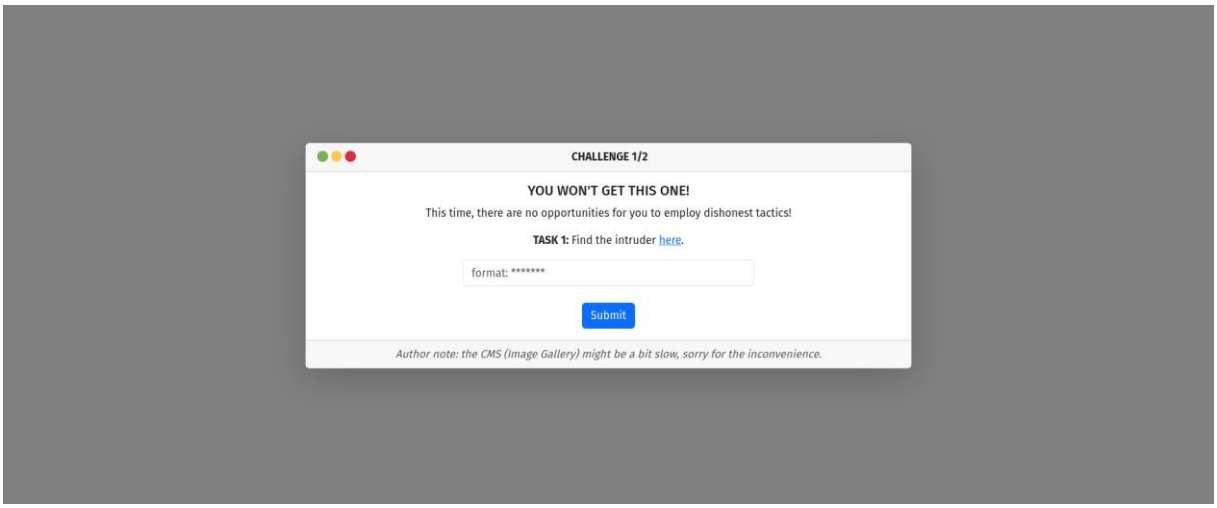
And here the second file is (sec2.txt) !

```
s7_inT

I know that you have cheated! that's why we're going to play another game but this time it's, HARDER!

find me at /y0ugon4r3gr37it
```

Sec2.txt content

Oops, we got caught, and,

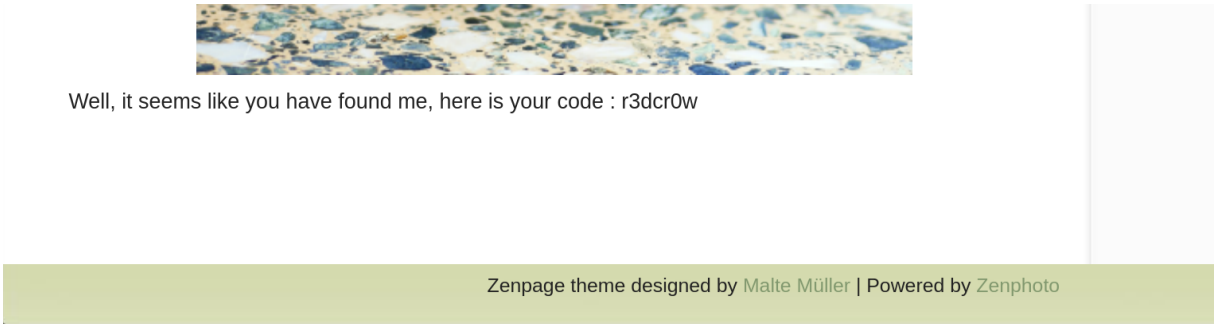
We’re getting in some sort of a maze of challenges but as long as we get our key !



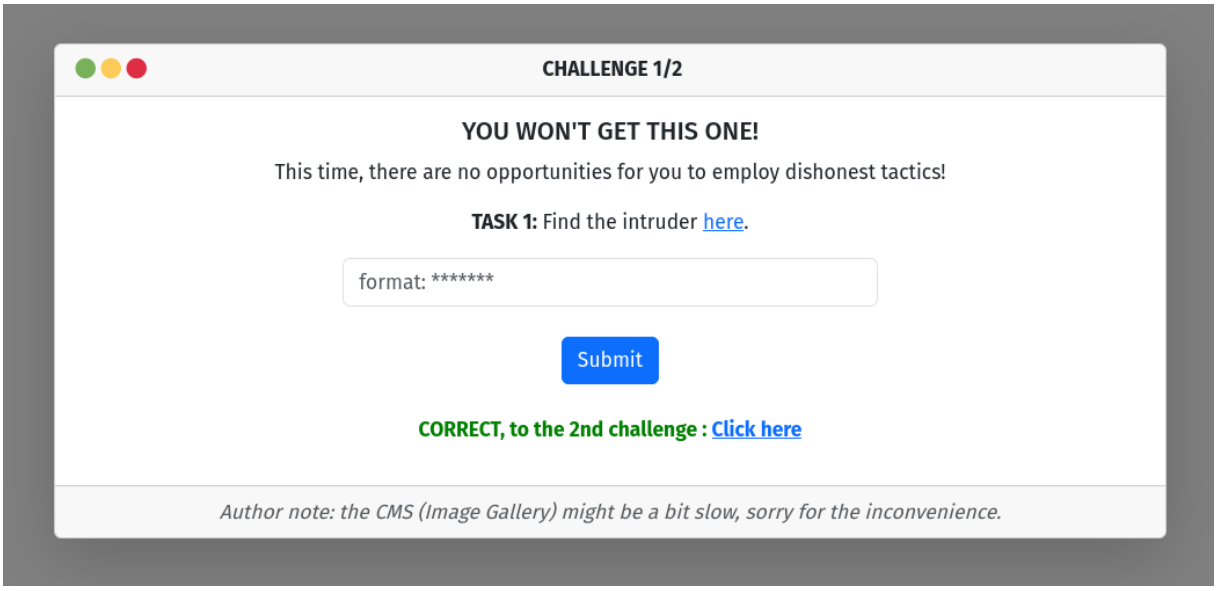
Navigating to /y0ugon4r3gr37it we have another challenge to solve.

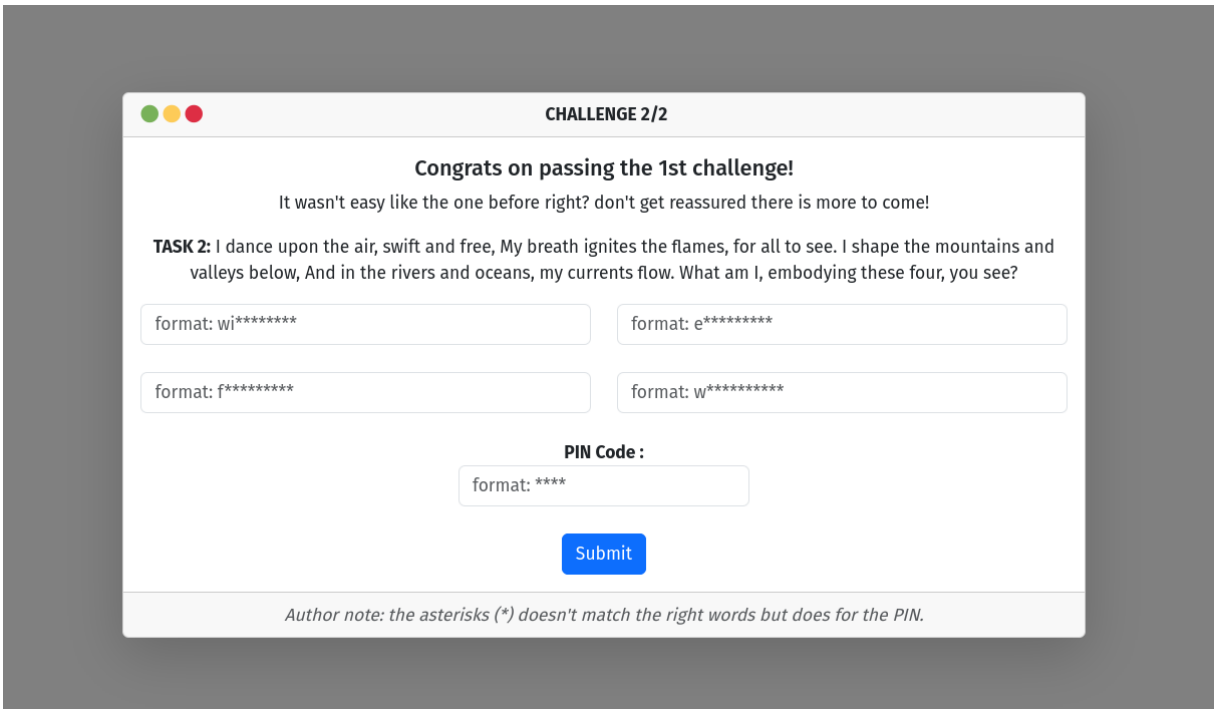
Clicking on “here” redirects us to some kind of a photo gallery CMS.

It seems like we have to through every single image looking for an “intruder”.



And there we have it, we got the code that allows us to move to the 2nd challenge.





For the 2nd challenge we have been give not 1 but 5 answers to submit. And from what the author says the asterisks doesn't match the exact words so we won't be able to relay on them only the pin code does match.

The Task Description:

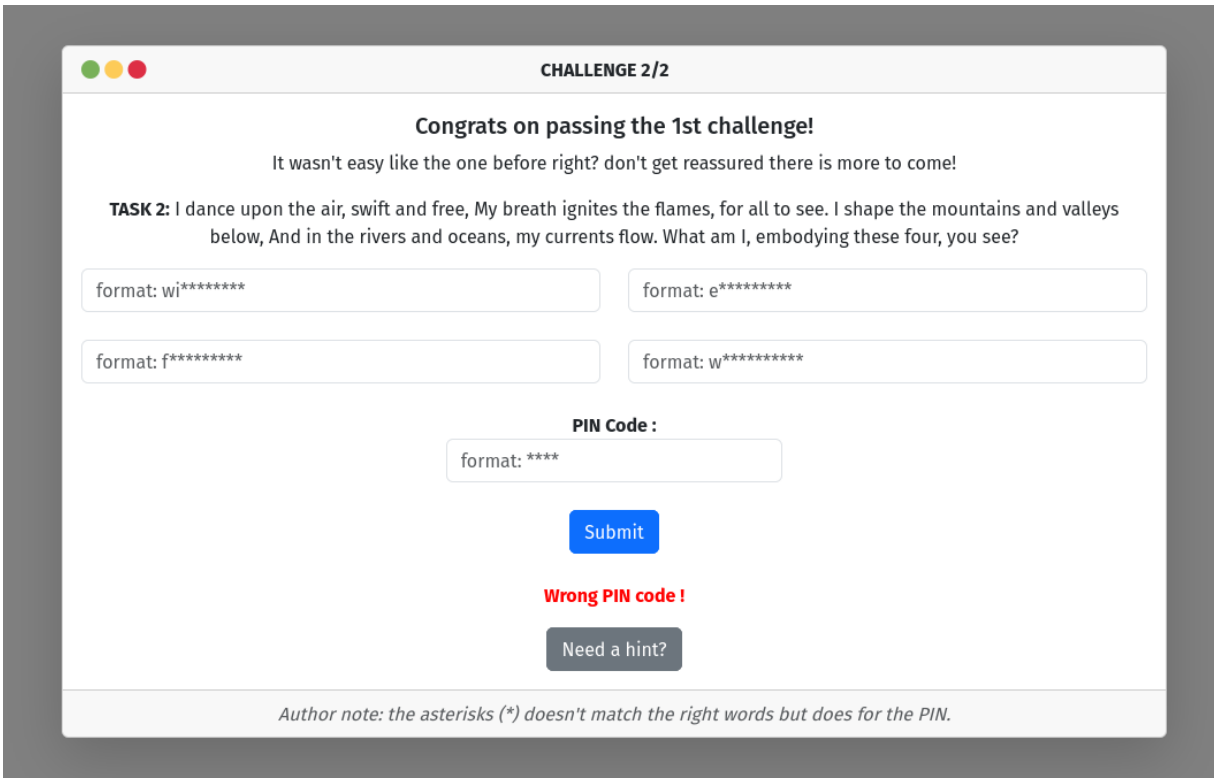
"I dance upon the **air**, swift and free, My breath ignites the **flames**, for all to see. I shape the **mountains and valleys** below, And in the **rivers and oceans**, my currents flow. What am I, embodying these four, you see ? "

Analysing the given riddle, we see that it's talking about the 4 nature elements :

1. Wind
2. Earth
3. Fire
4. Water

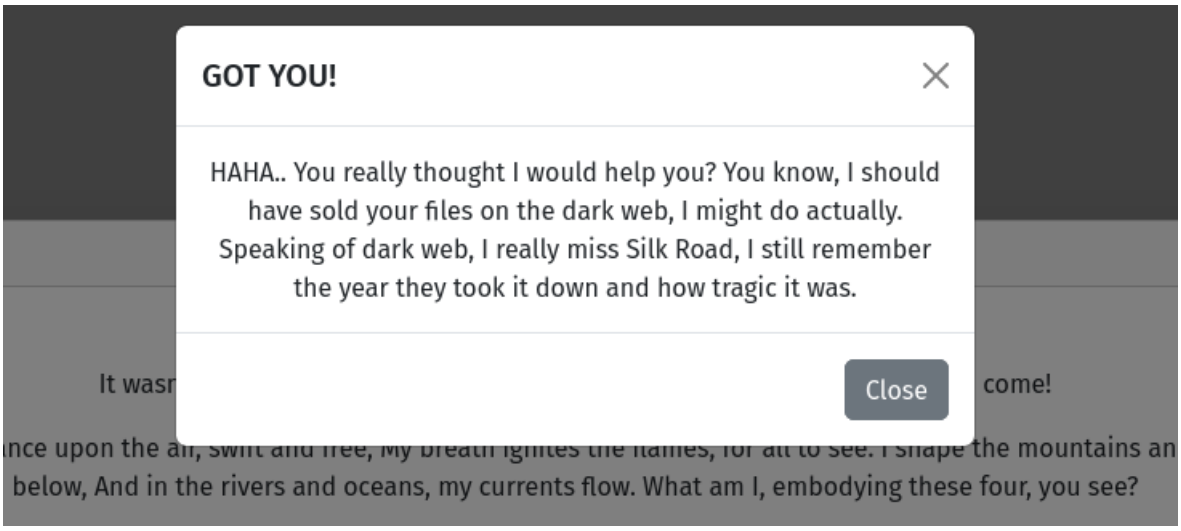
Looking through the page even more we can't seem to find the pin code that is being asked for.

As a habit, I always try intuitive things if I get to a dead end, for instance, 0000 as a pin code.



A “Need a hint?” suddenly appears after submitting the answers.

Clicking on the button, we get trolled by the hacker.



Inside of the hacker’s taunting message we see him mentioning Silk Road, an online black market that was taken down by the FBI on 2013.

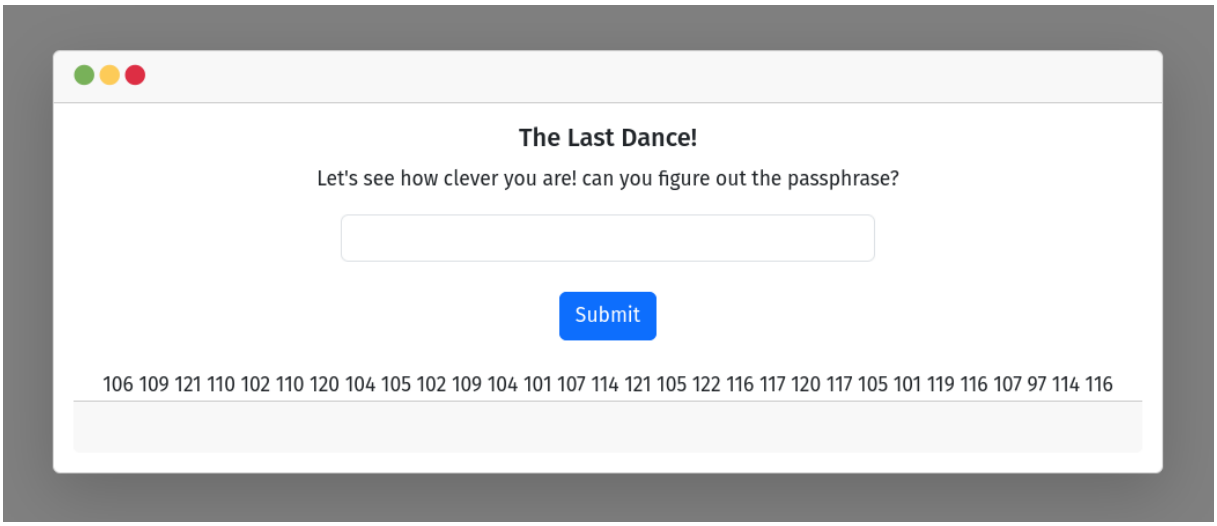
But what does that have to do with this? Reading the author’s message one more time we remember that the asterisks does match the PIN code but not the other answers, which leads us to a 4 long answer.

Trying the year 2013 as the hacker’s message also mentioned the take down of Silk Road, we succeed into submitting all 5 right answers.

```
0_7h3

Okey, enough playing, there is only 1 part of the key left.

Find me at /f1n4lst4g3
```

Sec3.txt content

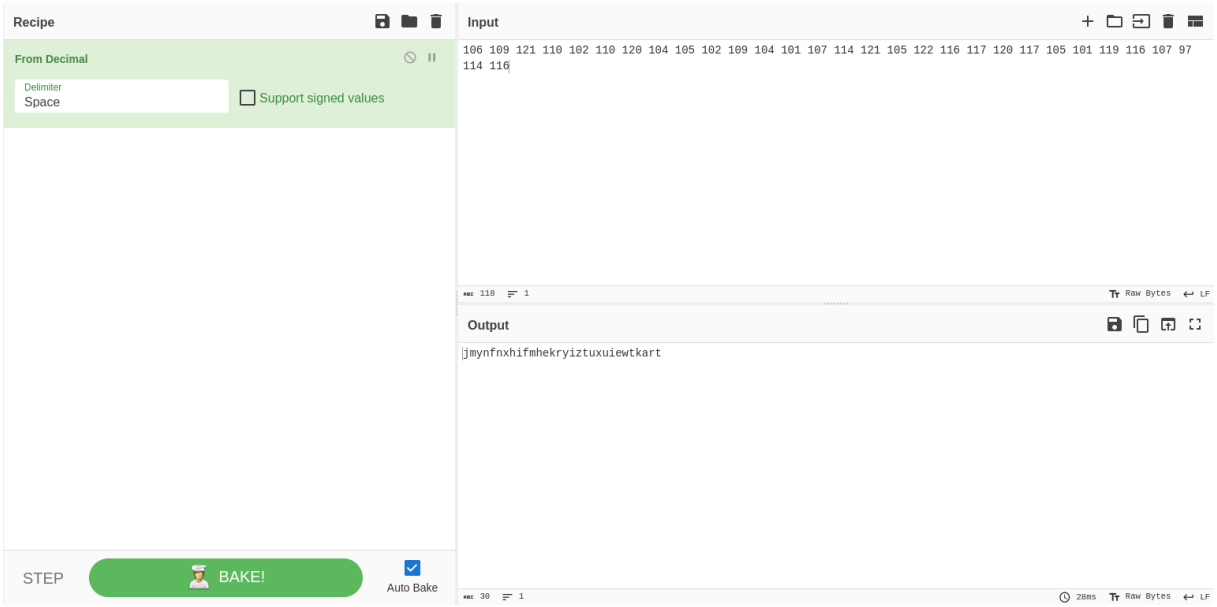
Okey, the last key part, here we go!



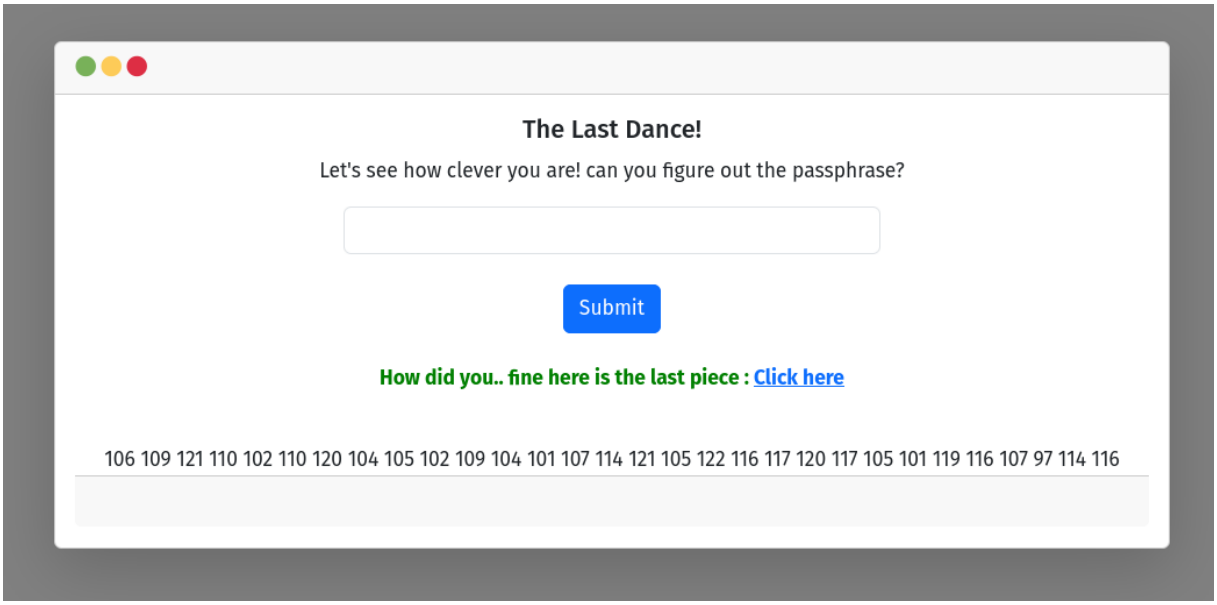
So apparently, we have to figure out how to get the passphrase in order to proceed.

Having only these numbers at our disposal we figured out that these numbers are ASCII characters and for each ASCII character is assigned a character in the alphabet.

There are plenty of methods to decode the characters as creating a python script but there are also websites on the net that can do the job for us, Cyberchef is our savior here.



There we go, we have our passphrase, submitting it will result in the last piece.




```
KhtncrYxhzdwtQ8

You really thought that I'll give you the last part that easy?
I've coded the last piece n times, you need to figure out how many times i did (figure out n) and the algorithm used,

I hope you have a good Base in cryptography!


+ Bonus: Gather the 4 pieces of the key and head to /bonus.
```

Sec4.txt

Yeah, of course, why would it be that easy.. Alright, we have our last piece but it’s encoded so many times using a specific algorithm so it becomes that.

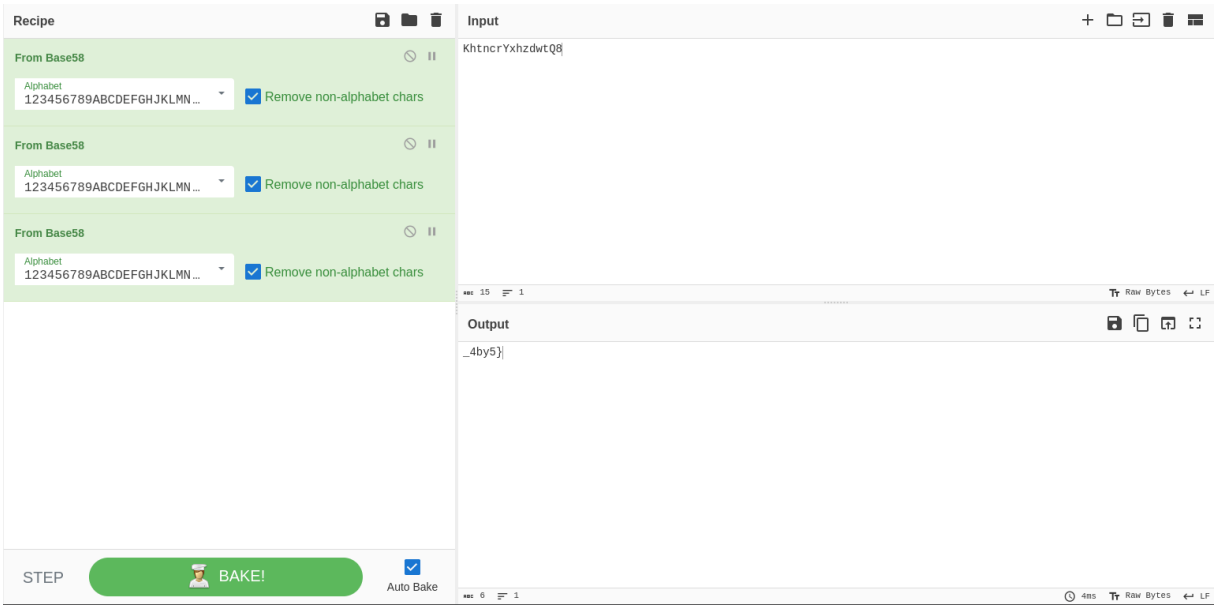
Even Cyberchef couldn't figure out what was the algorithm used here.

Having a closer look into the sec4.txt something seems odd, the word "Base" have its first character as an uppercase.

That might be the hint that will help us decode it !

Trying all the Base algorithms over and over will result in finding the correct algorithm as well as the number of times that the last piece got encrypted.

- Algorithm : Base58
- Number (n) : 3



We finally got the 4th piece !

Putting them all together will get us the key : **Securinets{l0s7_inT0_7h3_4by5}**

The sec4.txt mentions /bonus as well, I'll let you to it 😊

Thank You For Playing and Long Live Palestine

@ Ala Loghmari