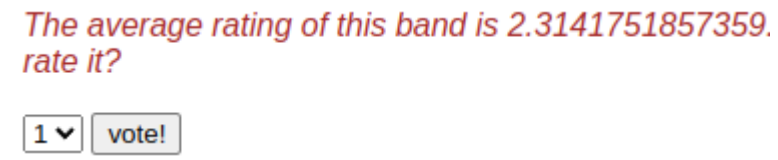
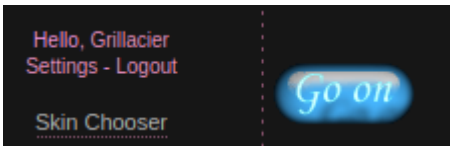
HackThisSite - Realistic

Level 1

On inspecte la page et on modifie la valeur d'une des options de vote du dernier groupe. Cela augmentera leur score pour les placer en première place :

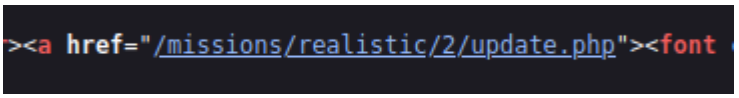


On clique sur vote! :

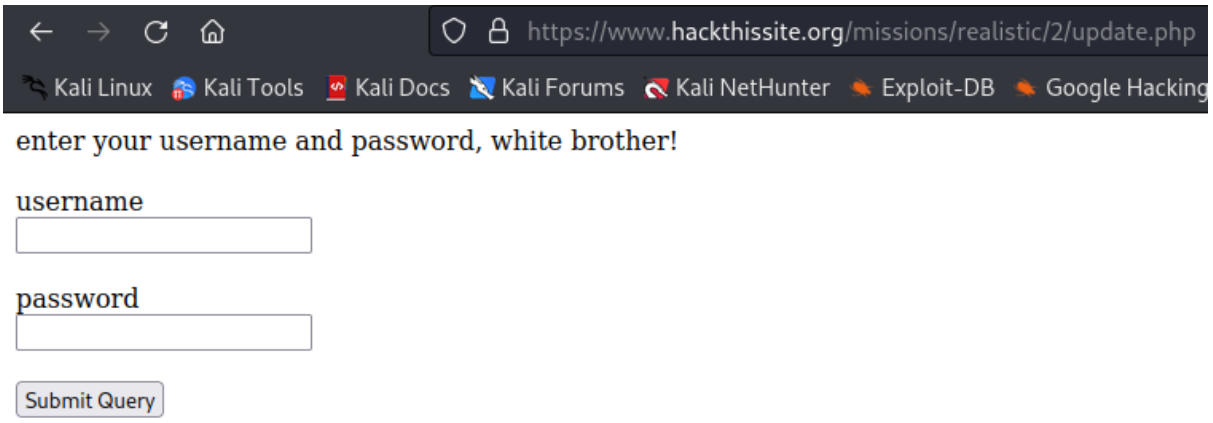


Level 2

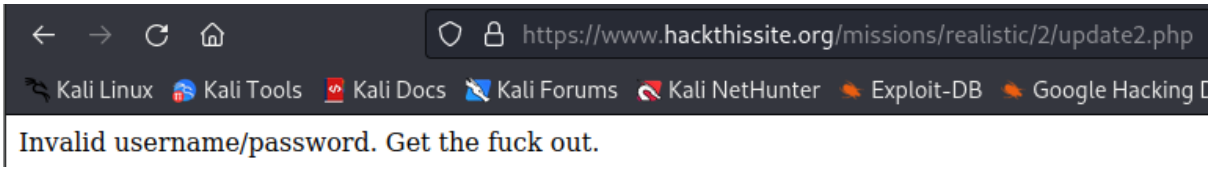
On affiche le code source de la page :



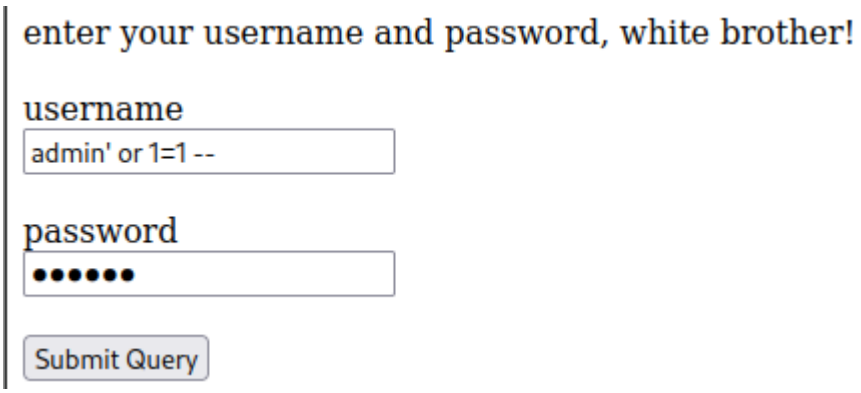
On accède à la page update.php :



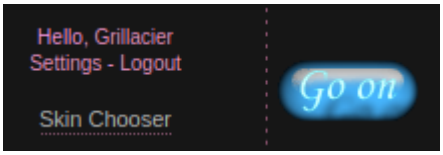
Rentrer des identifiants erronés nous envoie à cette page :



On écrit une commande SQL équivalente à "SELECT password FROM table WHERE name = 'admin' OR 1=1" :



Les “--” signalent le début d’un commentaire, ce qui ignore ce qu’on entre dans la ligne “password”. On clique sur Submit Query :

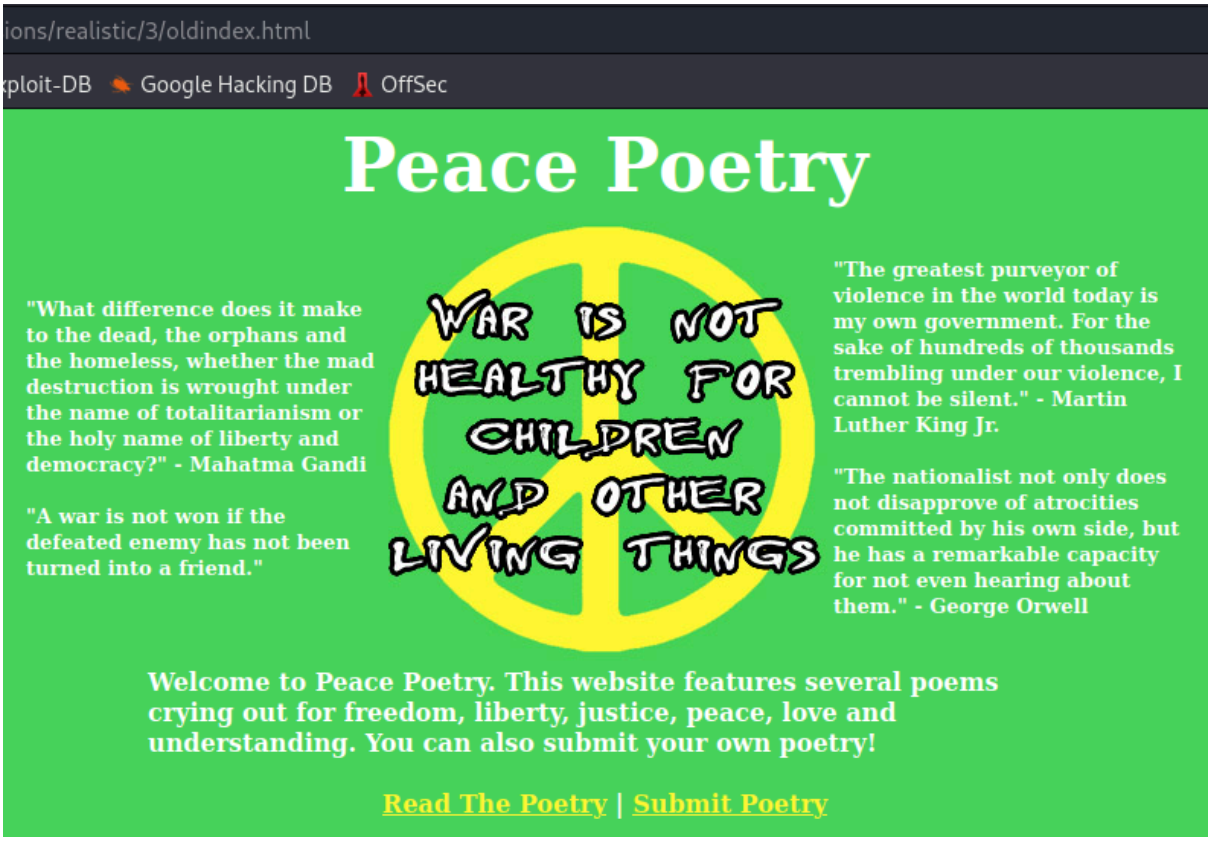


Level 3

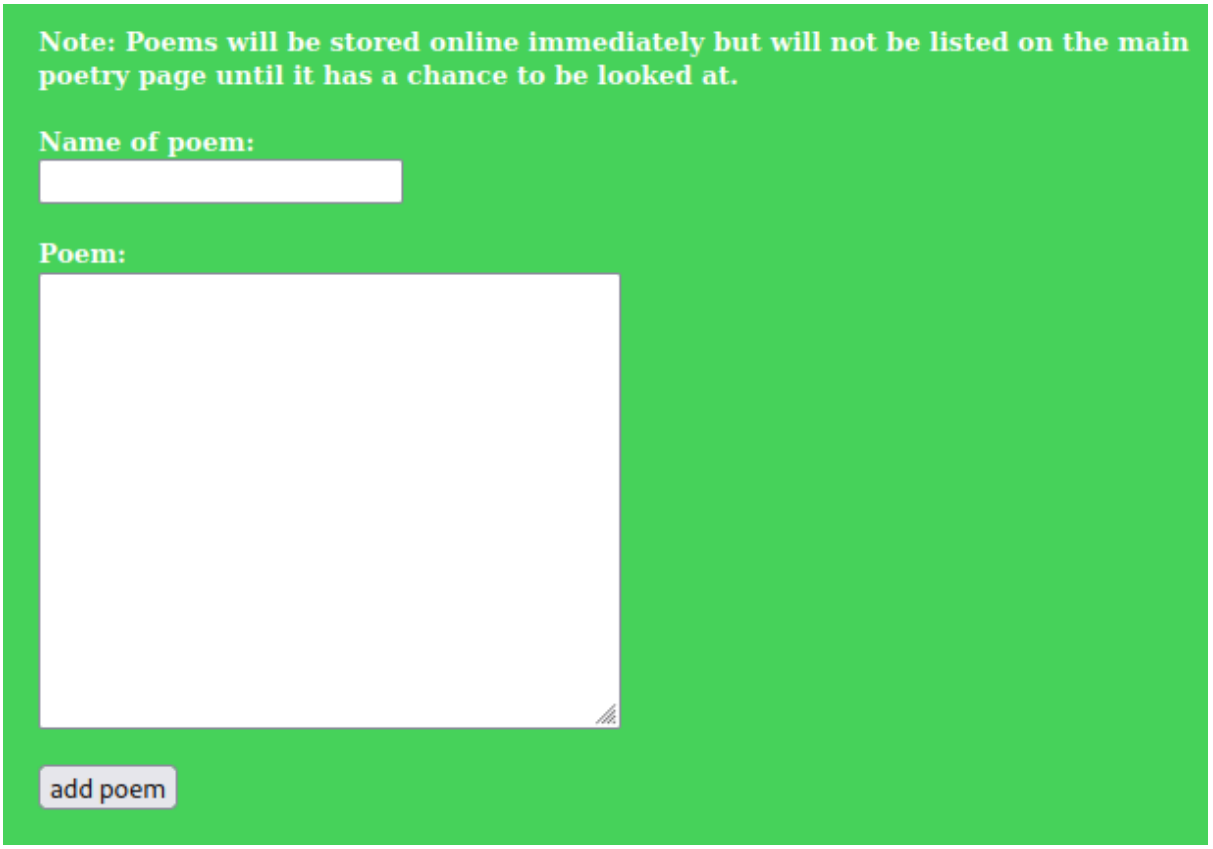
En inspectant la page, on trouve un commentaire :

```
<!--Note to the webmasterThis website has been hacked, but not totally destroyed. The old website is
still up. I simply copied the old index.html file to oldindex.html and remade this one. Sorry about the
inconvenience.-->
```

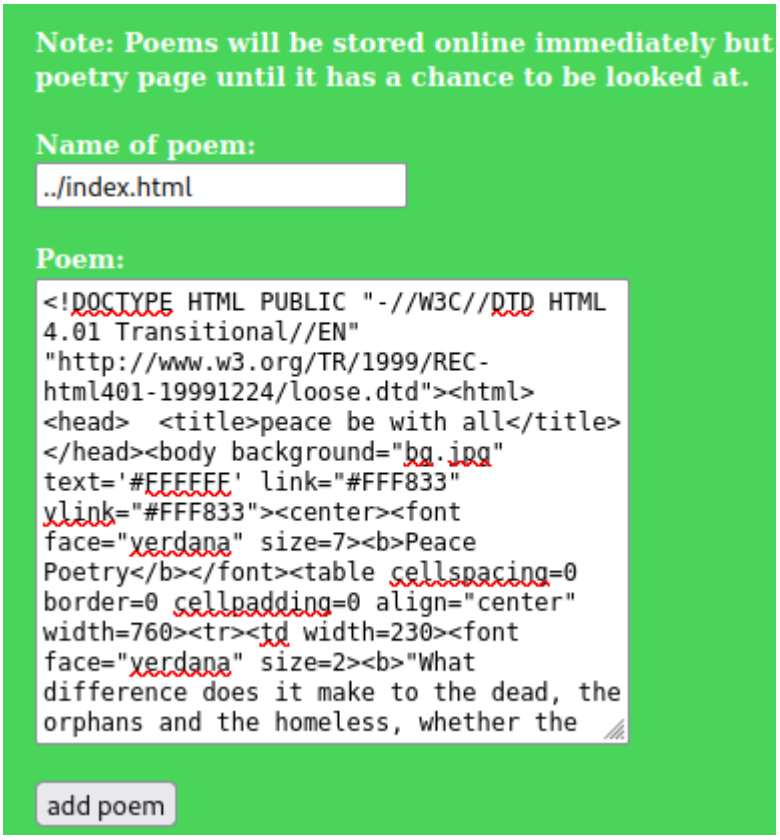
On découvre que l’ancienne page d’accueil se trouve dans oldindex.html :



Dans Submit Poetry, on trouve un formulaire :



On lui donne comme nom, le chemin vers la page d'accueil qu'on veut remplacer. Dans le champ "Poem", on colle le tout le code de la page oldindex.html :

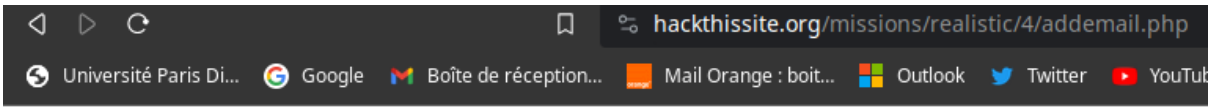


On clique sur add poem :

Level 4

On voit qu'on peut ajouter une adresse mail :

Essayer d'ajouter une adresse mail non valide nous montre ce message :



Error inserting into table "email"! Email not valid! Please contact an administrator of Fischer's

Le message d'erreur parle d'insertion et de table, on devra donc réaliser une injection SQL.
On réalisera l'injection à partir de cette page :

Le "?category=2" indique la présence de code SQL.

Yes, these are authentic alligator shoes, made

$140

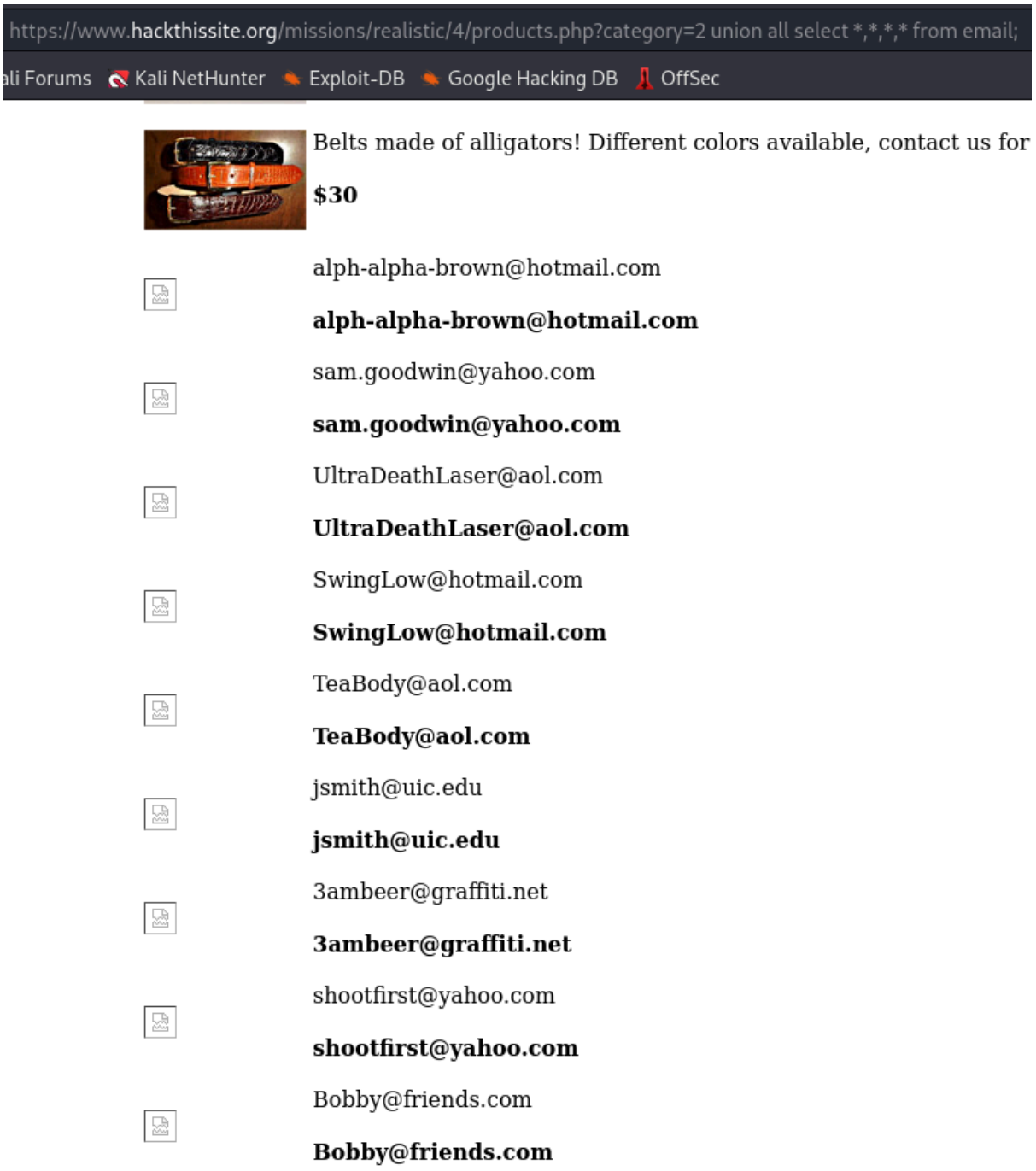
Alligator purses! We tear the skin off alligator

$70

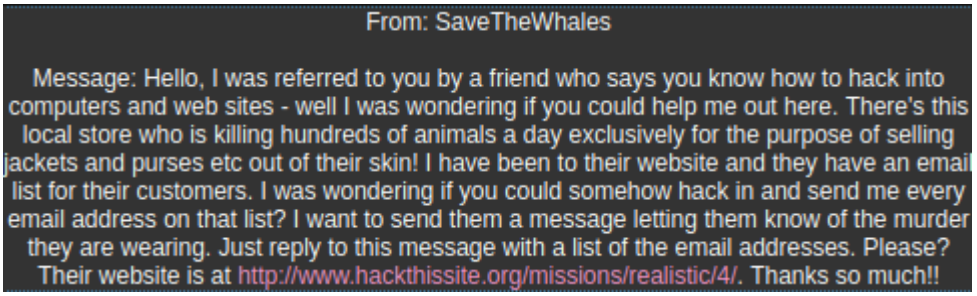
Belts made of alligators! Different colors avail

$30

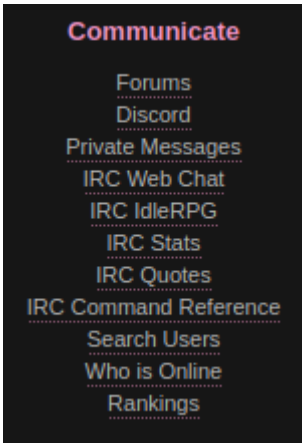
La page semble contenir trois colonnes : les images, la description de l'article et le prix. De plus, on ajoute une quatrième colonne pour les adresses mails qu'on peut ajouter à partir de la page d'accueil. On réalise un union all select sur la table email :



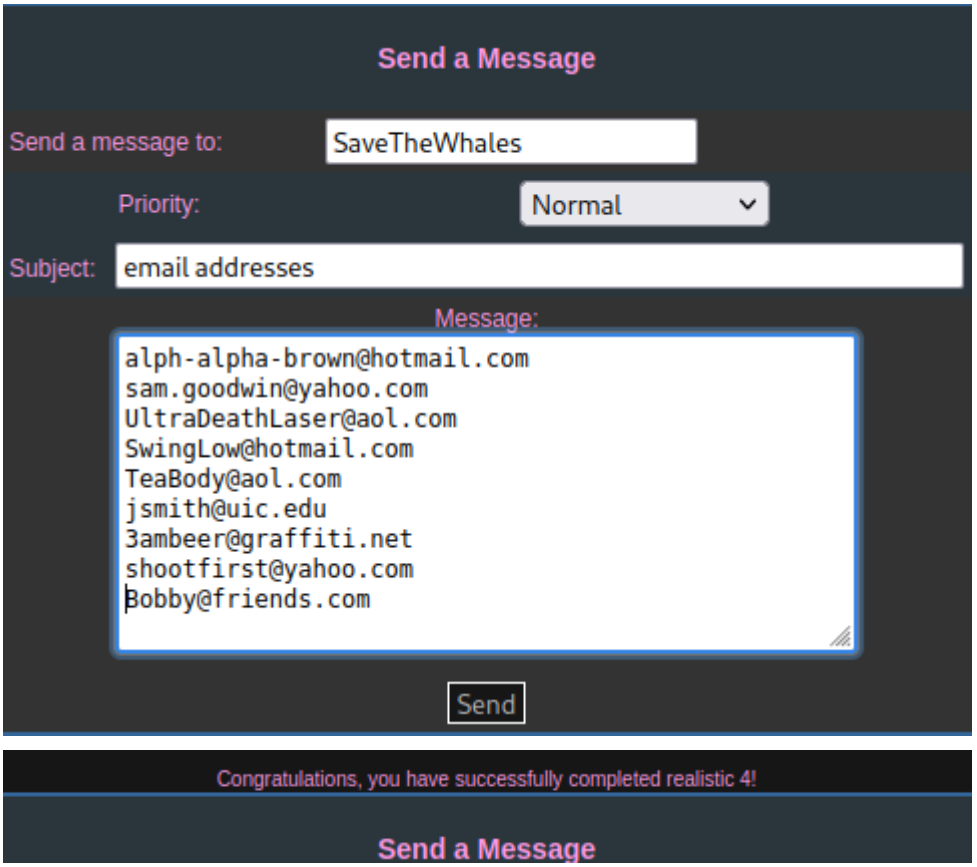
On obtient les adresses mails.



Il faut envoyer les adresses à l'utilisateur SaveTheWhales, on clique sur "Private Messages" dans la catégorie "Communicate" de hackthissite :

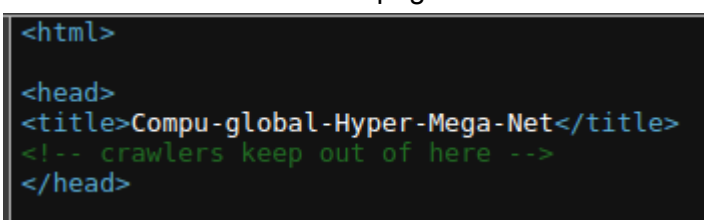


On cherche SaveTheWhales, on clique sur son nom et on lui envoie les mails trouvés :



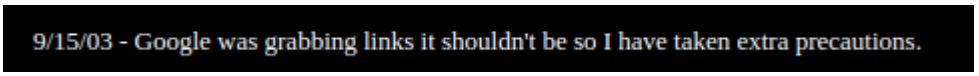
Level 5

Afficher le code source de la page d'accueil nous montre ce commentaire :

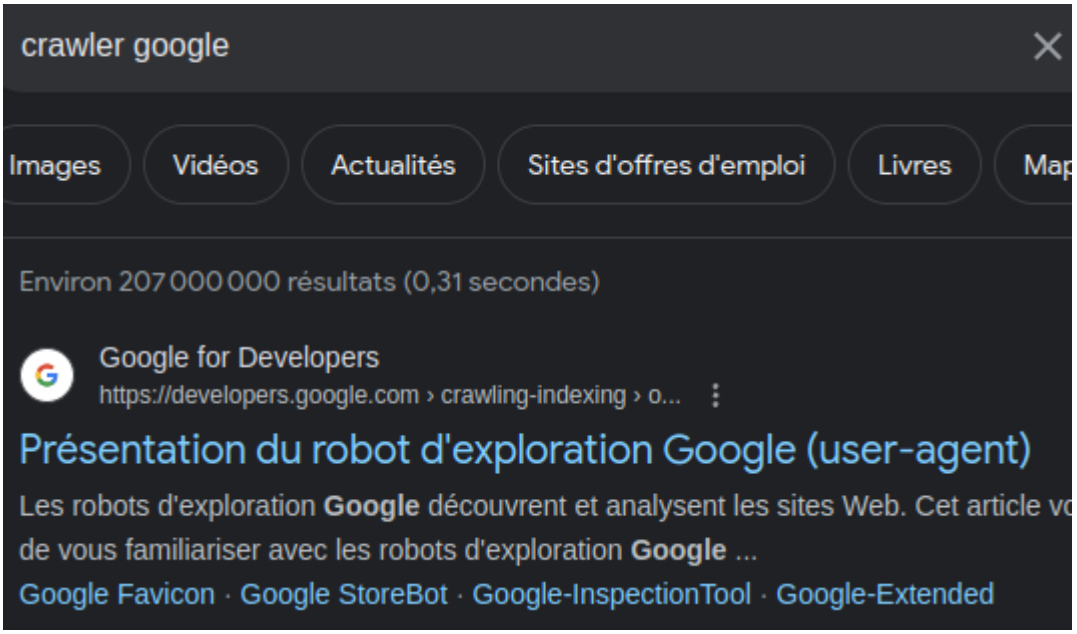


```
<html>

<head>
<title>Compu-global-Hyper-Mega-Net</title>
<!-- crawlers keep out of here -->
</head>
```

De plus, on a ce message sur la page News :

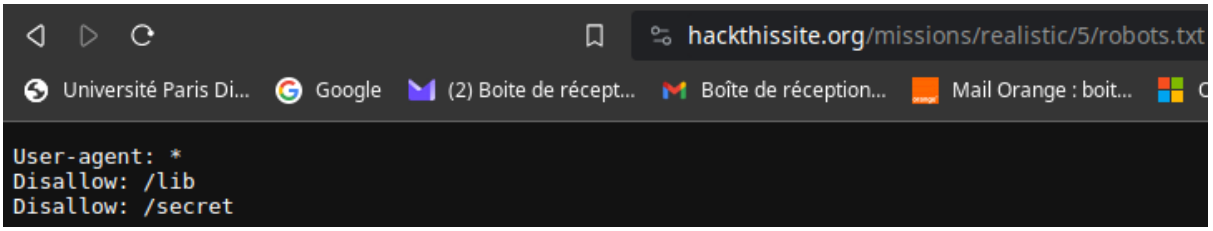


On fait donc une recherche avec les termes “crawler” et “google” :

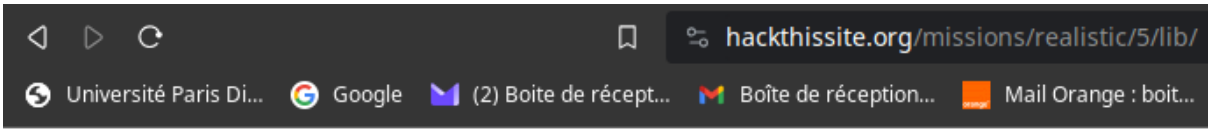


Sur le premier lien, on apprend l’existence d’un fichier robots.txt :

On essaye de s’y rendre à partir de la racine :



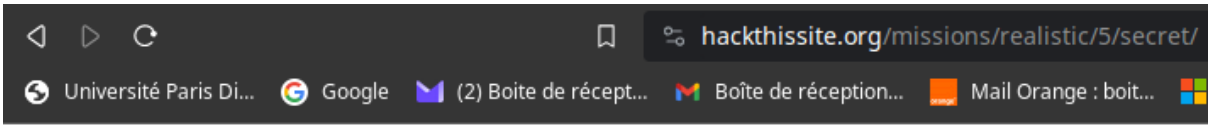
On découvre que les répertoires lib et secret sont masqués pour tous les utilisateurs. On se rend dans lib/ :



Index of /missions/realistic/5/lib

Name	Last modified	Size	Description
Parent Directory		-	
hash	2013-12-30 05:28	11K	

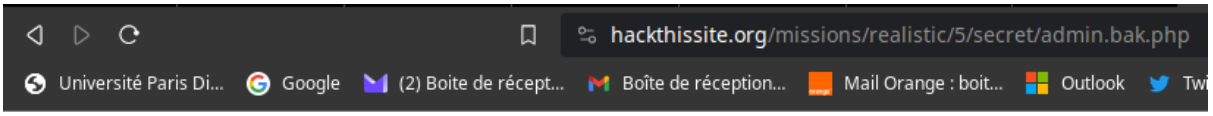
Le répertoire contient un unique fichier has, cliquer dessus le télécharge. On va ensuite dans le répertoire secret/ :



Index of /missions/realistic/5/secret

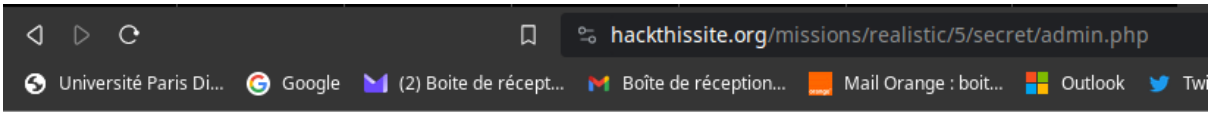
Name	Last modified	Size	Description
Parent Directory		-	
admin.bak.php	2013-12-30 05:28	230	
admin.php	2013-12-30 05:28	621	

Le contenu de admin.bak.php :



error matching hash 43500a7a9ff03e36d3114443538d2483

Le contenu de admin.php :



Invalid Password

On affiche le contenu du fichier téléchargé, on peut voir “MD4”, on en conclut donc que le hash utilisé est MD4 :

```
Error: MDupdate MD already done.
Error: MDupdate called with illegal count value %d.MD4 time trial. Processing
Characters processed per second: %ld.
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789$tI%%%%B "%s"
```

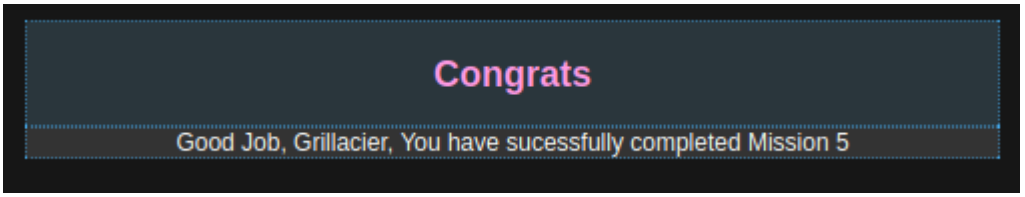
On crée un fichier contenant le hash du fichier admin.bak.php :

```
┌──(alaia㉿kali)-[~/Documents/cours/cyberav/tp]
└─$ echo 43500a7a9ff03e36d3114443538d2483 > hash.txt
```

On lance john the ripper sur ce fichier :

```
┌──(alaia㉿kali)-[~/Documents/cours/cyberav/tp]
└─$ sudo john --format=raw-MD4 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD4 [MD4 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
c12d8            (?)
1g 0:00:00:28 DONE 3/3 (2023-10-26 07:44) 0.03496g/s 39998Kp/s 39998Kc/s 3999
8KC/s ckd7i..c145v
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Mot de passe : **c12d8**
On rentre le mot de passe obtenu dans la page submit.html :



Level 6

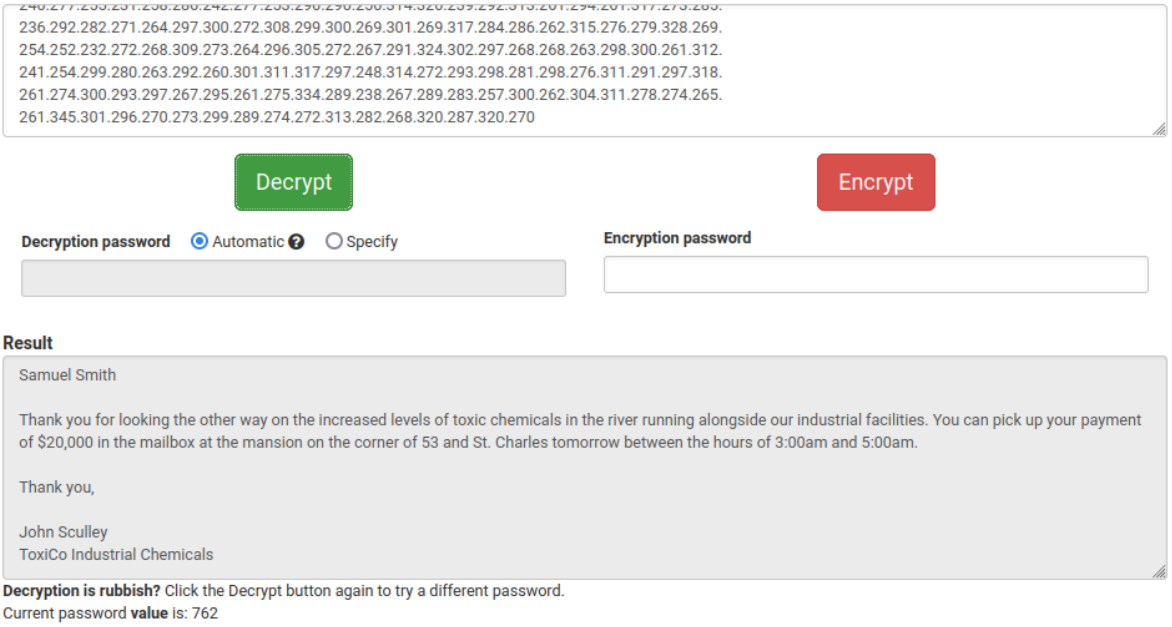
On teste le script avec un “a” :

En lançant plusieurs fois le chiffrement, les 3 nombres changent mais à chaque fois, leur somme est égale à 97, soit le code ASCII du “a”.
Si on ajoute “a” comme mot de passe, la somme donne maintenant 194. On soustrait 97 et on retrouve 97. Le code ASCII semble donc s’additionner aux nombres, il suffit ensuite de soustraire le code ASCII du mot de passe au résultat de l’addition pour trouver le code ASCII du message.
On ne comprend rien à la façon dont il faudrait décoder ça donc on cherche XECryption algorithm sur Google et on clique sur le premier lien où on colle le texte encodé :

XECryption

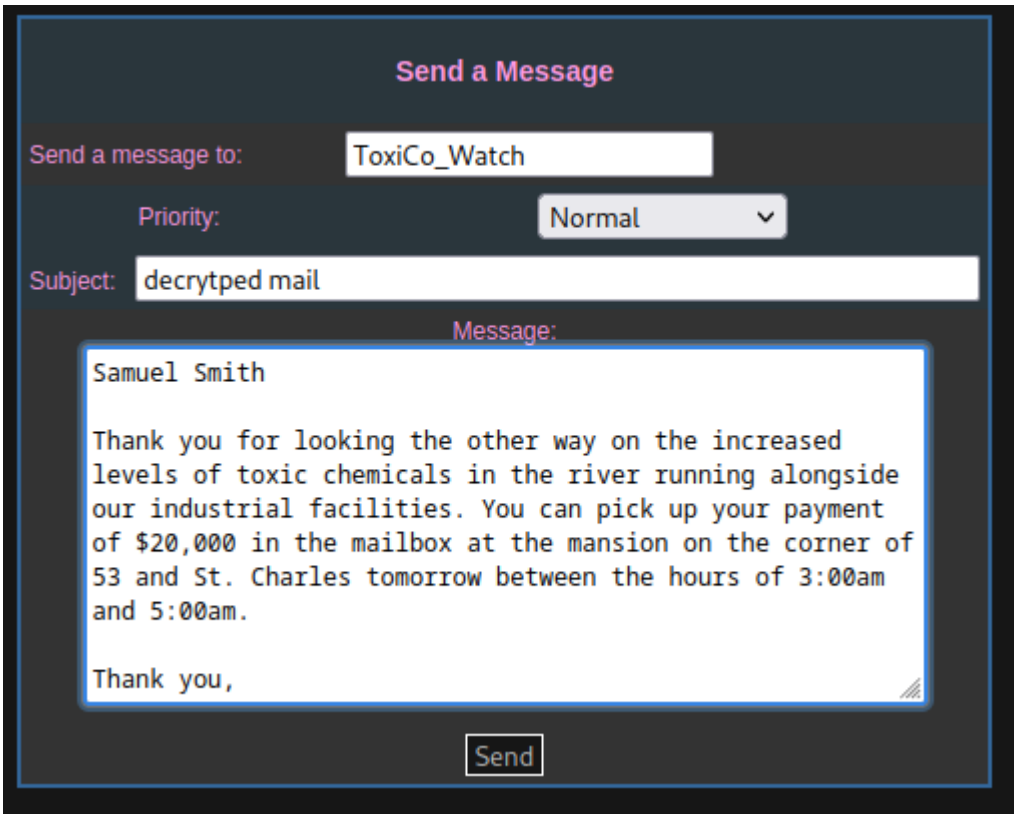
Web based decryption/encryption tool

XECryption is a simple encryption algorithm used in Realistic Mission 6 from HackThisSite.
This tool can be used to solve the challenge, but also to encrypt any plain text using XECryption and vice-versa.



On copie le mail déchiffré pour l'envoyer à l'utilisateur qui nous a contacté :

From: ToxiCo_Watch



Congratulations, you have successfully completed realistic 6!

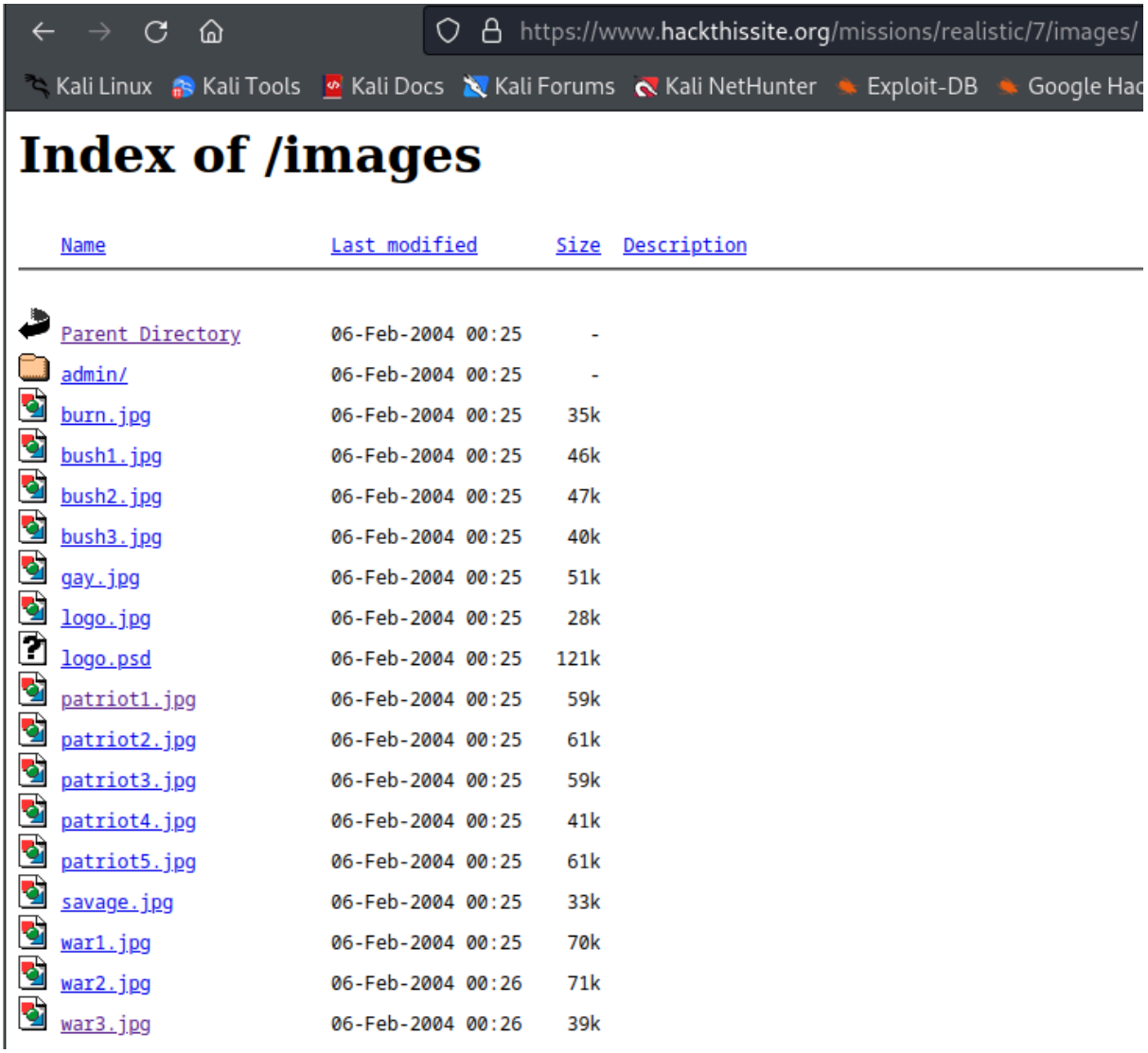
Level 7

On se promène sur le site et on regarde les codes source :

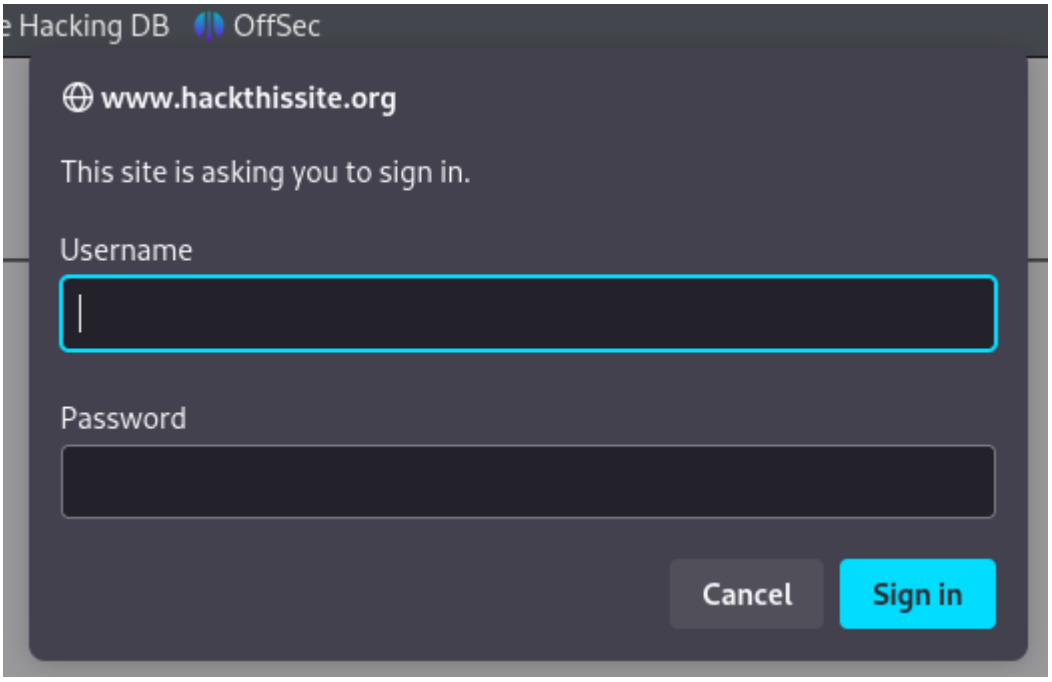
```
<center><a href="images/patriot1.jpg
"><img src="images/patriot1.jpg
```

view-source:https://www.hackthissite.org/missions/realistic/7/images/patriot1.jpg

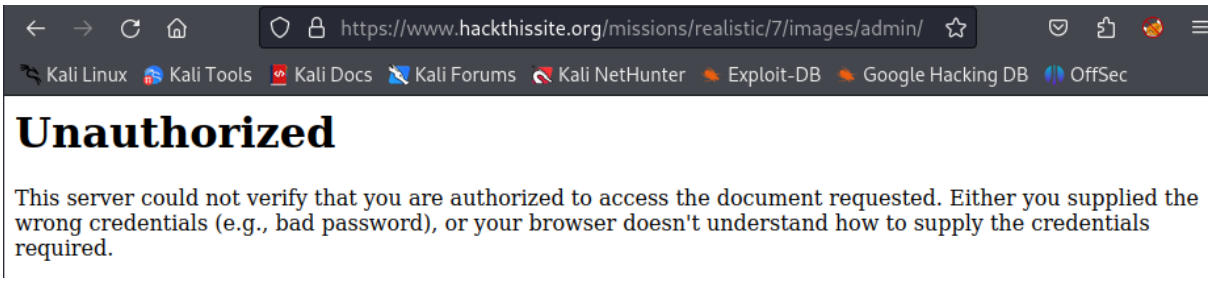
On a des chemins vers images/nom_image.jpg mais pas vers le répertoire images directement donc on y accède manuellement en supprimant le nom du fichier dans l'url :



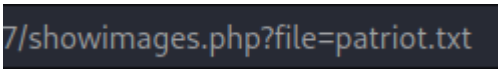
On sait maintenant que nous avons affaire à un serveur Apache2. On voit que le répertoire contient des images et un répertoire admin, on clique dessus :



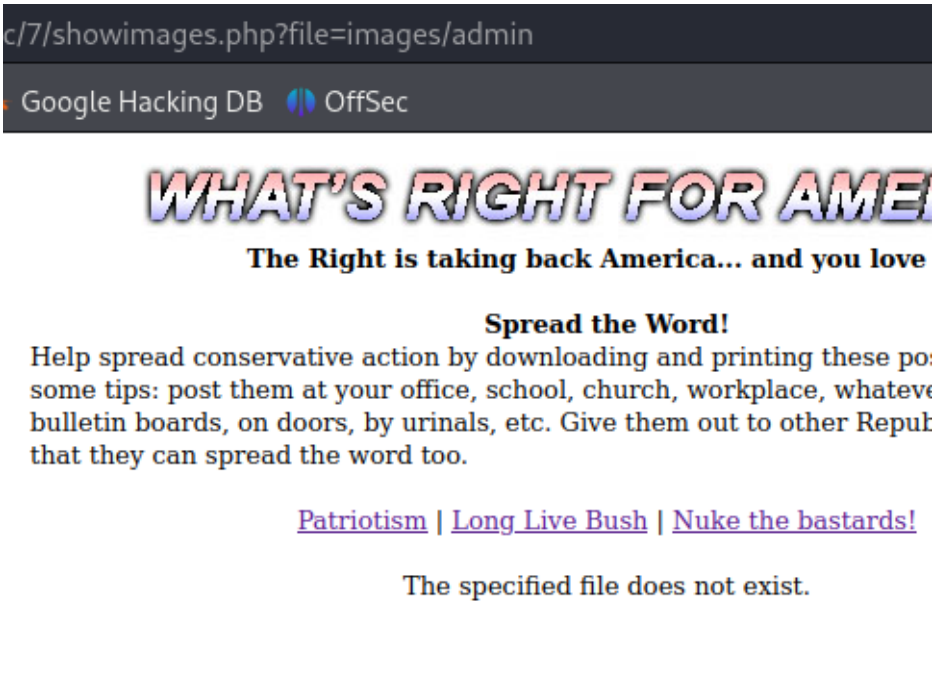
Quand on essaye de se connecter avec des identifiants erronés, la page se recharge.
Quand on clique sur Cancel, cette page apparaît :



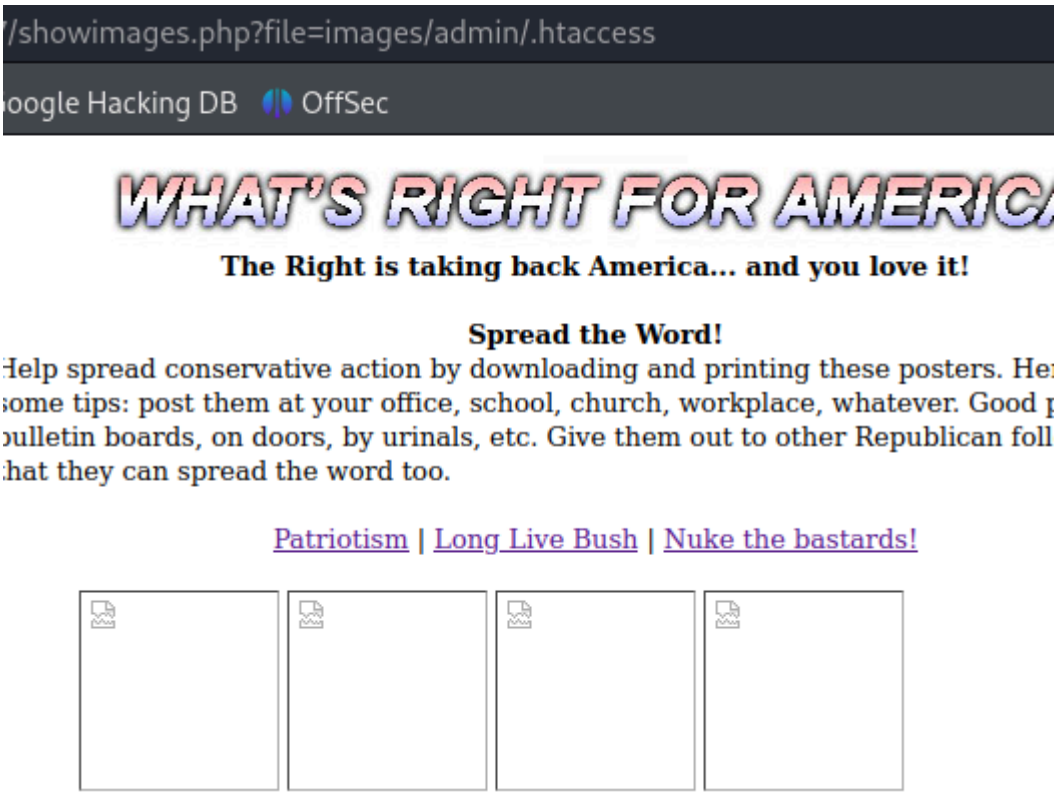
On retourne en arrière vers les pages contenant des photos :



On remplace le nom du fichier par le chemin vers le répertoire admin :



On obtient un message d'erreur. On essaye d'accéder au fichier .htaccess d'Apache :



On obtient 4 liens à la place des photos, on affiche le code source de la page :

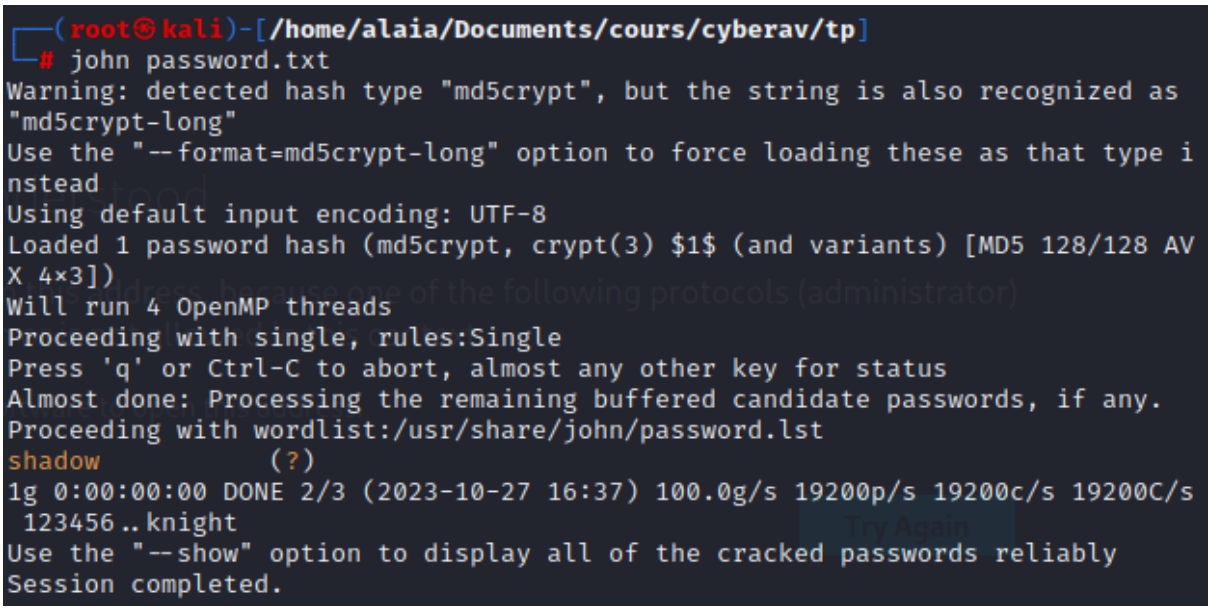
```
<center><a href="AuthName "Administration Access"
"><img src="AuthName "Administration Access"
" width=100></a> <a href="AuthType Basic
"><img src="AuthType Basic
" width=100></a> <a href="AuthUserFile /www/hackthissite.org/www/missions/realistic/7/images/admin/.htpasswd
"><img src="AuthUserFile /www/hackthissite.org/www/missions/realistic/7/images/admin/.htpasswd
" width=100></a> <a href="require valid-user
"><img src="require valid-user
" width=100></a> <a href=""><img src="" width=100></a> </center></font>
</td></tr></table>
```

On découvre l'existence d'un fichier .htpasswd, on y accède :

Cette fois, on obtient un seul lien. On fait un clic droit dessus et on l'ouvre dans un nouvel onglet :

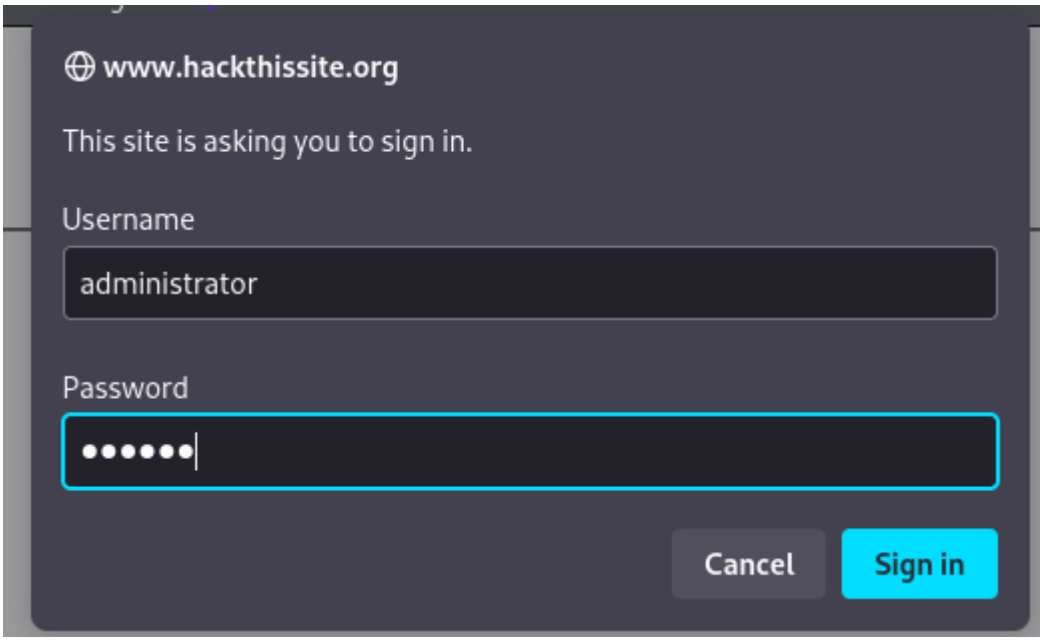
On possède maintenant le pseudo en clair, le mot de passe est chiffré et se trouve après les ":". On crée un fichier contenant ce code :

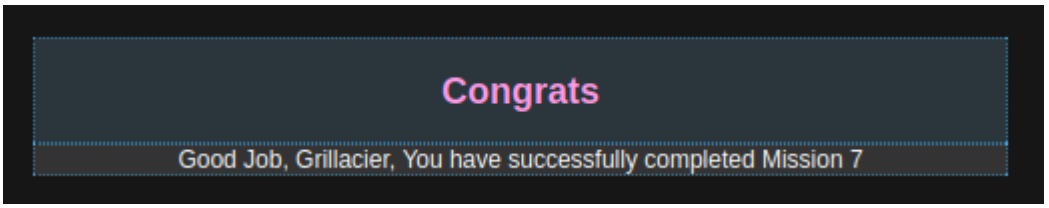
On lance john the ripper sur le fichier :



Mot de passe : **shadow**

On retourne sur la page d'identification et on se connecte :



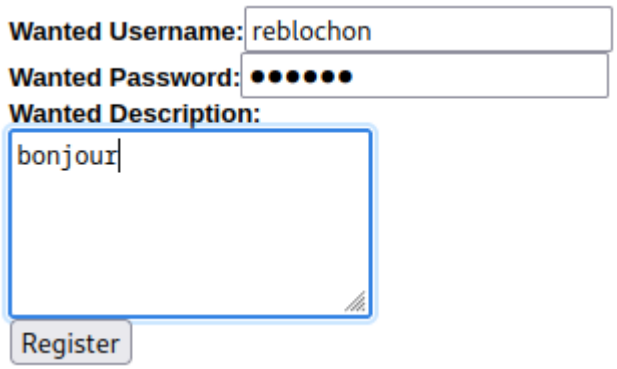


Level 8

On apprend sur la page d'accueil qu'il y a une base de données, on devra donc sûrement réaliser une injection SQL :

account, create an account, and more. We at the Tech Support hope to make this site easy and safe for you to use, this is our new site, and we are ready to build our database, so if your not registered, REGISTER! It's Free.

On crée un compte :

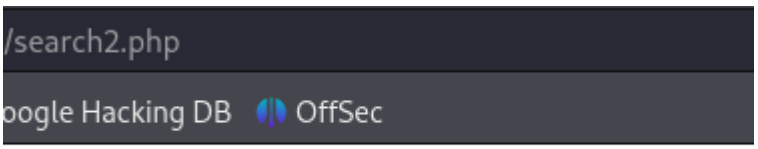


On peut chercher un utilisateur à partir de la page User Info :

Number Of Users Found: 1

dropCash : 123abc

Quand on cherche un utilisateur qui n'existe pas, on obtient ce message :



No Users Found

Mais quand on cherche un utilisateur du nom de ', on obtient ce message :

Error Getting Username Information From Table 'users'

On a trouvé notre vulnérabilité. On cherche l'utilisateur ' or 1=1 :

Username: ' or 1=1; Search

Ce qui nous donne le contenu de la table users :

Number Of Users Found: 19225

Lolita Goncalez : dancing queen

Tom Brown : Tom the brown

Lisa M. : I am sweet

Peter McDonald : fatman

Drake Alucard : BLOOD

Mike Power : need money

Wanda : wonder girl

Matt Johnson : 31337

Heinz Harald Kunze : da german guy :)

Karen Oldfield :

Chercher “gary” avec ctrl-f nous donne 581 résultats. Si on se rend au pied de la page, on peut voir le compte que l’on a créé plus tôt en dernier :

imene_gouc : TP HackThisSite

els : sisi bisi

reblochon : bonjour

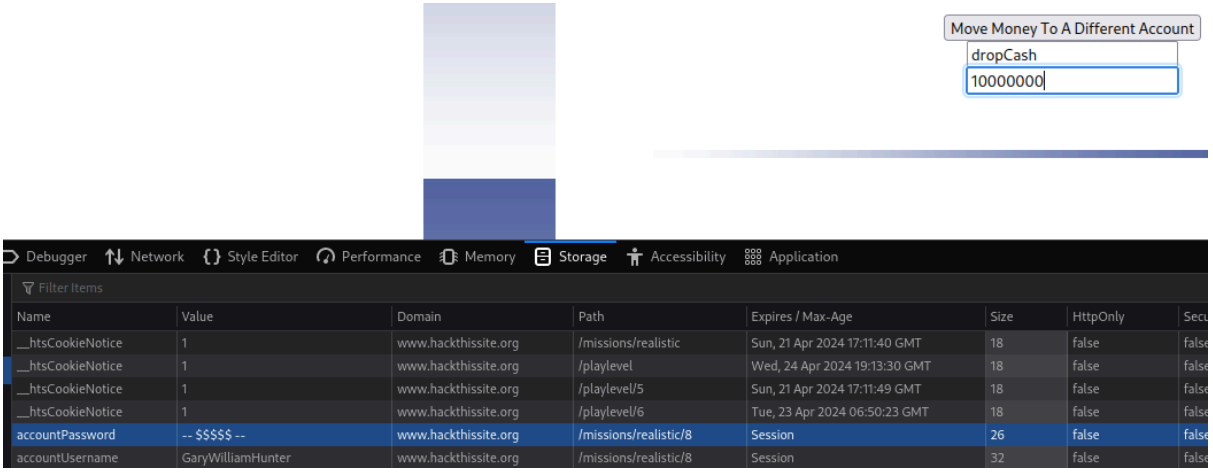
On peut conclure que le premier Gary Hunter sera le compte que nous cherchons et que les 580 suivants ont été créés par d’autres joueurs.
Le premier Gary Hunter :

GaryWilliamHunter : -- $$$$$ --

On se connecte avec son compte et on regarde les cookies :

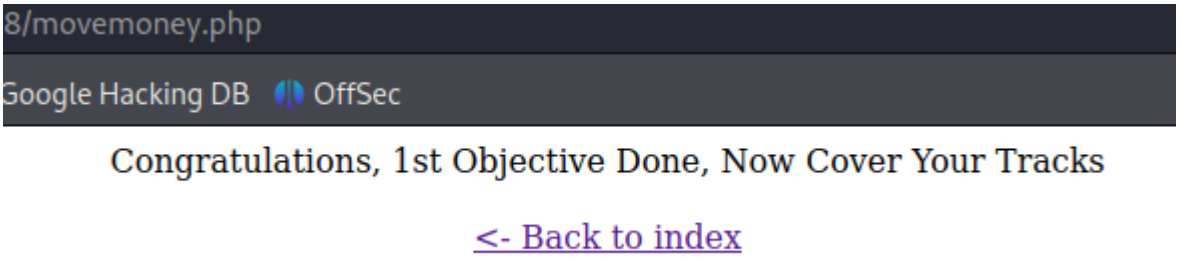
accountPassword	azerty	www.hackthissite.org	/missions/realistic/8	Session
accountUsername	reblochon	www.hackthissite.org	/missions/realistic/8	Session
HackThisSite	q3brrrc8t21jlhfoul039hsf46	www.hackthissite.org	/	Fri, 27 Oct 2023 23:10:37 GMT

Deux cookies de session ont été créés, un pour le pseudo et un pour le mot de passe. On rentre le pseudo de dropCash et la somme qu'on veut lui verser. Puis, on modifie les valeurs des cookies de session pour accéder au compte de GaryWilliamHunter :

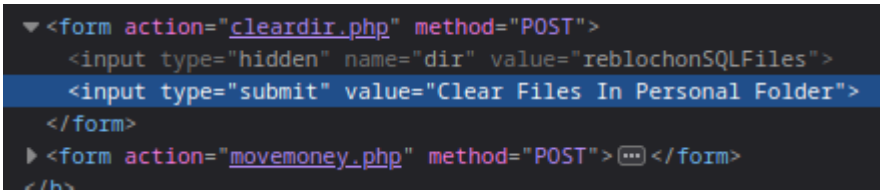


Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secu
__htsCookieNotice	1	www.hackthissite.org	/missions/realistic	Sun, 21 Apr 2024 17:11:40 GMT	18	false	false
__htsCookieNotice	1	www.hackthissite.org	/playlevel	Wed, 24 Apr 2024 19:13:30 GMT	18	false	false
__htsCookieNotice	1	www.hackthissite.org	/playlevel/5	Sun, 21 Apr 2024 17:11:49 GMT	18	false	false
__htsCookieNotice	1	www.hackthissite.org	/playlevel/6	Tue, 23 Apr 2024 06:50:23 GMT	18	false	false
accountPassword	-- $$$$$ --	www.hackthissite.org	/missions/realistic/8	Session	26	false	false
accountUsername	GaryWilliamHunter	www.hackthissite.org	/missions/realistic/8	Session	32	false	false

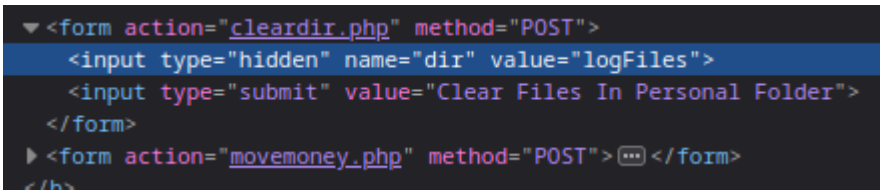
On clique sur le bouton "Move Money To A Different Account" :



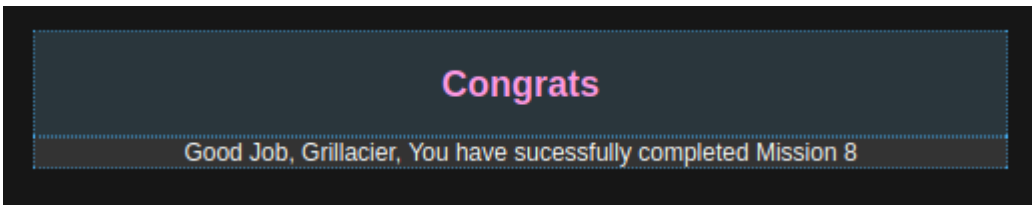
On se reconnecte et on inspecte le bouton "Clear Files In Personal Folder" :



On peut voir la valeur cachée de ce qui sera effacé. On remplace reblochonSQLFiles par logFiles :



Et enfin, on clique :

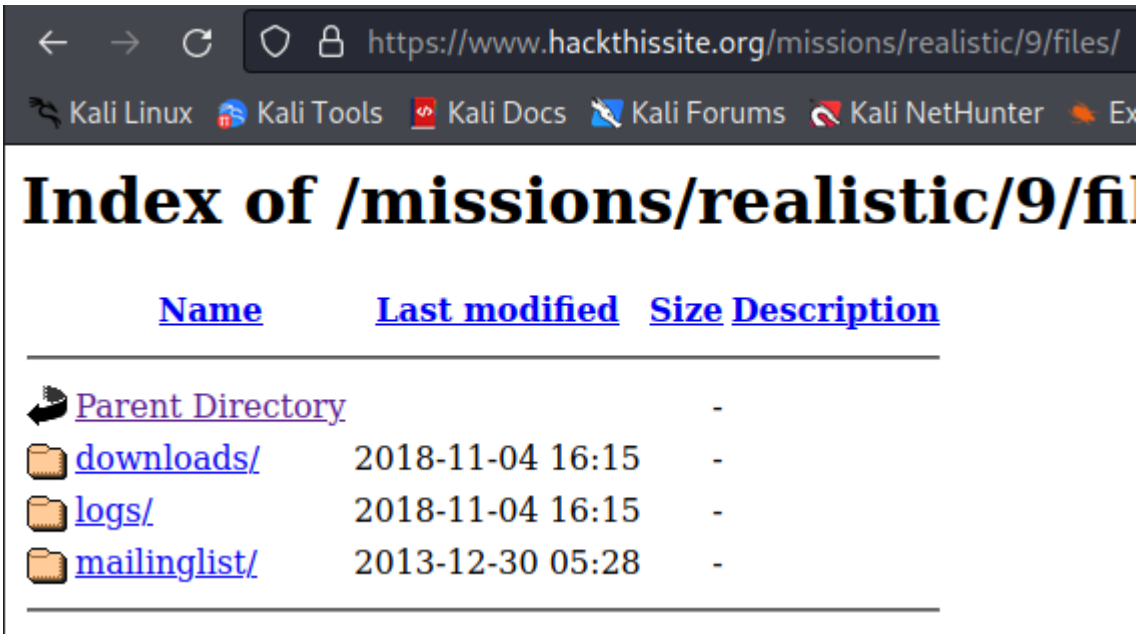


Level 9

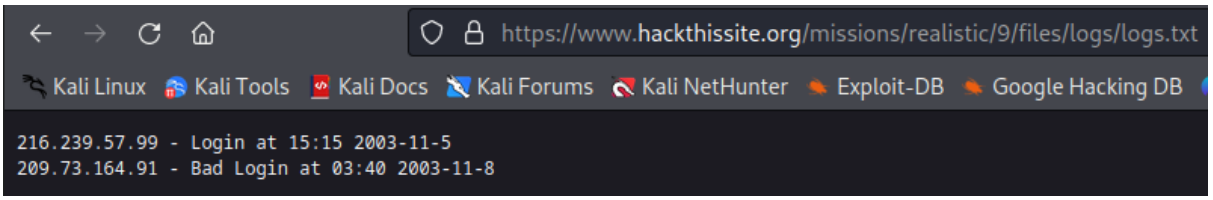
On se balade sur la site et sur la page demo, on regarde le code source :

```
You can test the software for 30 days, no installation needed!.<bR>
<br />
Download <a href="./files/downloads/CrappyDemo.exe.zip"><font color="
```

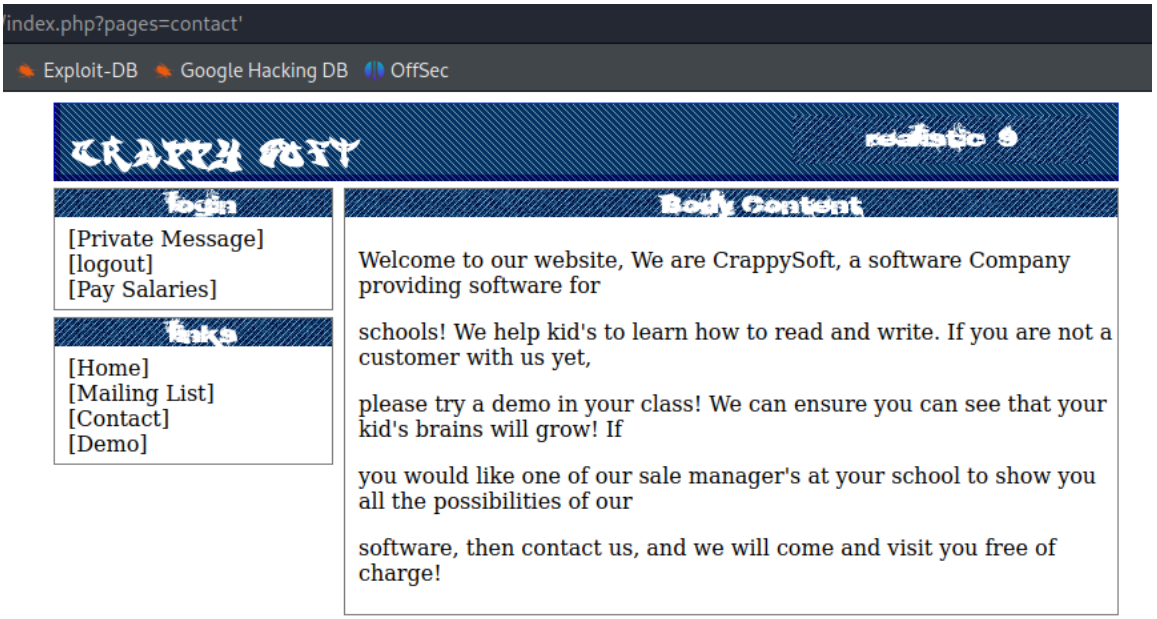
On découvre l'existence d'un répertoire files, on s'y rend :



Le répertoire mailinglist contient des adresses mail et logs contient un fichier logs.txt :



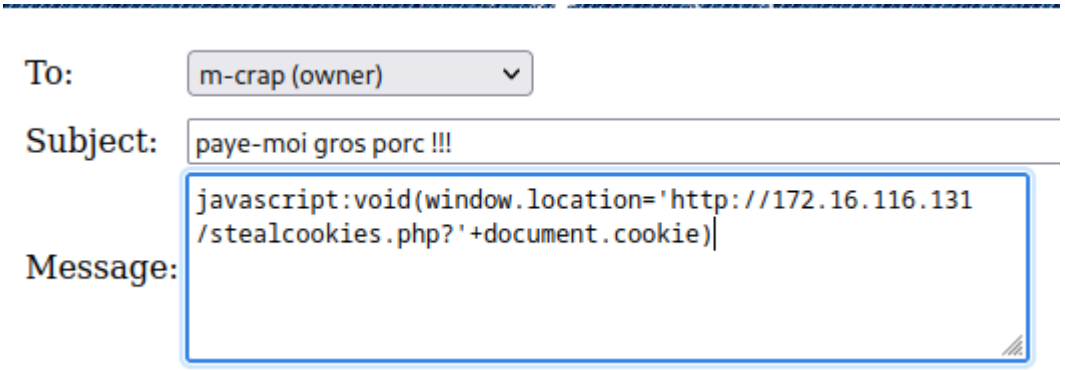
On se connecte avec le mail et le mot de passe qu'on a reçus :



On peut voir que des cookies ont été créés pour ce niveau :

intID	2	www.hackthissite.org	/missions/realistic/9	Session
movedTheMoneyIntodropCashAccountFinished	12XQeauy8OsZo	www.hackthissite.org	/missions/realistic/8	Session
strPassword	5b3de25c4dba60d2102281633d339b48	www.hackthissite.org	/missions/realistic/9	Session
strUsername	r-conner%40crappysoft.com	www.hackthissite.org	/missions/realistic/9	Session

On veut les remplacer pour usurper l'identité du patron et pouvoir envoyer de l'argent, pour cela on exploite une faille XSS dans l'onglet "Private Message" :

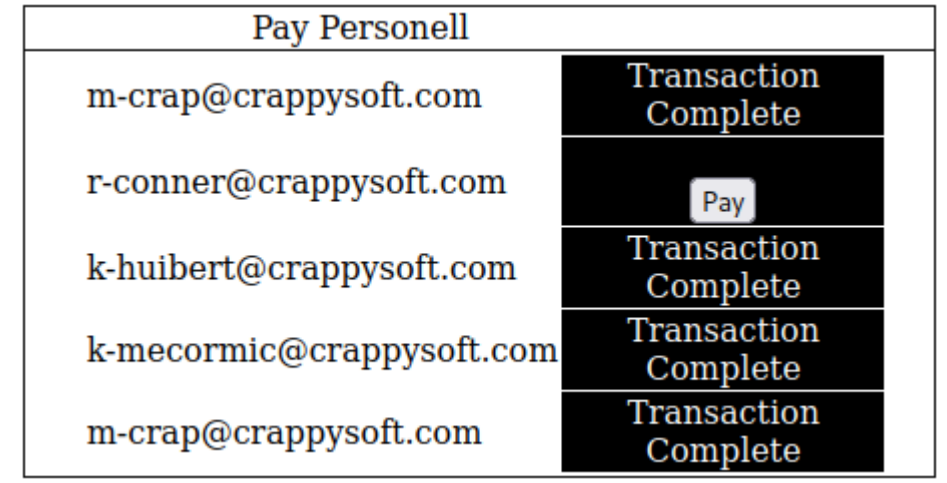


On obtient ce qu'on veut :

On modifie les cookies :

HackThisSite	qecsfbm33efnl5mhis68mq5gh2
intID	1
strPassword	94a35a3b7befff5eb2a8415af04aa16c
strUsername	m-crap%40crappysoft.com

On clique sur "Pay Salaries" :



On paye le 2e utilisateur :

YHEE THANKS MAN!! Thank's for my salary you really own!!
dont forget to clean the logs by subscribing to them!!

Pay Personell	
m-crap@crappysoft.com	Transaction Complete
r-conner@crappysoft.com	Transaction complete

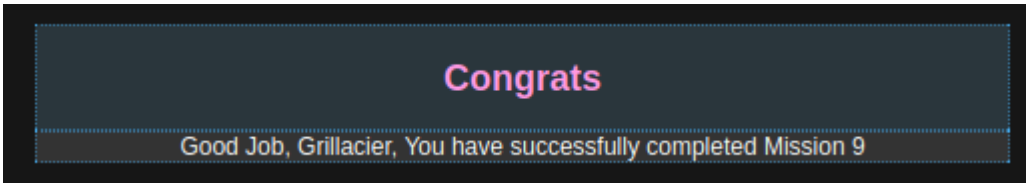
On doit maintenant effacer les logs. Ils se trouvent dans le fichier qu'on a découvert plus tôt.
Dans l'onglet "Mailing List", on inspecte la page :

```
<form action="subscribemailing.php" method="post">
  <input type="hidden" name="strFilename" value="./files/mailinglist/addresses.txt">
  <input type="text" name="strEmailAddress" value="you@somedomain.com">
  <br>
  <input type="submit" value="Subscribe!">
```

On modifie la valeur cachée pour y mettre le chemin des logs :

```
<form action="subscribemailing.php" method="post">
  <input type="hidden" name="strFilename" value="./files/logs/logs.txt">
  <input type="text" name="strEmailAddress" value="you@somedomain.com">
```

On valide :



Level 10

Dans le code source de la page d'accueil, on peut voir un lien vers une page du nom de staff.php :

```
<a href="staff.php">
    <img src="nothing.gif" width=150 height=20 border=0>
```

Il s'agit d'une page où les professeurs peuvent se connecter.
Dans la page "Student Access System", on se connecte avec les identifiants de l'élève qui nous a contacté. On peut voir que ses pseudo et mot de passe apparaissent dans l'URL :

/student.php?uusername=Zach+Sanchez&ppassword=liberty638

oogle Hacking DB OffSec

Holy Word High School

Home Page | Staff Listing | Student Access System

Zach Sanchez
721 Maple Avenue

Grades: (please select a course below)

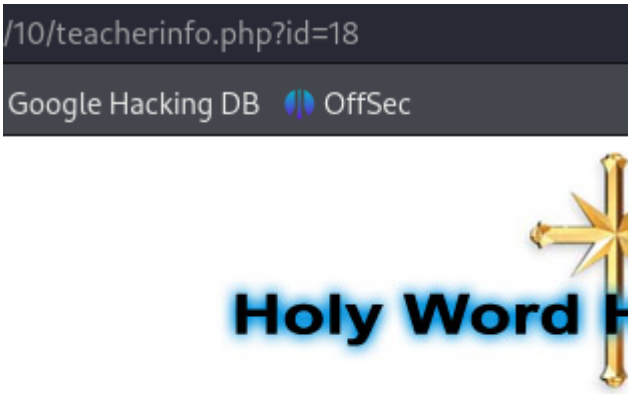
Mathematics
English Composition
Bible study
Gym
Computer

On va devoir changer ses notes en Bible Study, entre autres :

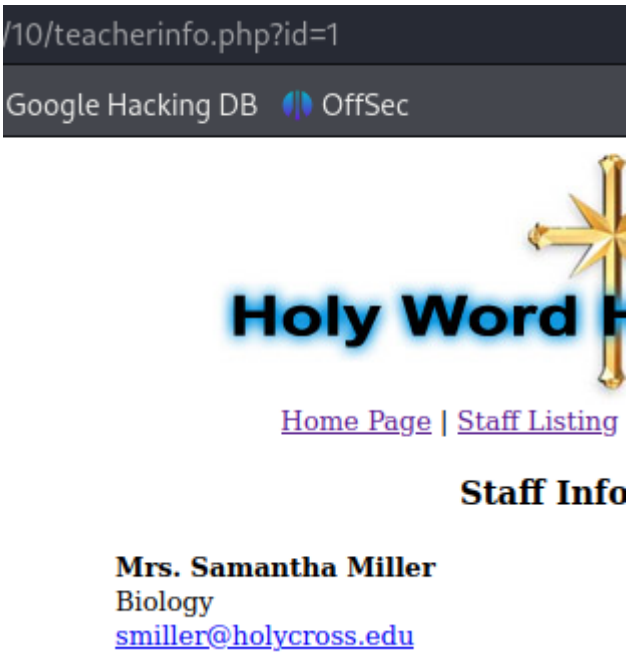
Semester	Course	Grade	Comments
1	Bible study	2	Disruptful in class.
2	Bible study	1	Does not follow teacher directions.

(5 = Excellent, 4 = Good, 3 = Average, 2 = Poor, 1 = Failure)

La page “Staff Listing” nous montre une liste des professeurs de l’école, chacun représenté par un id. Par exemple, le professeur de bible study a le numéro 18 :



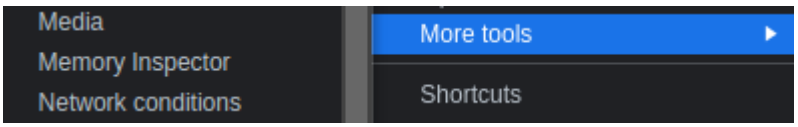
On essaye de se connecter avec des identifiants évidents comme jgoodman/password et jgoodman/jgoodman mais cela ne fonctionne pas. On se rend sur la page du professeur avec l'id 1 car c'est sûrement celui qui a des droits administrateurs :

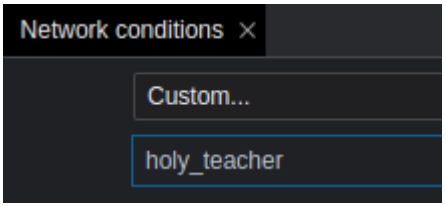


On essaye de se connecter et cette fois la combinaison smiller/smiller fonctionne :

Welcome, Mrs. Samantha Miller! Please remember that access to the staff administration area is restricted to the district-supplied 'holy_teacher' web browser.

Il faut maintenant modifier l'user agent :





Cela fait apparaître un control panel :

Mrs. Samantha Miller

control panel

Check Messages
Submit Grades
Change Grades

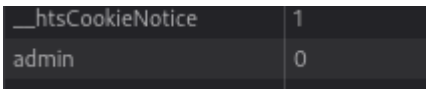
(note: you are not an administrator so you cannot change grades)

Welcome to your staff control panel. From here, you can check for messages, submit grades, and change grades.

Your info, as listed on the main website:

Hello Holy Word students! I teach Biology for the freshman class. My philosophy is, if you pay attention in class, show up every day and obey all teacher instructions, you will receive good marks. You decide what grade you get.

Le cookie admin étant égal à 0, on change sa valeur pour qu'il soit égal à 1 :



La note a maintenant disparu :

Mrs. Samantha Miller

control panel

Check Messages
Submit Grades
Change Grades

Welcome to your staff control panel. From here, you can check for messages, submit grades, and change grades.

Your info, as listed on the main website:

Hello Holy Word students! I teach Biology for the freshman class. My philosophy is, if you pay attention in class, show up every day and obey all teacher instructions, you will receive good marks. You decide what grade you get.

On clique sur “Change Grades” :

Mrs. Samantha Miller

control panel

Check Messages
Submit Grades
Change Grades

Student listing:

Zach Sanchez
Jerry Smith
Rachel Addison
Nancy Williams
Stacy Williams
Cory Lent
Henry Jordan
Andrew Peterson
Courtney Turner
Amanda Goodman
Janine Johnson
Tony Farina

Puis sur l'étudiant dont on veut modifier les notes :

tic/10/staff.php?action=changegrades&changeaction=viewstudent&studentid=1

Google Hacking DB OffSec

Mrs. Samantha Miller

control panel

Check Messages
Submit Grades
Change Grades

Zach Sanchez
721 Maple Avenue

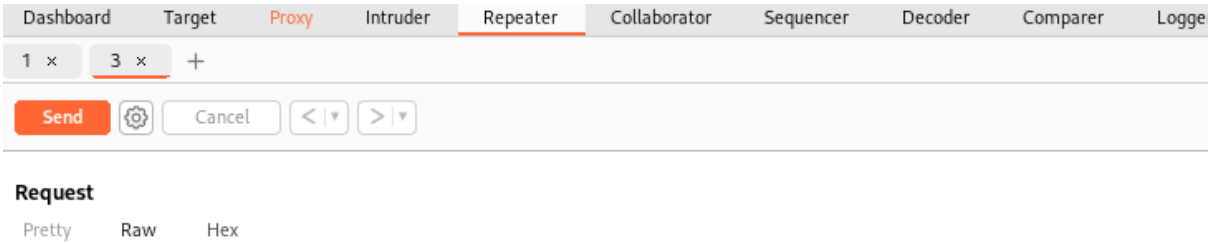
Course	Grade	Comments	Semester	Modify
Bible study	2	Disruptful in class.	1	see below
Bible study	1	Does not follow teacher direct	2	see below
Computer	3	Inattentive	1	see below
Computer	4	Good efforts about learning.	1	see below
English Composition	3	Inattentive	1	see below
English Composition	4	Good writer... would like to se	2	see below
Gym	3	Poor class attitude.	1	see below
Gym	1	Had objections to me forcing s	2	see below
Mathematics	5	Does well	2	see below
Mathematics	5	Excels in algebra and logic.	2	see below

Sorry, it is too late into the school year to change grades now. The grades will be printed and mailed in just a few days.

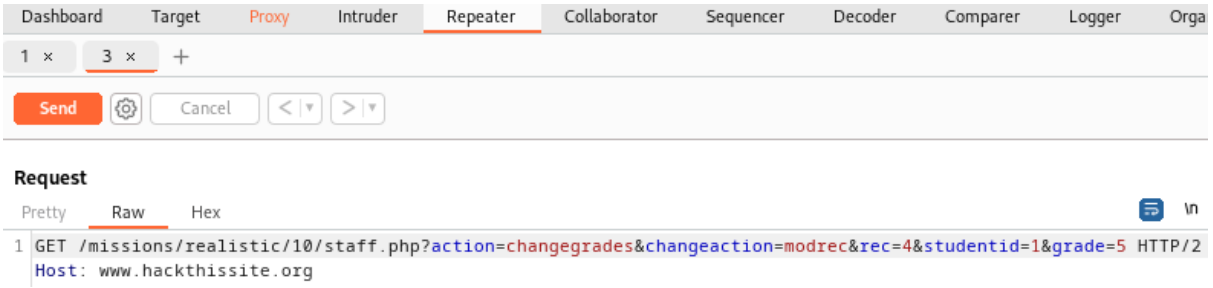
Les notes ne peuvent pas être modifiées directement sur le site. On observe le code source et on voit une méthode post :

```
<tr><td>
<form action="staff.php?action=changegrades&changeaction=modrec&rec=4&studentid=1" method="post"></form>
Bible study</td><td width=5> </td>
```

On intercepte la page avec burpsuite puis on l'envoie au répeteur :



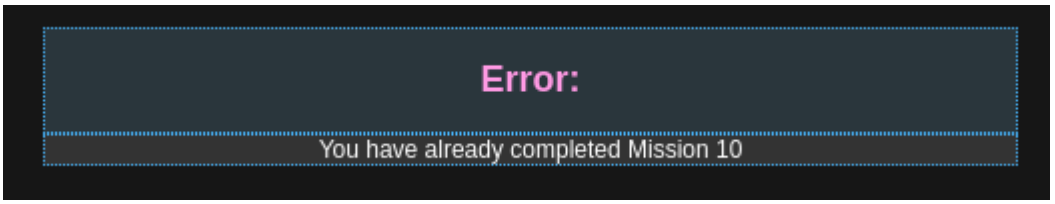
On remplace l'action par celle qu'on a trouvé dans le code source et on y ajoute "grade=5" :



On clique sur "Send" et on obtient ce message si l'action est correctement effectuée :

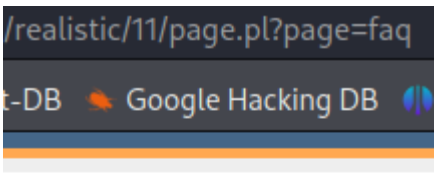
```
1 HTTP/2 200 OK
```

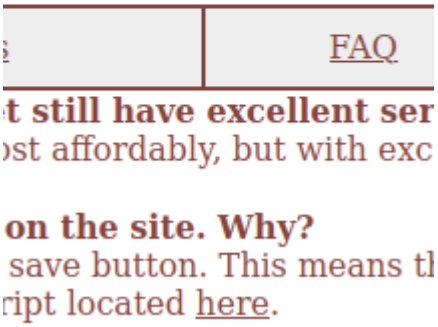
On recommence en changeant la valeur de rec jusqu'à ce que le niveau se valide :



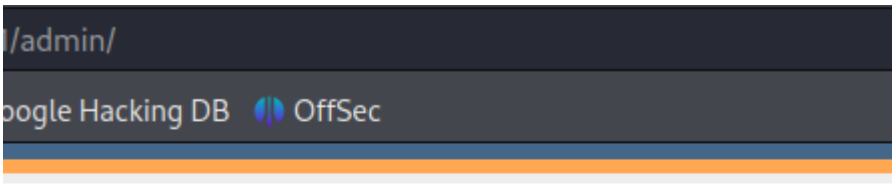
Level 11

On peut cliquer sur un lien à partir de la page FAQ :



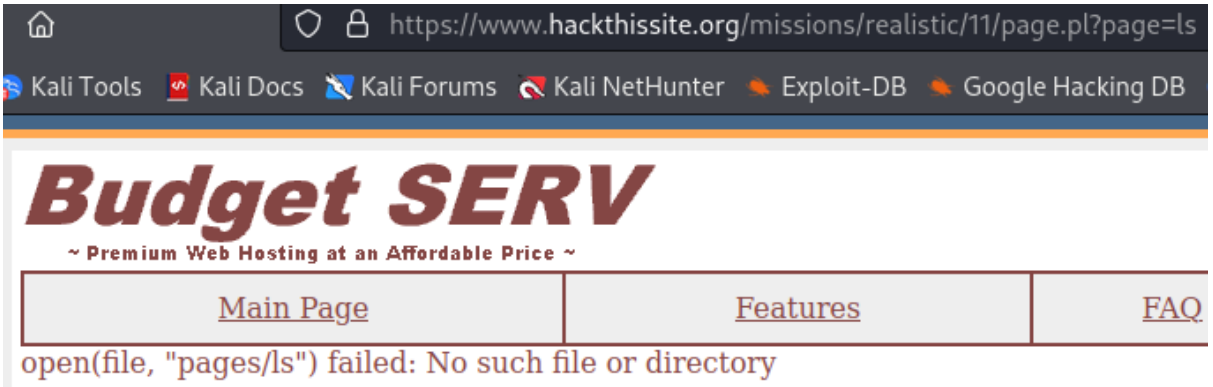


On arrive sur la page admin mais on ne connaît pas encore les identifiants :

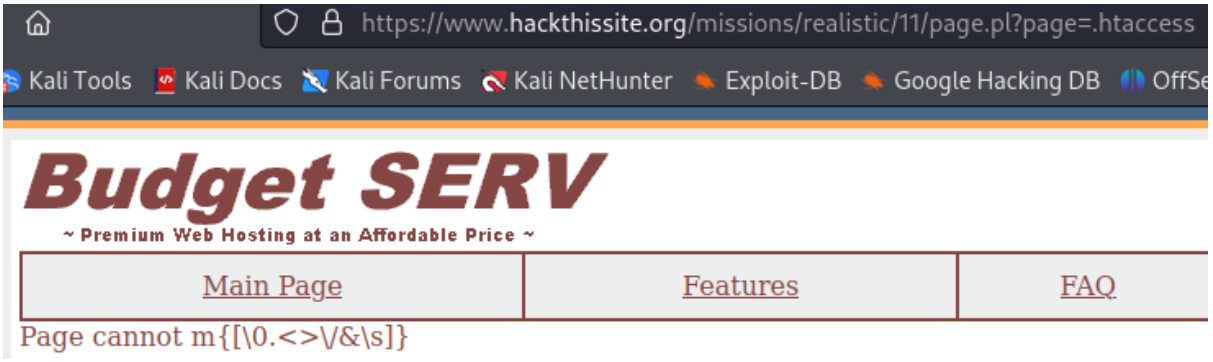


On voit que les différentes pages du site sont affichées à partir de page.pl qui est un script perl :

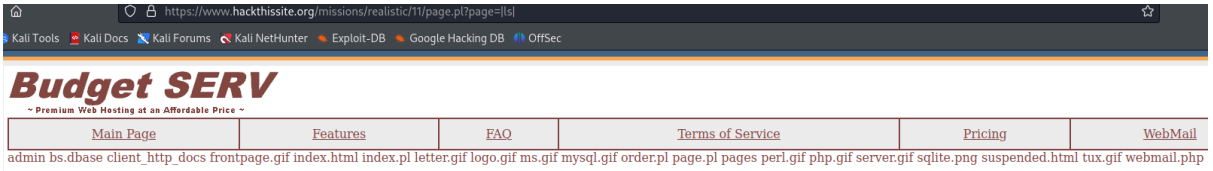
Si on remplace le “main” de l’url par le nom d’une page qui n’existe pas, on obtient ce message d’erreur :



Et si on essaye d'accéder à une page dont le nom commence par un point, on obtient ce message d'erreur :



Pour utiliser un script perl, on doit ajouter "||" autour du nom d'une commande. On obtient le résultat de la commande ls :

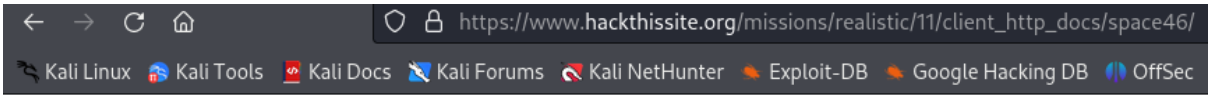


On accède à la page client_http_docs :

Index of /var/www/budgetserv/client_http_do

- Parent Directory
- space46/
- wonderdiet/
- potatoworks/
- therightwayradio/

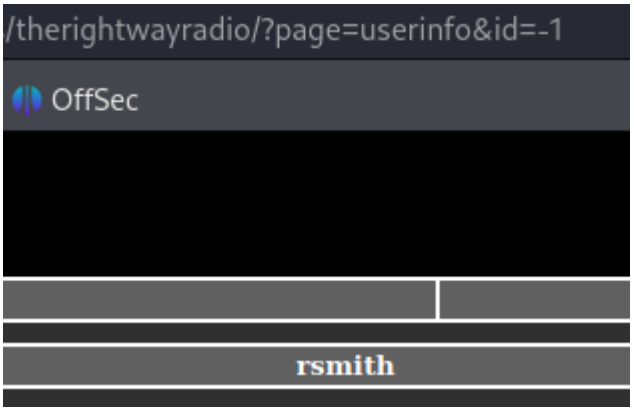
La page space46 :



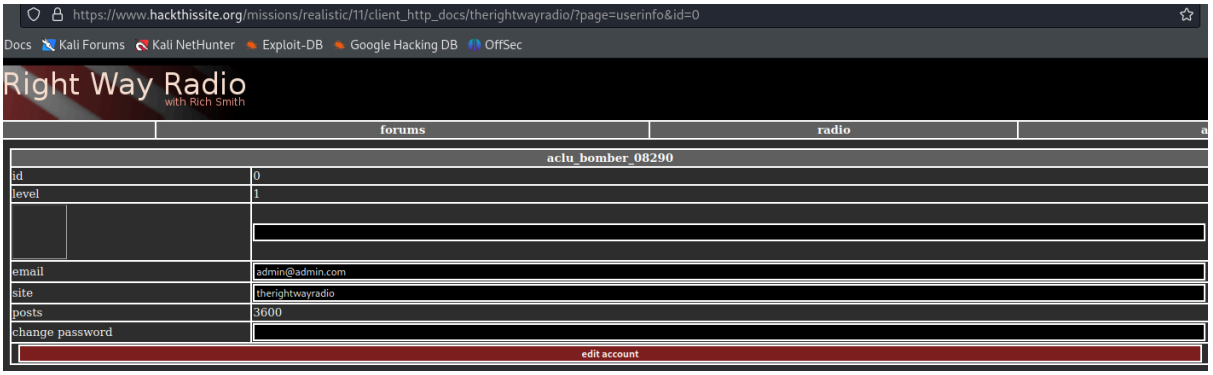
This account has been suspended.

La page therightwayradio :

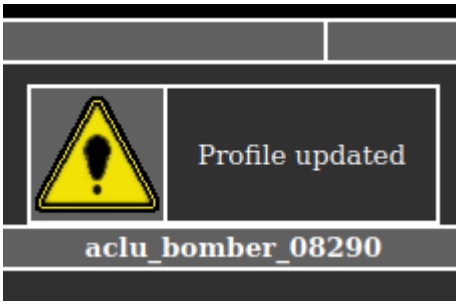
On clique sur le nom d'utilisateur qu'on voit sur la page d'accueil :



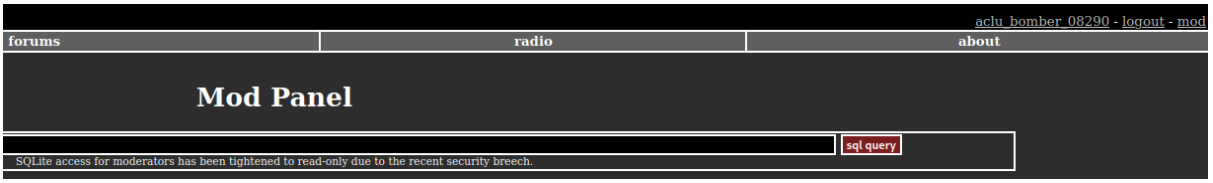
On voit que son id est le -1, on essaye d'accéder à l'id 0 :



On voit qu'il s'agit d'un admin et qu'on peut modifier son compte. On change son mot de passe en 123456789 et on se connecte à son compte :



À droite, on clique sur la page "mod". On peut écrire des requêtes SQL :



D'après le site de l'hébergeur, ils utilisent MySQL et SQLite :

Linux Operating Systems
As a customer of BudgetSERV, you can choose for your site to be on RedHat, Suse, or FreeBSD servers.

Windows Operating System
Customers of BudgetSERV may also choose to run on one of our two Windows 2003 Servers.

FrontPage Support
BudgetSERV technical support can help you learn the ins and outs of FrontPage for use in web development.

PHP
Our servers support PHP scripting, to help make your site more dynamic and interactive.

MySQL
MySQL is a database engine that can be used along with PHP or Perl to easily create and maintain databases.

SQLite
SQLite is a database engine that can be used along with PHP or Perl to easily create and maintain databases as individual files.

Perl
Our servers support Perl scripting, to help make your site more dynamic and interactive.

Dans la liste des fichiers précédemment découverte, on a découvert l'existence d'un fichier bs.dbase. On inspecte la page et on modifie le chemin de la base de données :

```
<input type="hidden" name="page" value="mod">
<input type="hidden" name="sql_db" value="rwr.dbase">
<input type="text" name="sql_query" style="width: 80%">
```

```
<form method="post" action="./?page=mod" enctype="multipart/form-data">
<input type="hidden" name="page" value="mod">
<input type="hidden" name="sql_db" value="../../../bs.dbase">
```

On commence par réaliser une requête sur une de ces tables :

2. Alternative Names

The schema table can always be referenced using the name "sqlite_schema", names are also recognized, including:

1. sqlite_master
2. sqlite_temp_schema
3. sqlite_temp_master

On obtient deux tables :

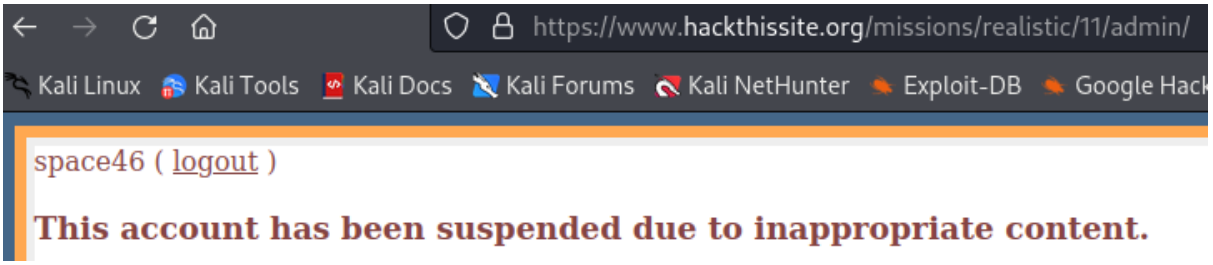
name
web_hosting

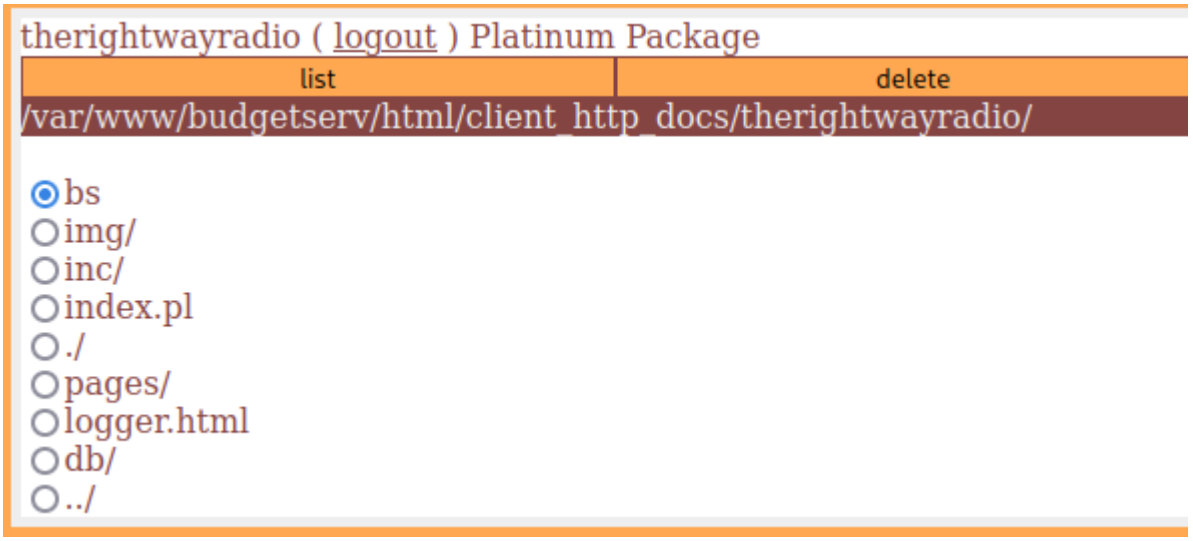
```
SELECT name FROM sqlite_master WHERE type ='table';
```

On affiche le contenu de la table web_hosting :

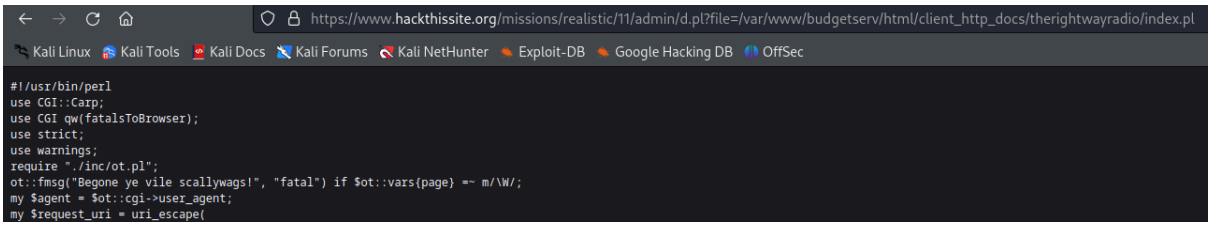
web_user	web_package	web_email	web_pass
space46	-1	space46@space46.nod	notofthisworld
therightwayradio	4	rsmith@therightwayradio.nod	letgodsortitout
wonderdiet	1	admin@wonderdiet.nod	suckereveryminute

On retourne sur la page admin du site hébergeur pour tester les identifiants :

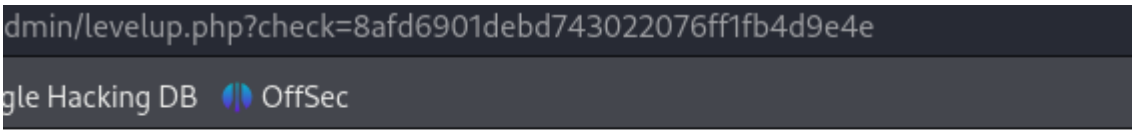




En cliquant sur “download”, on est envoyé sur une page :



On modifie l’url afin de télécharger le backup du site space46 :

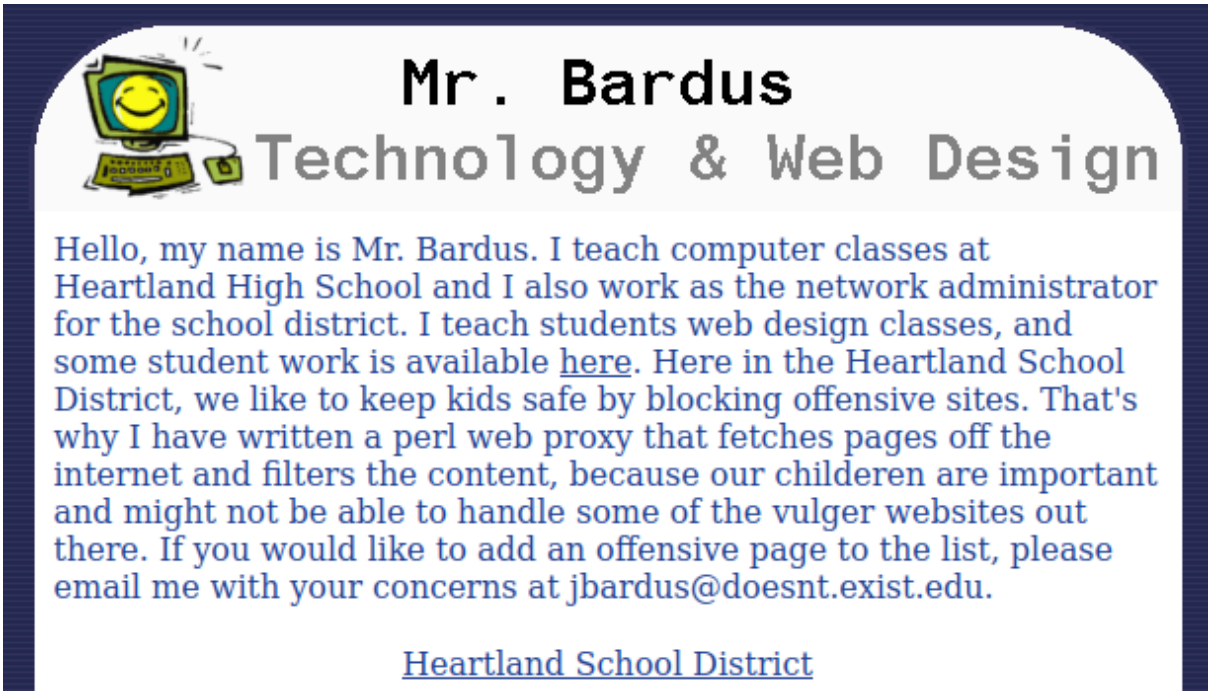


Congratulations

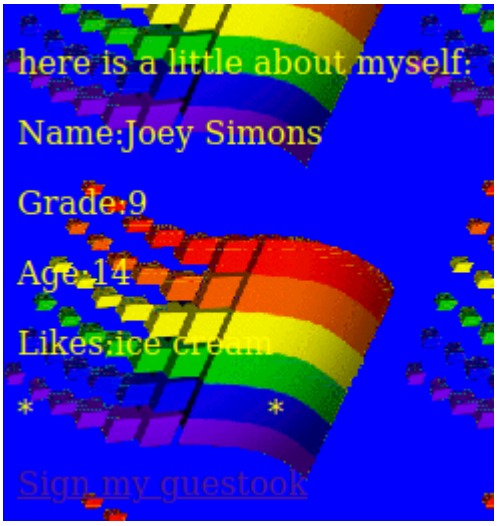
Good Job, Grillacier, You have sucessfully completed Mission 11

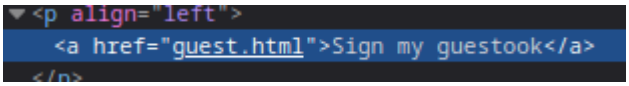
Level 12

On se balade sur le site de l’école et on accède à la page contenant les travaux d’élèves :

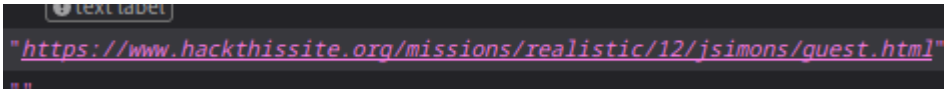


Le site d'un des élèves possède un lien vers un guestbook :

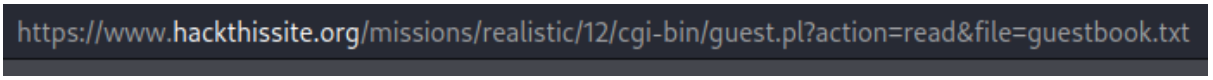




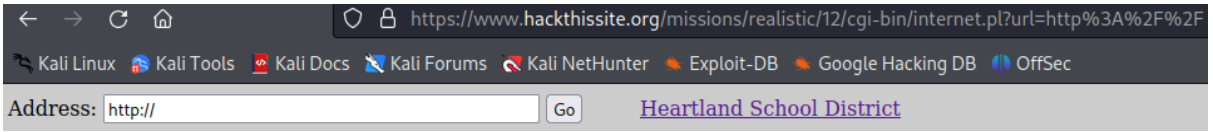
On inspecte la page et on trouve ce lien :



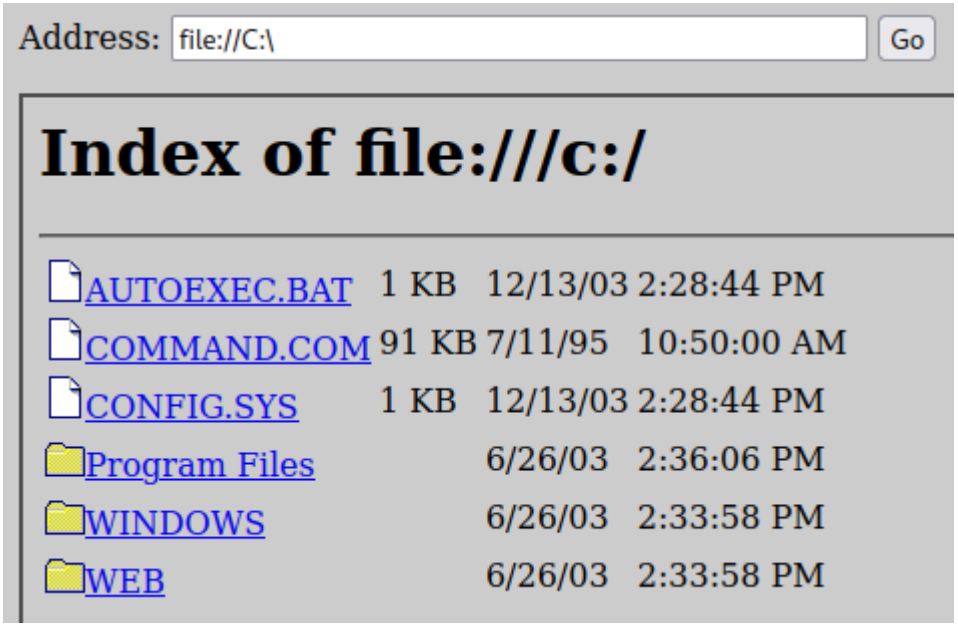
Quand on écrit un message et qu'on clique sur le bouton, on obtient cette URL :



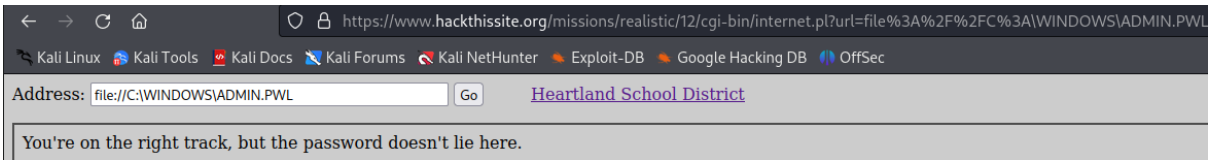
On garde cette page de côté et on retourne sur le site de l'école pour utiliser la barre d'adresse en haut de page :



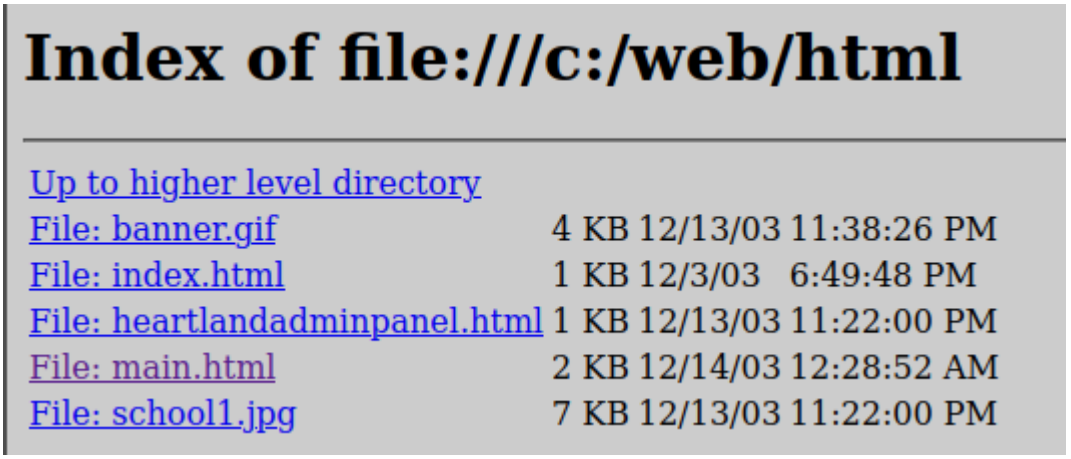
On sait que le site utilise un serveur Windows 95, on se rend sur le disque C :



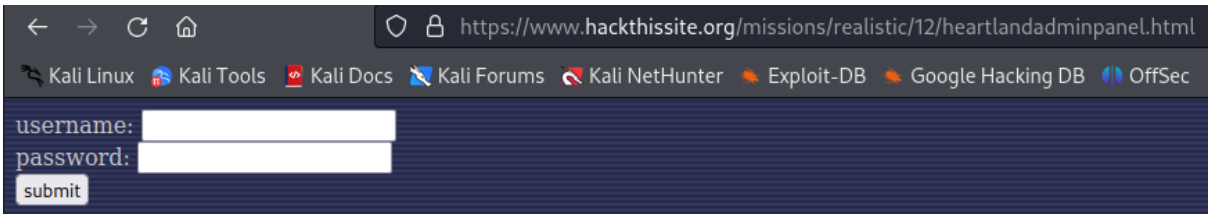
On ajoute les noms des dossiers et fichiers pour se déplacer dans l'arborescence :



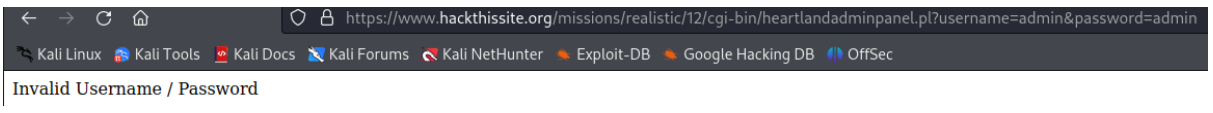
On découvre l'existence d'un fichier heartlandaminpanel.html :



On s'y rend et on nous demande de se connecter :

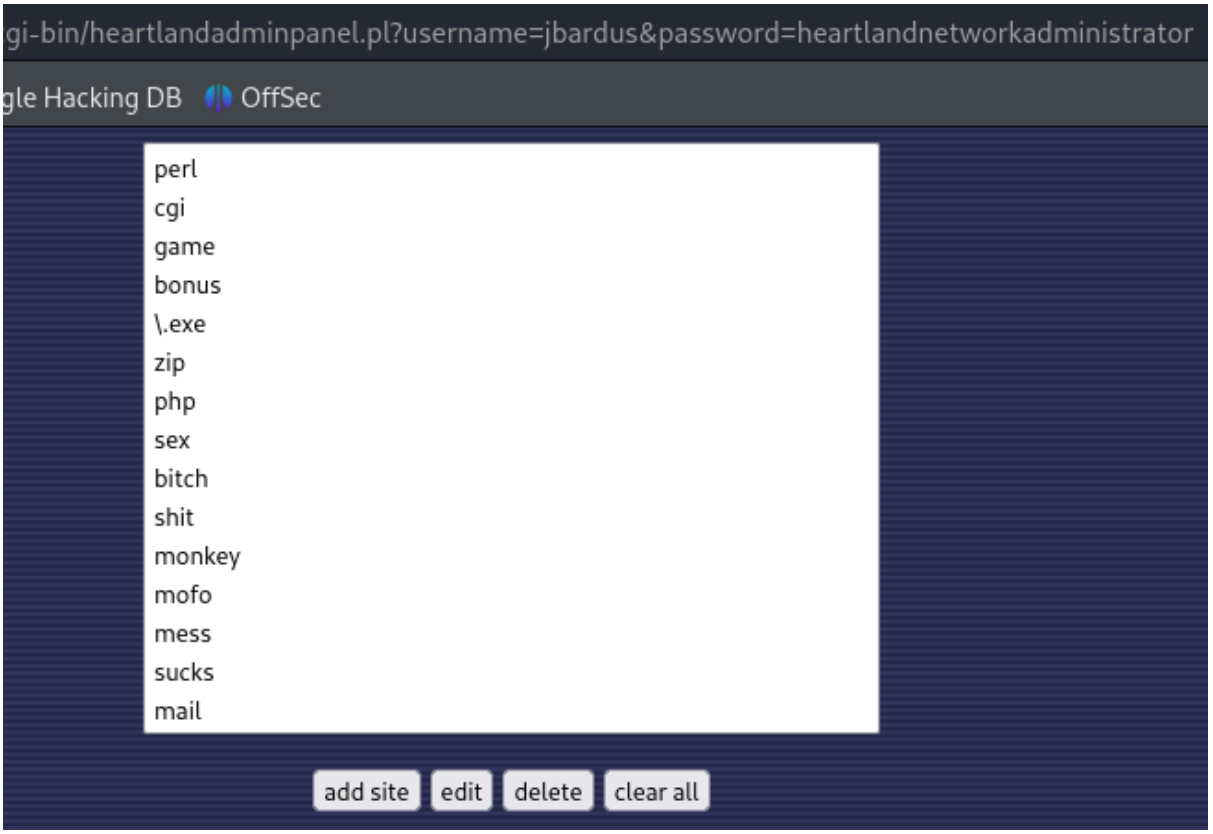


Essayer de se connecter avec des identifiants erronés nous dévoile l'existence d'un fichier perl du même nom que la page de connexion :

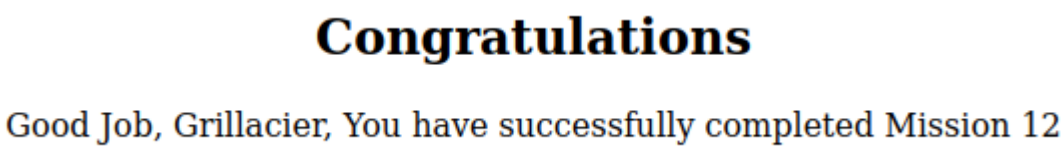


On retourne sur le site de l'élève pour accéder à ce script :

La première valeur ressemble à un pseudo, la deuxième est sûrement un mot de passe. On essaye de se connecter sur la page admin avec ces informations :



On peut voir tout ce qui a été bloqué par l'administrateur. On clique sur "clear all" :

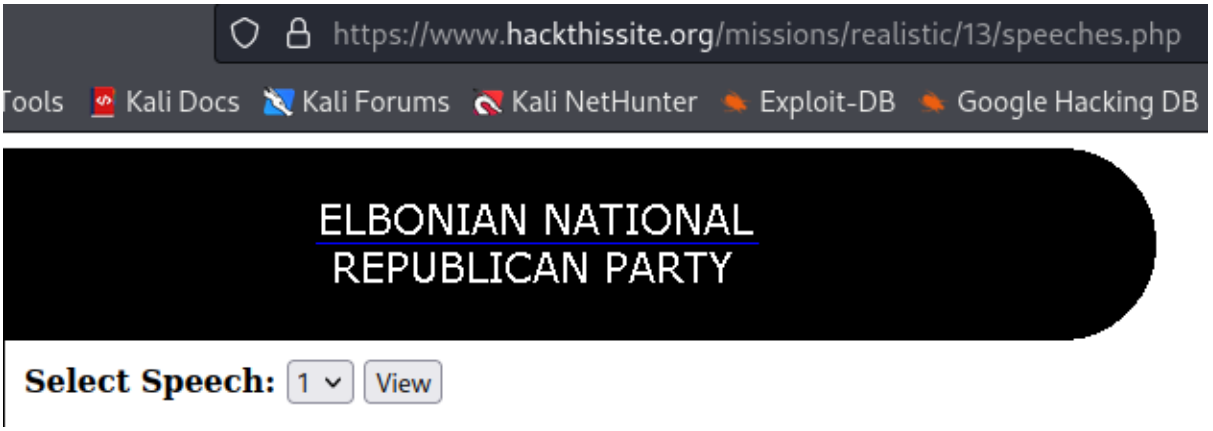


Level 13

On se rend sur la page “Newletter” où on apprend qu’il existe une page cachée où on peut se connecter :

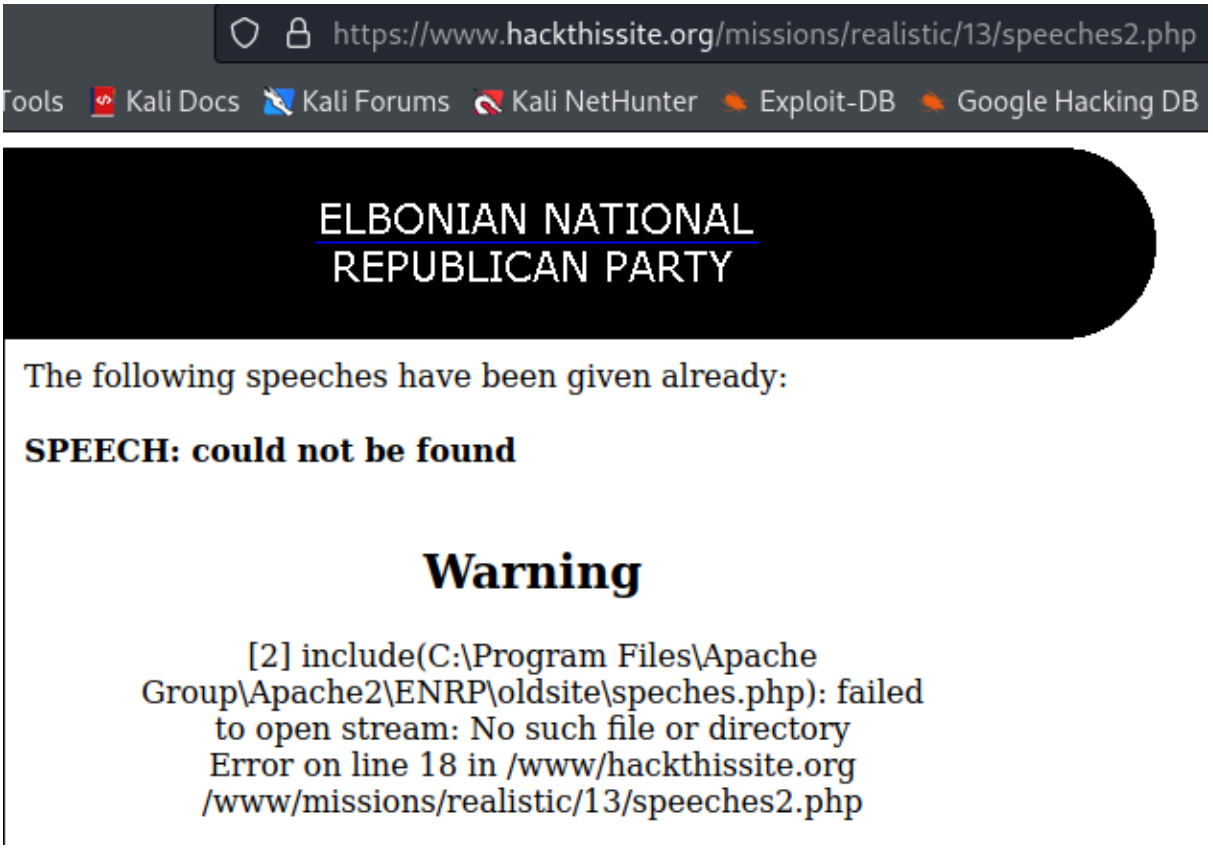
```
Our old Newsletters have all been cleared! We've
decided to start clean with this section to. It'll be
about another month before we have the rest of the
first new edition of the Newsletter done. One thing to
remember though, when you want to order our newsletter,
make sure you have the hidden login url and your
password handy.
```

On se rend sur la page “Speeches” :

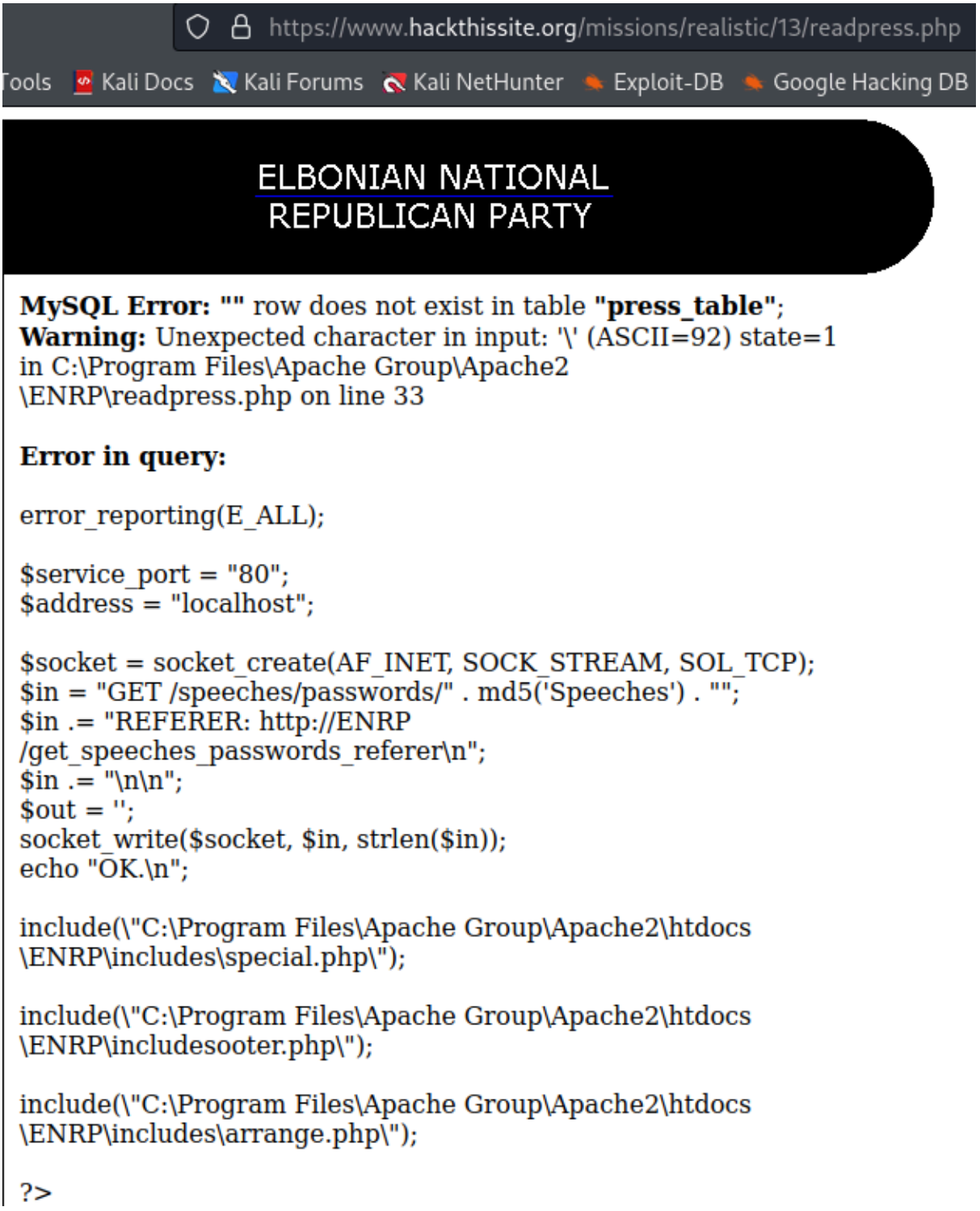


On peut choisir un numéro et et cliquer sur “View”, ce qui nous donne ce message :

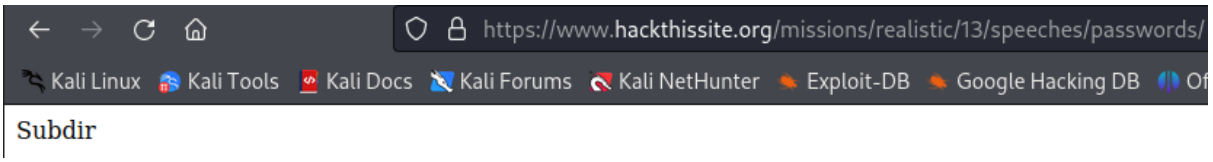
Mais lorsqu’on se rend manuellement à la page speeches2.php, on obtient plusieurs messages d’erreur :



La même chose se passe quand on réessaye dans la page “Press Releases” :



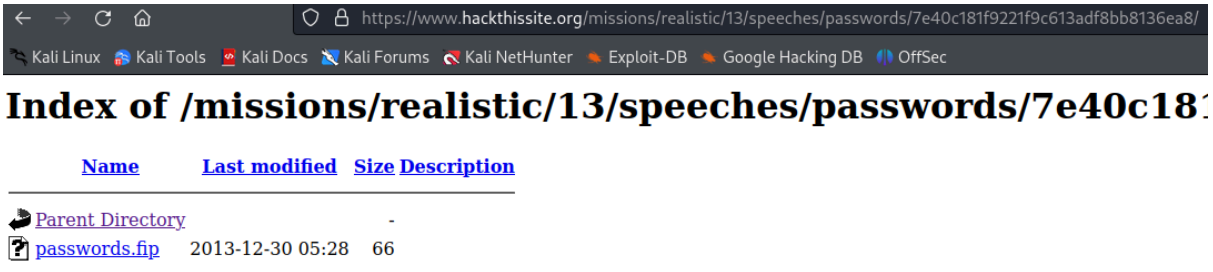
Le message d'erreur nous apprend l'existence d'un répertoire /speeches/passwords/ :



Le prochain sous-répertoire est le hash MD5 du mot "Speeches", on le trouve grâce à une commande dans le terminal :

```
┌──(alaia㉿kali)-[~/Documents/cours/cyberav/tp]
└─$ echo -n Speeches | md5sum
7e40c181f9221f9c613adf8bb8136ea8  -
```

Le répertoire contient un seul fichier :



Le fichier est composé d'une seule ligne au format login:mdp :

```
7bc35830abab8fced52657d38ea048df:21232f297a57a5a743894a0e4a801fc3
```

On suppose que ce sont aussi des hash MD5 puisque ce hash a déjà été utilisé précédemment dans ce niveau. On utilise john the ripper :

```
┌──(alaia㉿kali)-[~/Documents/cours/cyberav/tp]
└─$ john --format=raw-md5 level13login
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
moni1            (?)
1g 0:00:00:01 DONE 3/3 (2023-11-01 12:16) 0.6451g/s 1914Kp/s 1914Kc/s 1914KC/
s miny7..mouc2
Use the "--show --format=Raw-MD5" options to display all of the cracked passw
ords reliably
Session completed.
```

```
┌──(alaia㉿kali)-[~/Documents/cours/cyberav/tp]
└─$ john --format=raw-md5 level13pass
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
admin            (?)
1g 0:00:00:00 DONE 2/3 (2023-11-01 12:17) 100.0g/s 288000p/s 288000c/s 288000
C/s nina..buzz
Use the "--show --format=Raw-MD5" options to display all of the cracked passw
ords reliably
Session completed.
```

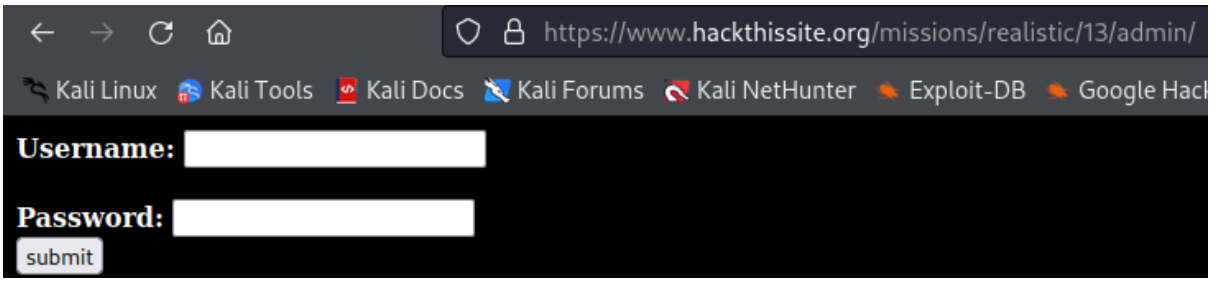
Les identifiants sont **moni1** et **admin**.
Parmi les erreurs de la page speeches2.php, on trouve une page admin :

Warning

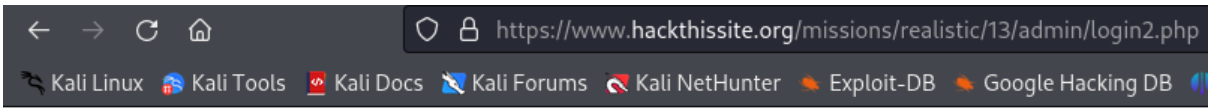
[2] include(C:\Program Files\Apache Group\Apache2\ENRP\admin\passes.php): failed to open stream: No such file or directory
Error on line 25 in /www/hackthissite.org /www/missions/realistic/13/speeches2.php

Warning

[2] include(): Failed opening 'C:\Program Files\Apache Group\Apache2\ENRP\admin \passes.php' for inclusion (include_path='.:/usr /local/share/pear')
Error on line 25 in /www/hackthissite.org /www/missions/realistic/13/speeches2.php



On essaye de se connecter :



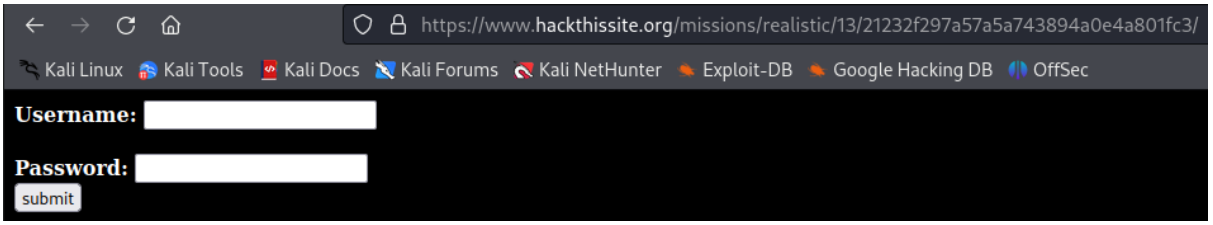
"admin" does not match password for "moni1"

On ne se trouve pas sur la fameuse page cachée. On retourne voir les messages d'erreur de tout à l'heure :

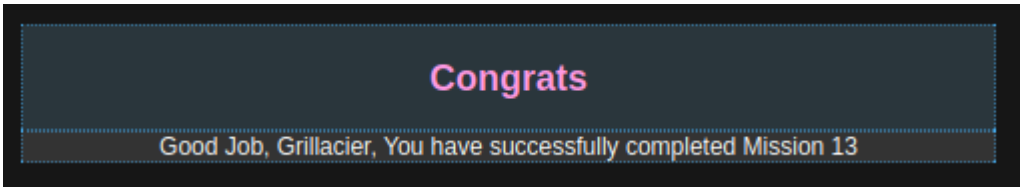
Warning

[2] include(): Failed opening 'C:\Program Files\Apache Group\Apache2 \ENRP\21232f297a57a5a743894a0e4a801fc3 \speches.php' for inclusion (include_path='.:/usr /local/share/pear')
Error on line 24 in /www/hackthissite.org /www/missions/realistic/13/speeches2.php

Cette fois-ci, on se rend à la page 21232f297a57a5a743894a0e4a801fc3 :

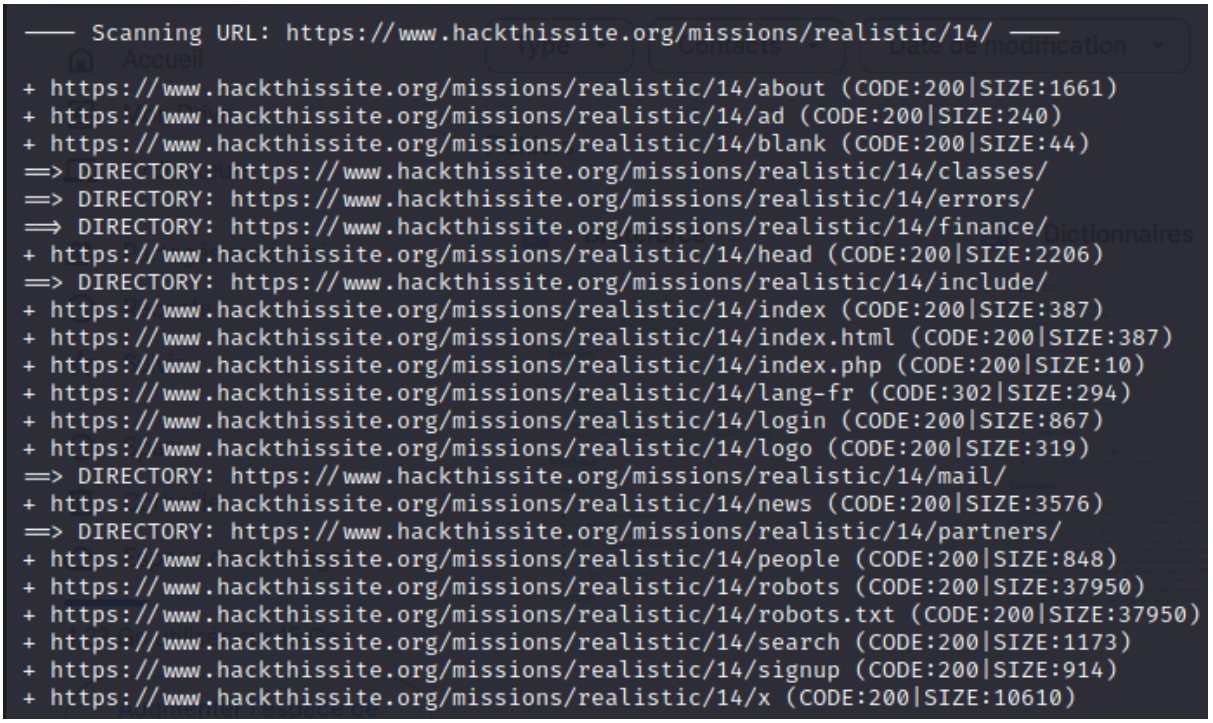


Il s'agit d'une autre page de connexion, identique à la page admin. On s'y connecte :



Level 14

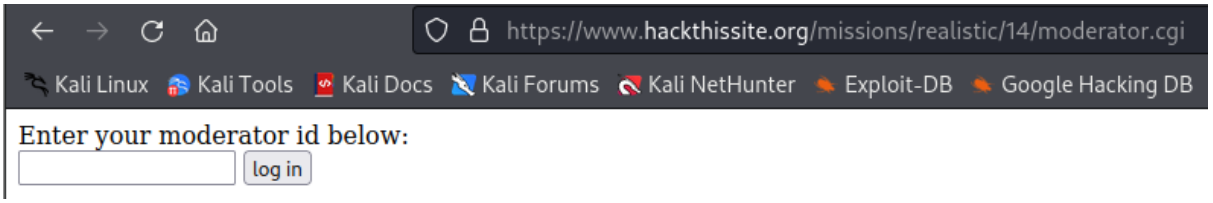
On cherche les fichiers du site :



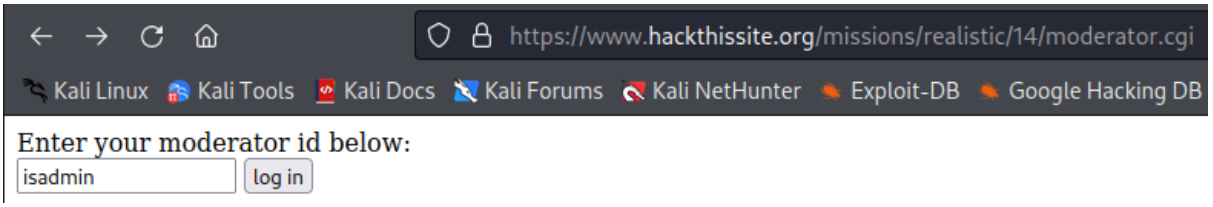
On ne trouve rien de pertinent donc on affine la recherche pour n'afficher que les fichiers .cgi qui sont assez utilisés sur le site :

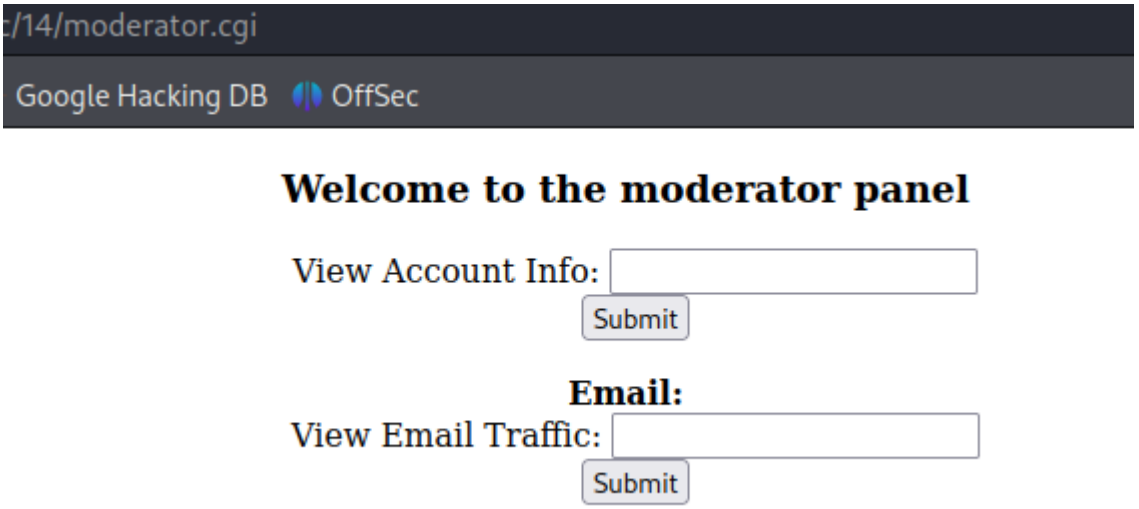
```
┌──(alaia㉿kali)-[~]
└─$ dirb https://www.hackthissite.org/missions/realistic/14/ -X .cgi

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Nov  1 19:13:17 2023
URL_BASE: https://www.hackthissite.org/missions/realistic/14/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.cgi) | (.cgi) [NUM = 1]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://www.hackthissite.org/missions/realistic/14/ ----
+ https://www.hackthissite.org/missions/realistic/14/administrator.cgi (CODE:200|SIZE:176)
+ https://www.hackthissite.org/missions/realistic/14/adserver.cgi (CODE:200|SIZE:6541)
+ https://www.hackthissite.org/missions/realistic/14/index.cgi (CODE:200|SIZE:2422)
+ https://www.hackthissite.org/missions/realistic/14/moderator.cgi (CODE:200|SIZE:218)
+ https://www.hackthissite.org/missions/realistic/14/news.cgi (CODE:200|SIZE:2670)
+ https://www.hackthissite.org/missions/realistic/14/people.cgi (CODE:200|SIZE:1139)
+ https://www.hackthissite.org/missions/realistic/14/search.cgi (CODE:200|SIZE:1121)


-----------------
END_TIME: Thu Nov  2 05:22:53 2023
DOWNLOADED: 4612 - FOUND: 7
```

On ne peut pas accéder à administrator.cgi mais moderator.cgi nous donne ceci :

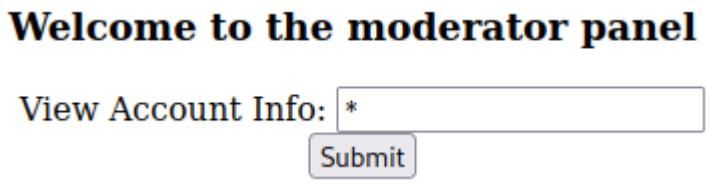


On veut se connecter en tant qu'admin :





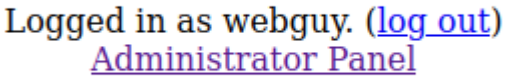
On cherche l'utilisateur * :



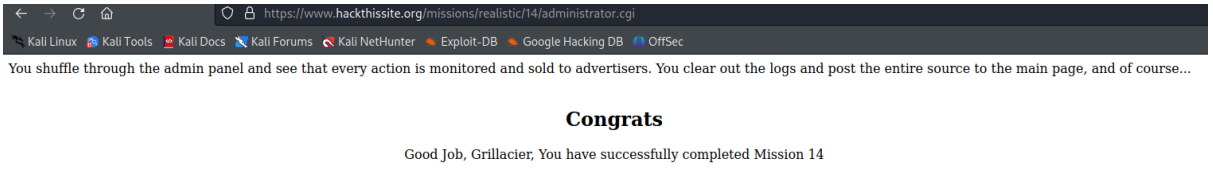
On obtient les informations d'un compte :

Admin Account
username: webguy
password: reallyreallylongpasswordthatisveryveryveryhardtoguessorcrack
Sha1 hash: 861d2106cb2f6cf54d59450e59cd8ba4cc5a5a05
email address: webguy@yuppers.nod
first name: Bob
middle name: Underwood
last name: Yuppers
month of birth: Male
day of birth: Unmarried
year of birth: September
gender: 24
marital status: 1973
country: United States
state: Idaho
city: Boise
address: 9451 Poplar Road
phone number: 539-124-5155
occupation: webmaster
income: 8650000
dependents: 0
first interest/hobby: programming
second interest/hobby: eating out
third interest/hobby: fund raising for Republicans
fourth interest/hobby: making TV ads
fifth interest/hobby: encryption
about: Hello, I am Bob Underwood Yuppers, and I am the CEO and founded Yuppers Internet Solutions.

On utilise le pseudo et le mot de passe trouvés pour se connecter :



On a maintenant accès à la page administrator.cgi, on clique sur le lien :



Level 15

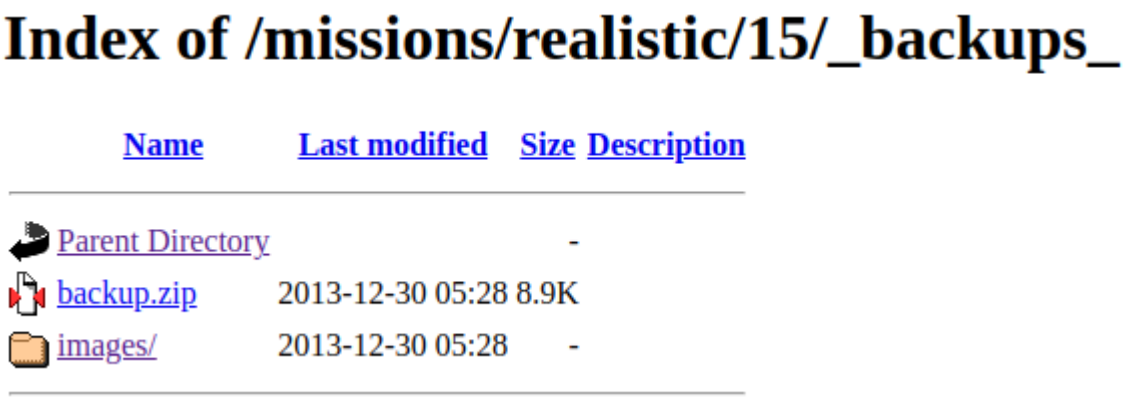
On trouve des informations dans le code source de la page d'accueil :

```
<meta name="KeyWords"     content="laser,war,smart bombs,night vision aid">
<meta name="Author"       content="webadmin: Susy Slack,
                                   email s.slack@seculas.com">
<meta name="Description"  content="secuLas is an industry leader in defense and special mission lasers.
                                   We are proud of our product spectrum and reputation which bases on
                                   the highest ethical standards">
```

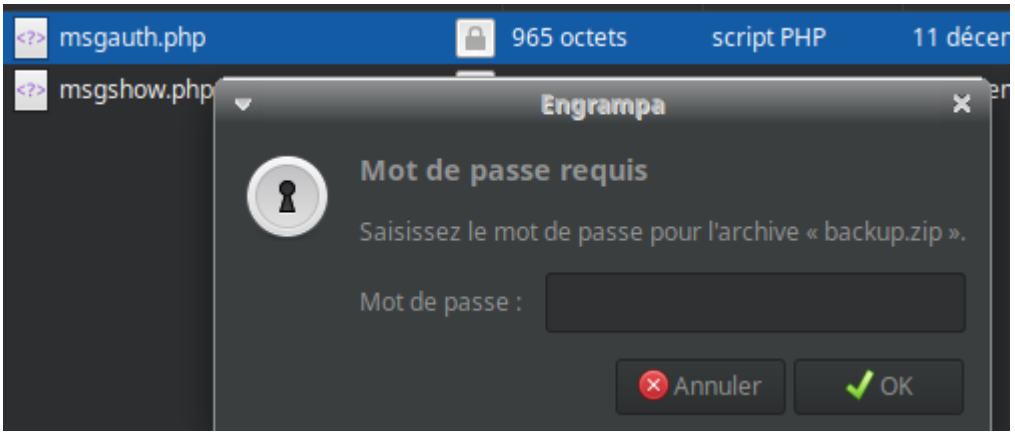
On se rend sur la page "Jobs" pour envoyer une candidature, puis on regarde le code source :

```
gn:center";><br /><br /><b><big>Your application has be
g src="_backups_/images/ok.gif" width="20" height="20"
```

Il y a un répertoire _backups_ sur le serveur :



On télécharge le fichier backup.zip qui s'y trouve. Le contenu est protégé par un mot de passe mais on peut afficher le nom et la taille des fichiers :

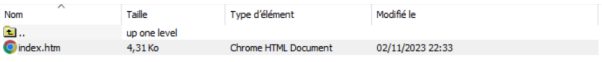


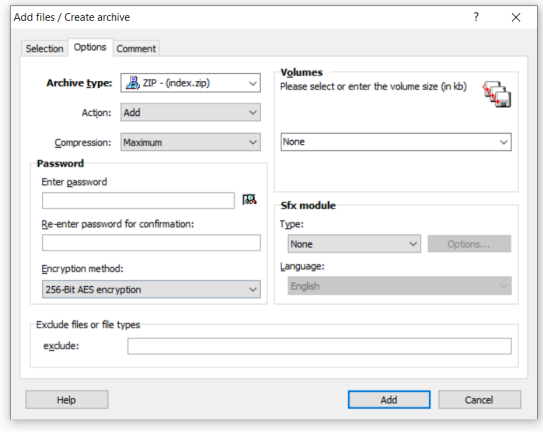

```
┌──(alaia㉿kali)-[~/Documents/cours/cyberav/tp]
└─$ unzip -l backup.zip
Archive:  backup.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
        0  2004-12-08 15:55   internal_messages/
      336  2004-12-08 15:44   internal_messages/msgshow.php
      965  2004-12-11 10:02   internal_messages/msgauth.php
        0  2004-12-05 12:51   misc (files from different folders)/
     4423  2004-12-04 12:41   misc (files from different folders)/index.htm
    16860  2004-12-05 12:51   misc (files from different folders)/shell.php
---------                     -------
    22584                     6 files
```

L'archive contient un fichier index.htm comme sur le site actuel, on télécharge la page avec wget :

```
┌──(alaia㉿kali)-[~/Documents/cours/cyberav/tp]
└─$ wget https://www.hackthissite.org/missions/realistic/15/index.htm
--2023-11-02 13:39:32--  https://www.hackthissite.org/missions/realistic/15/i
ndex.htm
Resolving www.hackthissite.org (www.hackthissite.org)... 137.74.187.104, 137.
74.187.103, 137.74.187.102, ...
Connecting to www.hackthissite.org (www.hackthissite.org)|137.74.187.104|:443
... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4423 (4.3K) [text/html]
Saving to: 'index.htm'

index.htm           100%[===================>]   4.32K  --.-KB/s    in 0s

2023-11-02 13:39:33 (82.8 MB/s) - 'index.htm' saved [4423/4423]
```

On crée un archive avec le fichier qu'on vient de récupérer :





On lance pkcrack pour trouver le mot de passe de l'archive :

```
┌──(root㉿kali)-[/home/alaia/Documents/pkcrack/bin]
└─# ./pkcrack -C ../../cours/cyberav/tp/backup.zip -c "misc (files from diffe
rent folders)/index.htm" -P ../../cours/cyberav/tp/index.zip -p index.htm -d
../../cours/cyberav/tp/result.zip -a
Files read. Starting stage 1 on Thu Nov  2 17:43:18 2023
Generating 1st generation of possible key2_1256 values ... done.
Found 4194304 possible key2-values.
Now we're trying to reduce these ...
Done. Left with 7670 possible Values. bestOffset is 24.
Stage 1 completed. Starting stage 2 on Thu Nov  2 17:43:29 2023
Ta-daaaaa! key0=f23a33d0, key1=106331c0, key2=6fd03c13
Probabilistic test succeeded for 1237 bytes.
Ta-daaaaa! key0=f23a33d0, key1=106331c0, key2=6fd03c13
Probabilistic test succeeded for 1237 bytes.
Stage 2 completed. Starting zipdecrypt on Thu Nov  2 17:46:28 2023
Decrypting internal_messages/ (351b31f4c660557eb3f9f7ae) ... OK!
Decrypting internal_messages/msgshow.php (d8070ee17e5e7b223bbe9bad) ... OK!
Decrypting internal_messages/msgauth.php (0d40acf30b5938d0a9c45b80) ... OK!
Decrypting misc (files from different folders)/ (bbf20bd1728f44ce85dc6f96) ...
 OK!
Decrypting misc (files from different folders)/index.htm (7cf5ab4329f7d177fc8
82c95) ... OK!
Decrypting misc (files from different folders)/shell.php (390c6ccd48169466e90
f6496) ... OK!
Finished on Thu Nov  2 17:46:28 2023
```

On apprend qu'il existe un fichier internal_messages.php, du même nom que le répertoire parent :

```
┌──(alaia㉿kali)-[~/Documents/cours/cyberav/
└─$ cat result/internal_messages/msgshow.php
<?php
/*-- called by internal_messages.php --*/
session_start();


include("showmessages.inc.php"); /* under co

$msg_password = $_POST['password'];
$msg_username = $_POST['username'];
$filename = "msgpasswords.txt";

include("msgauth.php");


showmessage($msg_username);
```

/15/internal_messages/internal_messages.php

Google Hacking DB OffSec

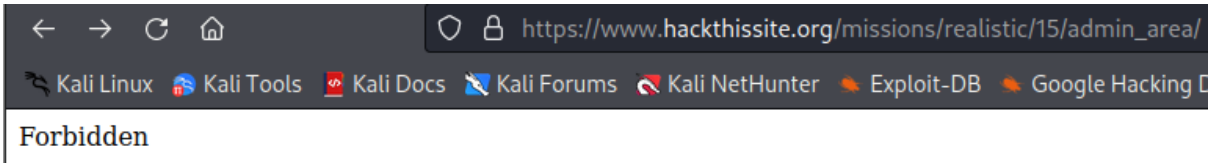
Internal messages

New messages		
# of messages	for	(enter passwd to read)
2	Dr. Nuts	read messages
1	J. Bardus	read messages
1	admin	read messages

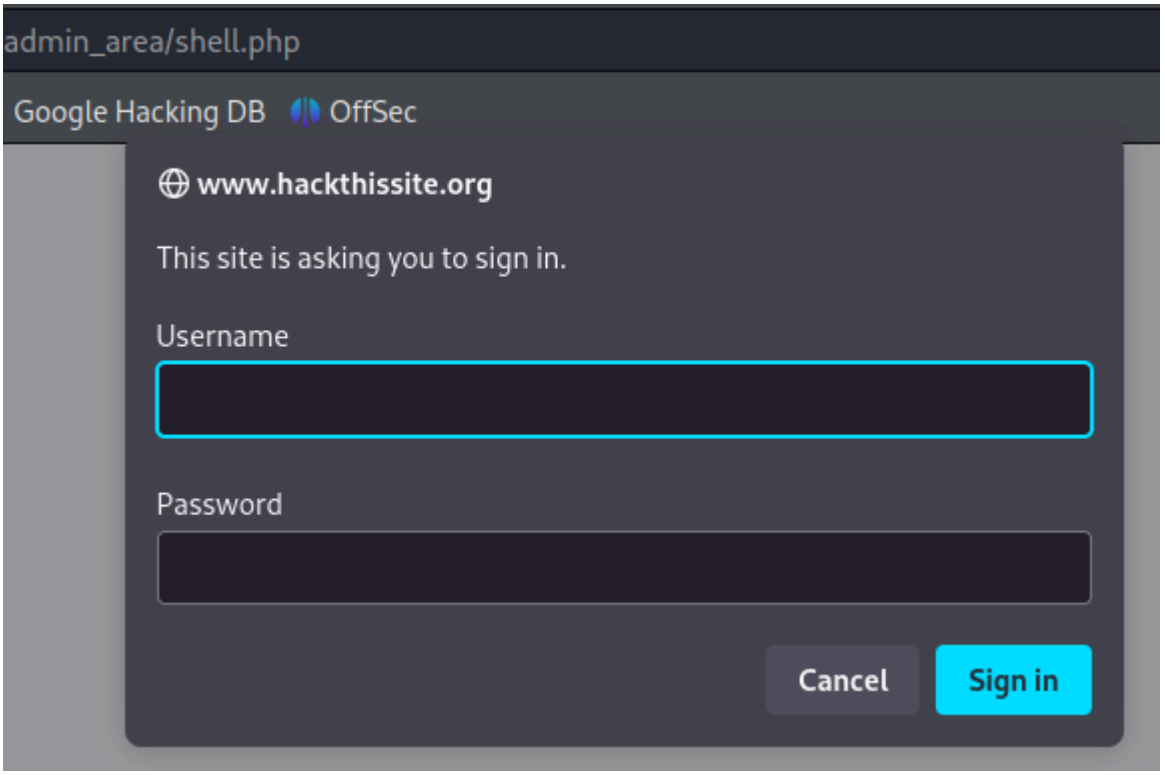
On cherche d'autres répepertoires/fichiers avec dirb :

```
┌──(alaia㉿kali)-[~/Documents/cours/cyberav/tp]
└─$ dirb https://www.hackthissite.org/missions/realistic/15/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Nov  2 18:39:59 2023
URL_BASE: https://www.hackthissite.org/missions/realistic/15/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://www.hackthissite.org/missions/realistic/15/ ----
+ https://www.hackthissite.org/missions/realistic/15/admin.cgi (CODE:403|SIZE:
+ https://www.hackthissite.org/missions/realistic/15/admin.pl (CODE:403|SIZE:1
==> DIRECTORY: https://www.hackthissite.org/missions/realistic/15/admin_area/
```

On trouve “admin_area” :



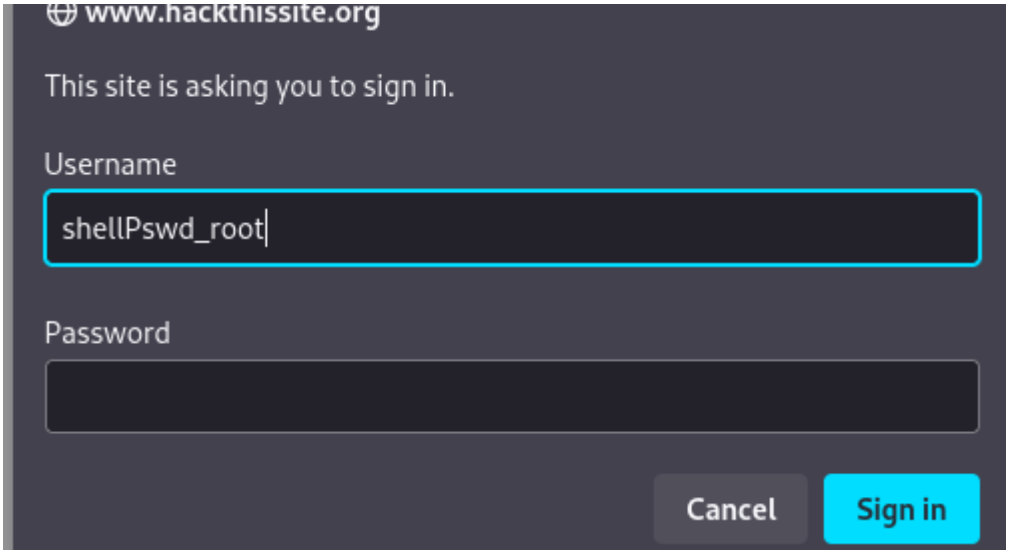
L’archive contient aussi un fichier shell.php, on essaye d’y accéder à partir du site :



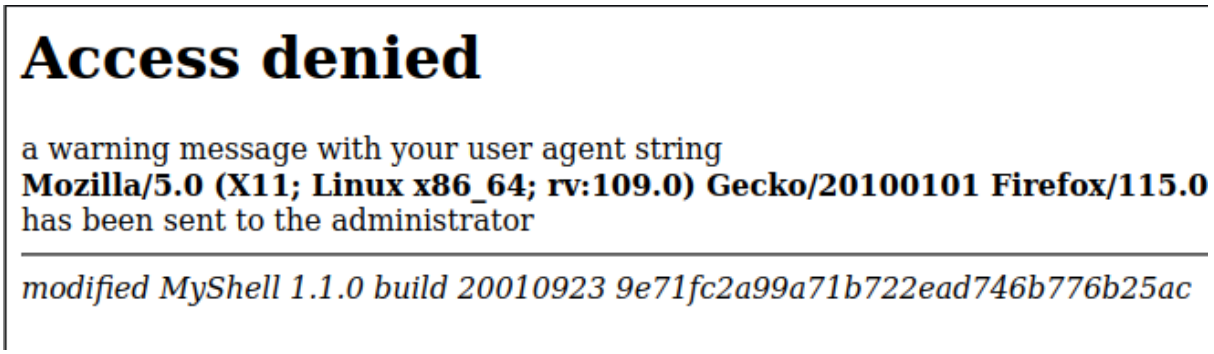
Le code du fichier nous donne un pseudo mais le mot de passe est caché :

```
$selfSecure = 1;
$shellUser_root   = "root";
$shellPswd_root   = "******************************"; // hash removed in this backup-file
$shellUser_others = "others";
$shellPswd_others = "******************************"; // hash removed in this backup-file
```

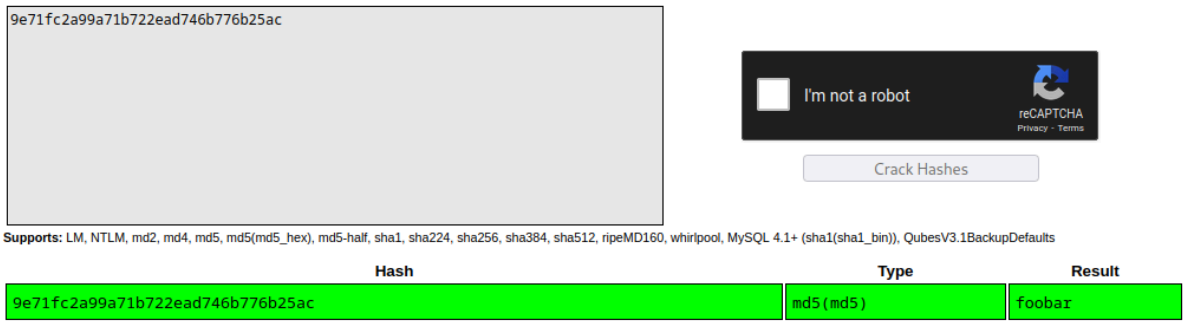
On copie le nom de la variable contenant le mot de passe dans le champ “Username”, on se connecte, et quand la fenêtre réapparaît, on clique sur “Cancel” :



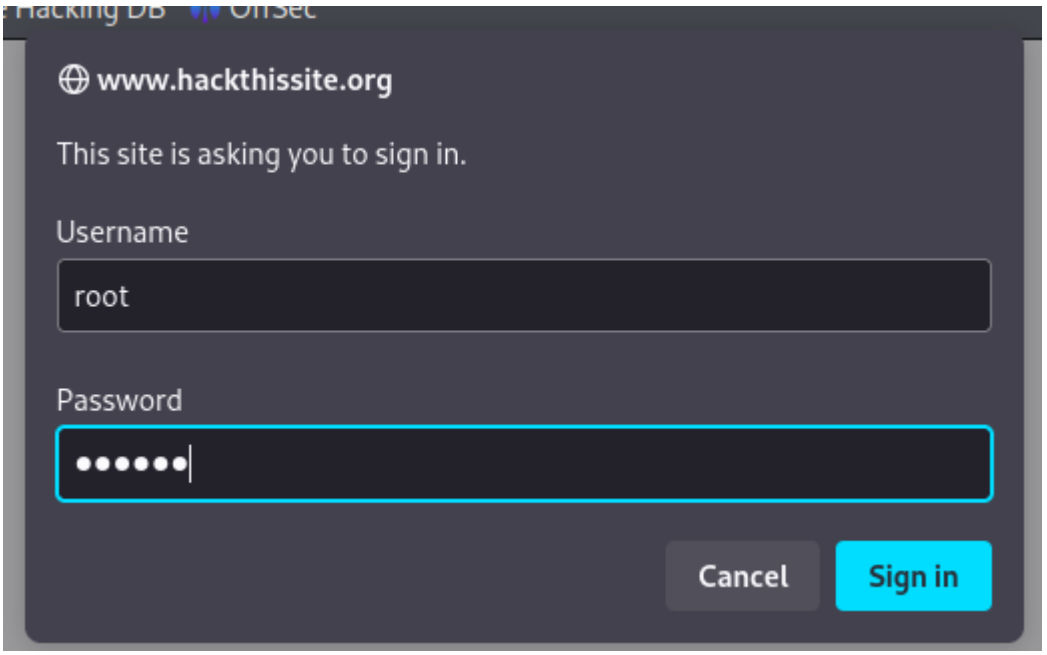
On obtient un message d’erreur ainsi qu’une chaîne de caractères ressemblant à un hash :



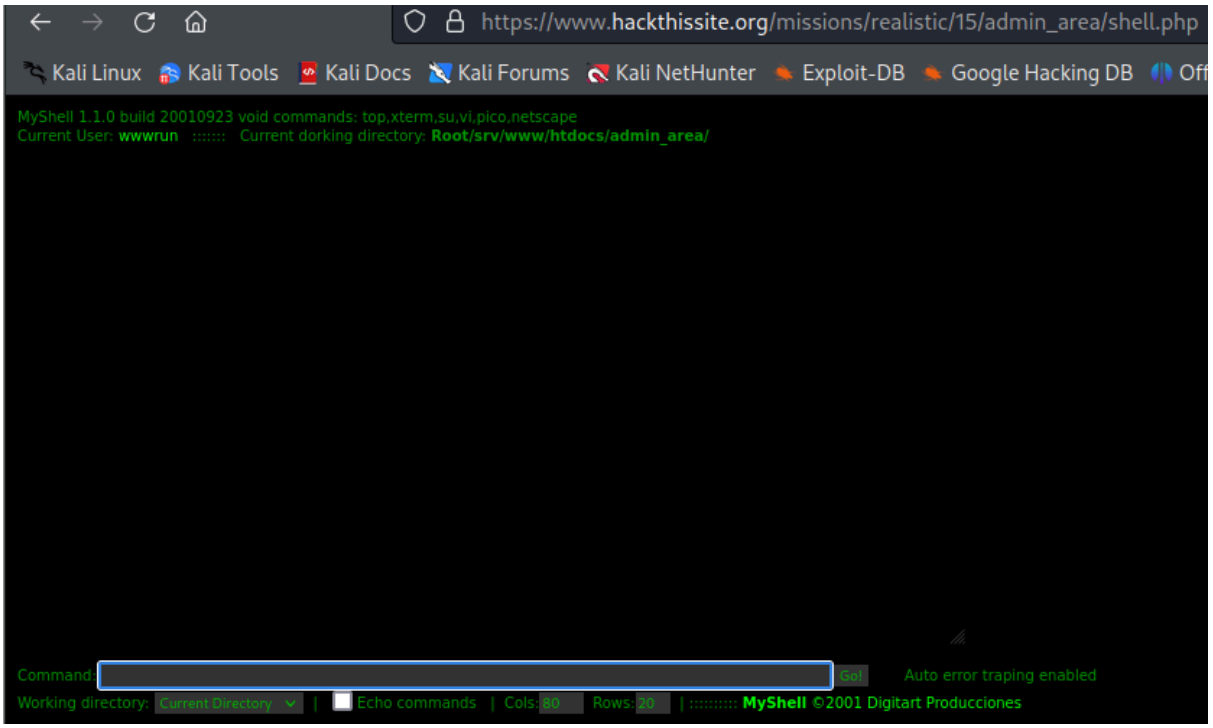
John the Ripper étant une feignasse, on se rend sur crackstation :



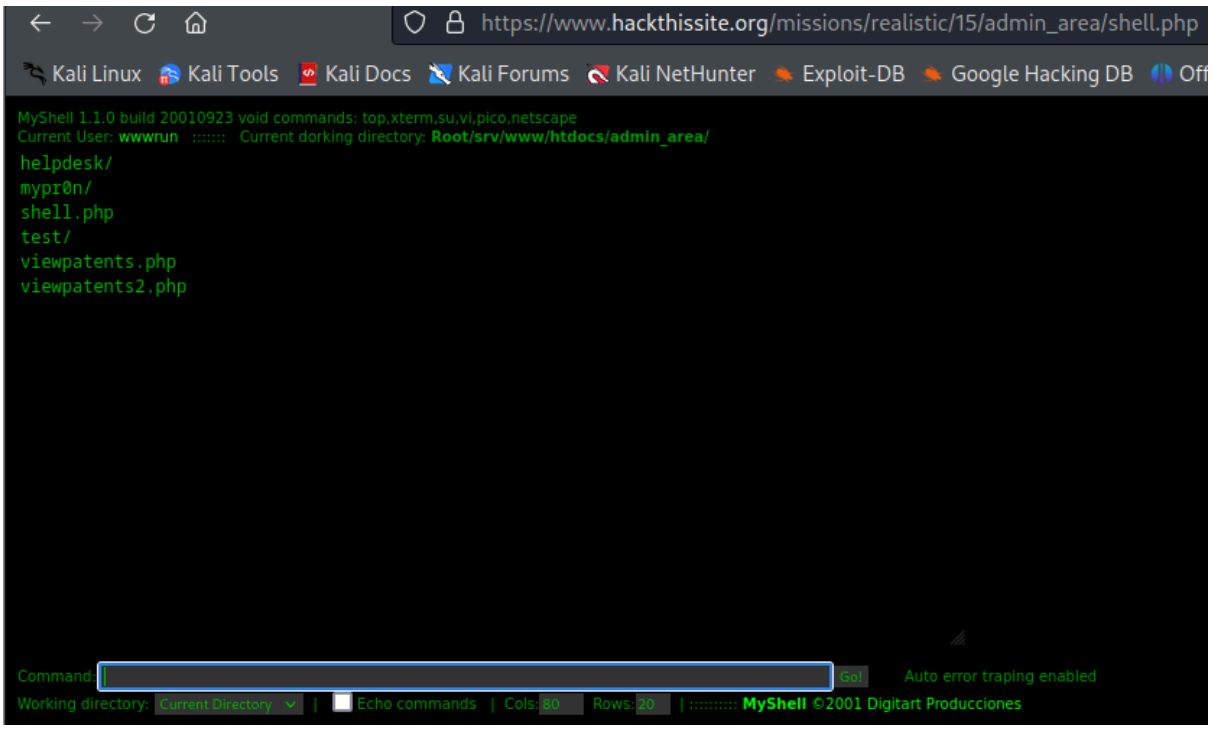
Le mot de passe est "**foobar**”. On se connecte :



Hacker voice I'm in.



La seule commande qui fonctionne est ls :



On se rend donc sur les différentes pages à partir du navigateur.
viewpatents.php nous demande de nous connecter :

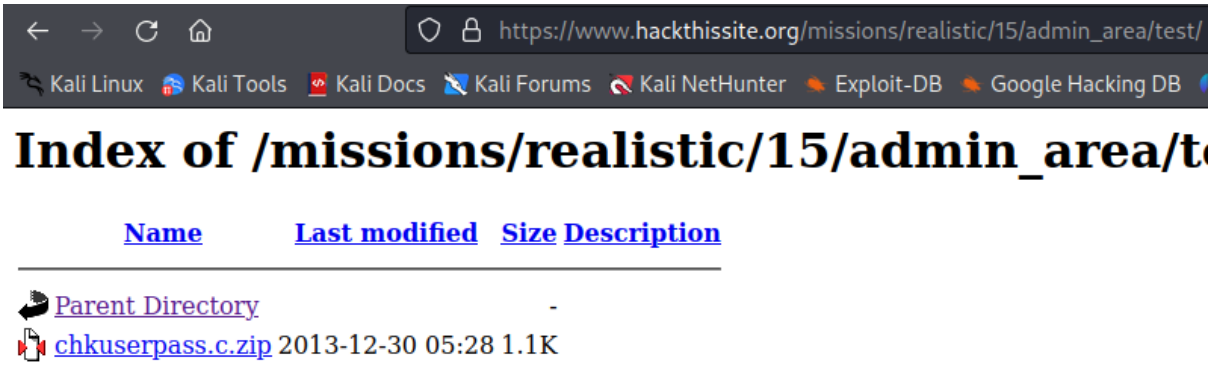
View latest patents and developments

Username:
Password:

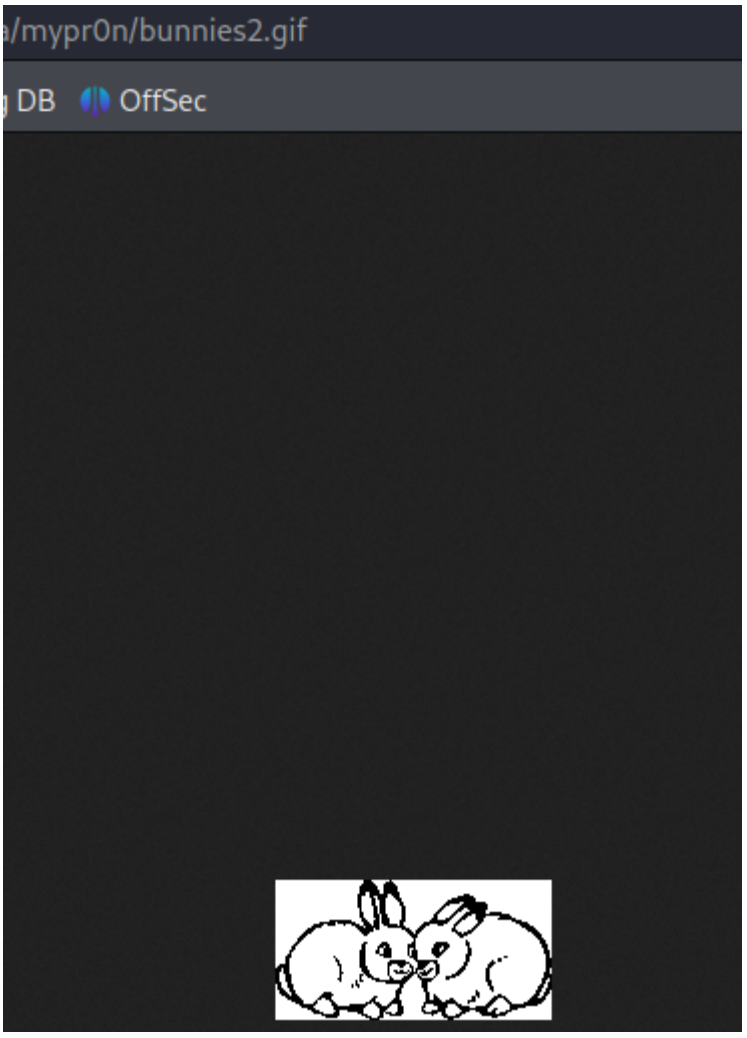
OK Reset

*Every attempt to access secret information is strongly prohibited. We are determined to find and sue **every** person that tries to access without having the permission.*

Dans test/, on télécharge un fichier :



Dans mypr0n/, on trouve plusieurs images dont une de deux lapins. C'est mignon :

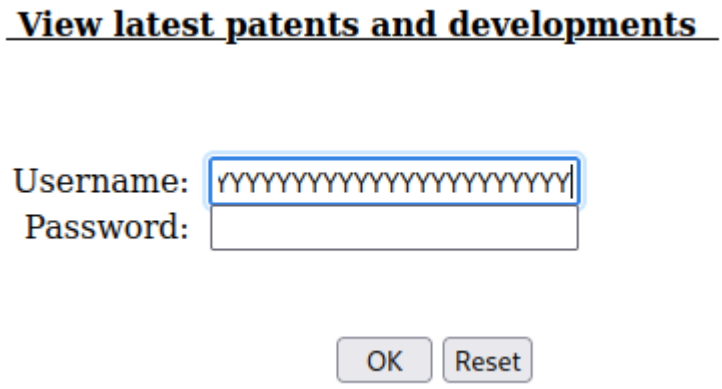


Le reste ne semble pas utile.
On regarde le contenu de l'archive qu'on vient de télécharger. On trouve du code écrit en C :

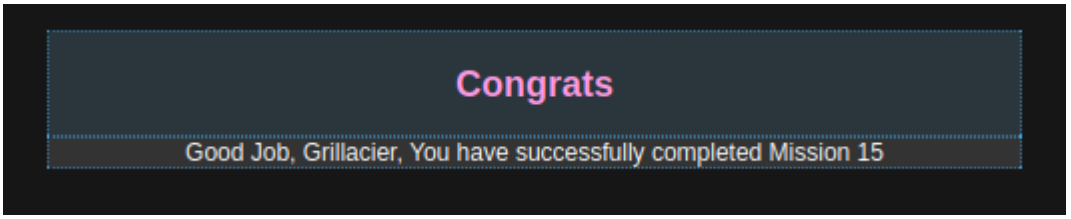
```
/*-------------------------------------------------------*/
/*   Modified md5 hash                       J.Bardus    */
/*   Check if username and password are valid.           */
/*                                                       */
/*   I set up this exra secure password checker to       */
/*   validate username/password in the 'latest development */
/*   and patents' - section.                             */
/*                                                       */
/*   Since some users -and even administrators-           */
/*   use short passwords I make this a bit more          */
/*   secure. A less than 4 chars password is filled      */
/*   up with some extra characters.                      */
/*   The hash is built from a string which is built      */
/*   by concatenating username and password.             */
/*   I use my own modified md5-algo with an additional   */
/*   XOR, which is performed at different stages in      */
/*   the md5-algo.                                       */
/*   This all together makes it impossible to reverse    */
/*   or brute force this algo.                           */
/*   (The good old security through obscurity though)    */
/*-------------------------------------------------------*/
```

```
/*-------------------------------------------------------*/
/*  checks given username and password                   */
/*  return value: 'Y' or 'N'                             */
/*-------------------------------------------------------*/
char checkit(char* username, char* password, char* hash)
{
 char is_pass_correct = 'N';    /* initialize to NO
 char *fillstring = "_T*4$n";   /* Use this string to make a
                                /* less than 4chars password
                                /* longer
 char concatenated[200];
 strcpy(concatenated, username);

 /*  if a password is less than 4 chars long,  */
 /*  add some extra characters                 */
 if (strlen(password) < 4)
   strcat(concatenated, fillstring);

 strcat(concatenated, password);

 if (strcmp(mymd5(concatenated), hash) == 0)
   is_pass_correct = 'Y';

return is_pass_correct;
```

Les pseudos doivent avoir entre 4 et 200 caractères et un pseudo valide renvoie un “Y”. On veut forcer le programme à nous renvoyer un “Y”, pour cela, on choisit un pseudo composé uniquement de “Y” et d’une longueur supérieure à 200. Ici, on a 228 “Y” :

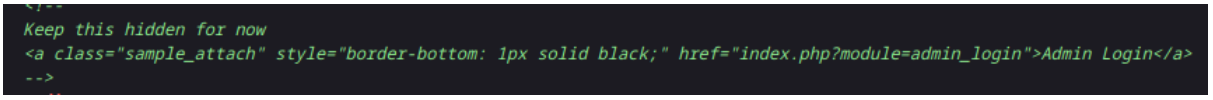


On clique sur “OK” :



Level 16

On découvre l’existence d’une page admin_login en regardant les commentaires dans le code source :



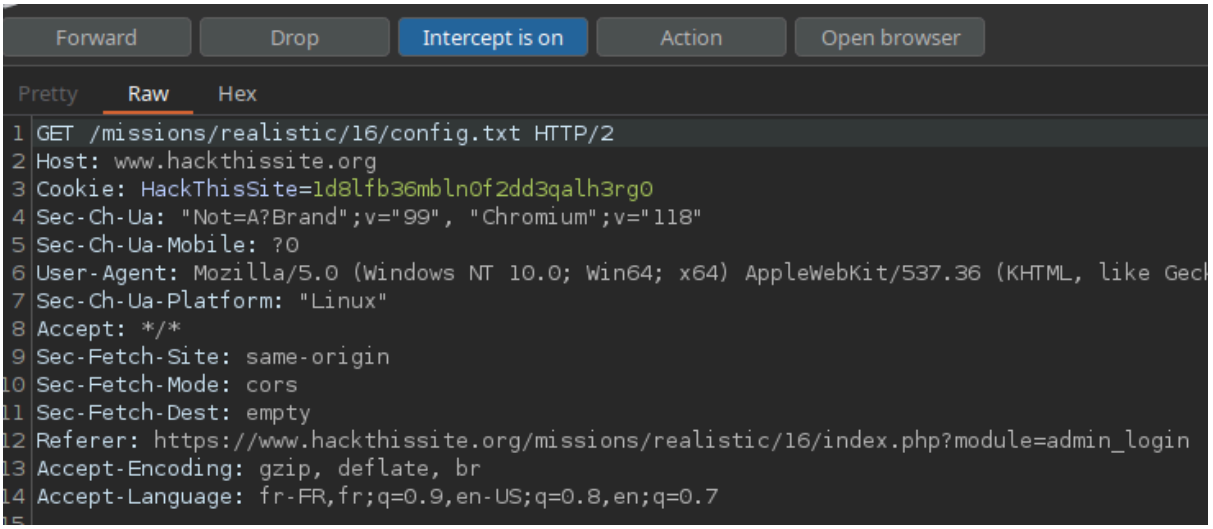
Pour l’instant, on ne voit rien dans la page :

On regarde le code source et on voit que la page utilise flash :

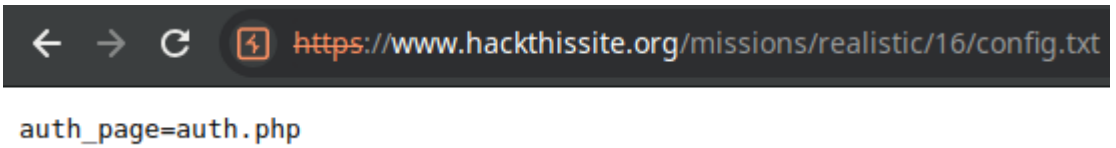
```
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=9,0,0,0"
```

On télécharge l'extension Ruffle et on peut enfin voir le contenu :

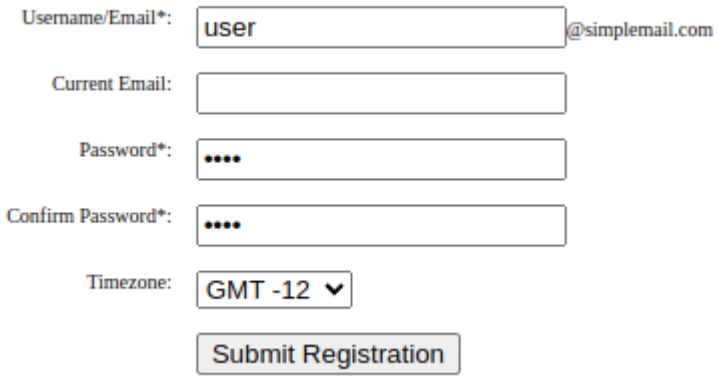
On dégaine notre meilleur ami burpsuite qui nous montre un fichier config.txt :



Son contenu :



On retourne sur le site et on se crée un compte :



On se connecte et on consulte ses mails. Actualiser la page fait apparaître un nouveau spam, c’est rigolo :

Logged in as: **user@simplemail.com**

From:	Date:	Size:	Subject:
xtrasize@spam.com	11/2/23, 9:17:25 am	31 kb	XtraSize+ -- Paris Hilton likes them BIG!!!
MegaTHICK@spam.com	11/2/23, 9:17:24 am	92 kb	Stretch her out with MegaTHICK!!!
MegaTHICK@spam.com	11/2/23, 9:17:24 am	80 kb	Stretch her out with MegaTHICK!!!
Chukwu Babatunde <dchthe4g@spam.com>	11/2/23, 9:17:23 am	63 kb	Large sum of money from NIGERIA PRESIDENT!
Viagra@spam.com	11/2/23, 9:17:23 am	40 kb	Please your woman... or man!
GetBiggerNow@spam.com	11/2/23, 9:17:21 am	96 kb	Make that pathetic twig Hu-u-u-u-ge!
Chukwu Babatunde <dchthe4g@spam.com>	11/2/23, 9:17:21 am	70 kb	Large sum of money from NIGERIA PRESIDENT!
xtrasize@spam.com	11/2/23, 9:17:20 am	62 kb	XtraSize+ -- Paris Hilton likes them BIG!!!
BiggerManhood@spam.com	11/2/23, 9:17:20 am	127 kb	GROW 2000X BIGGER FORMULA
Viagra@spam.com	11/2/23, 9:17:20 am	78 kb	Please your woman... or man!
Viagra@spam.com	11/2/23, 9:17:19 am	165 kb	Please your woman... or man!

On modifie son compte et on regarde le code source :

```
         Logged in as: <b>user@simplemail.com</b><hr /><br /><
<!--
This is just for debugging:

Notice: The file "./users/user/config.txt" was saved successfully
-->
```

Le contenu de ce fichier :

https://www.hackthissite.org/missions/realistic/16/users/user/config.txt

```
No Personal Message;
-12;
;

\\These is the user config file notes, anything with \\ in front is ignored
\\Line 1: Personal message
\\Line 2: Timezone
\\Line 3: Current Email
```

On se déconnecte et on crée un nouveau compte qu'on va cette fois appeler ".." :

Username/Email*: .. @simplemail.com

Current Email:

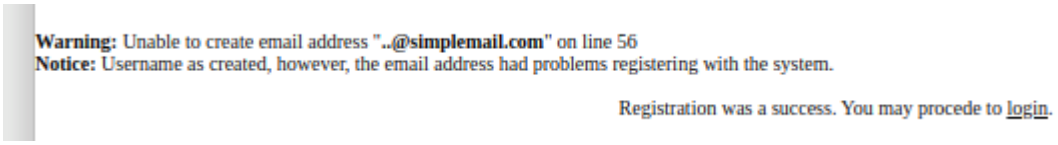
Password*: ••••

Confirm Password*: ••••

Timezone: GMT -12

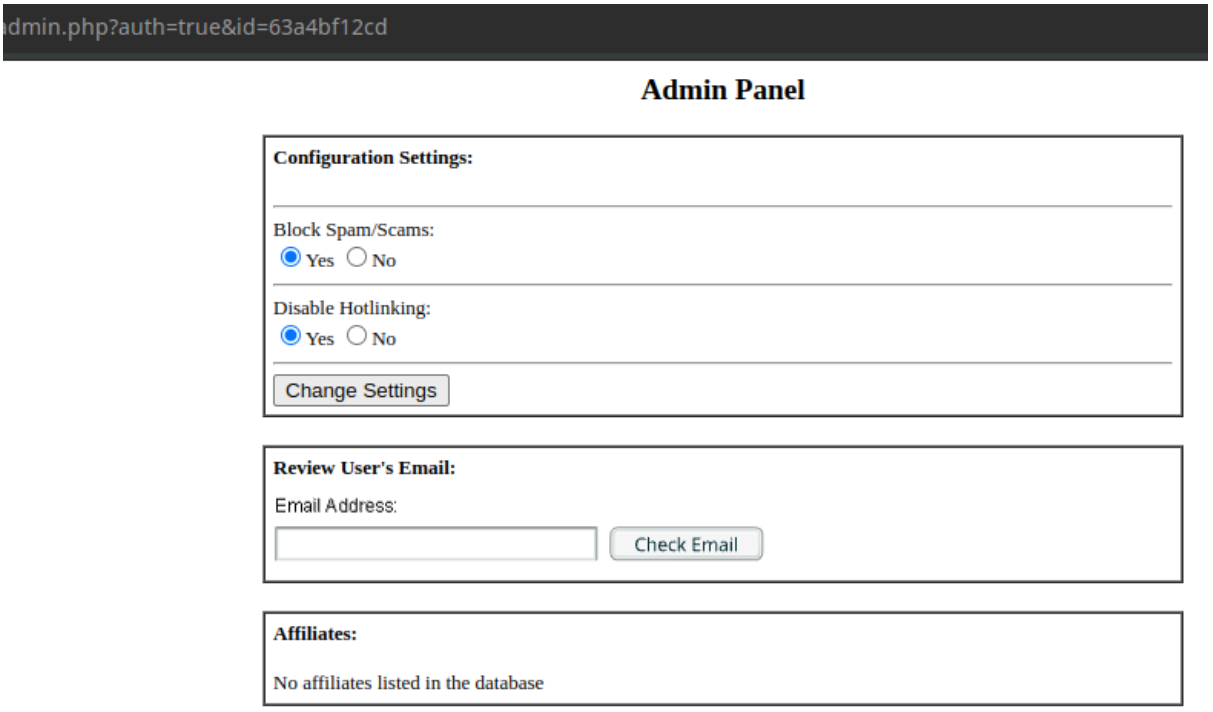
Submit Registration

On obtient un message d'erreur et un message de confirmation en même temps :



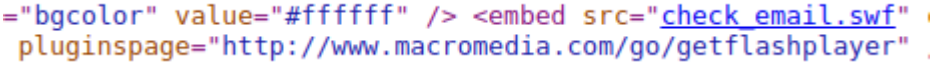
On se connecte à ce nouveau compte et on modifie son message personnel :

On se connecte à notre premier compte, mais à partir de la page admin cette fois :

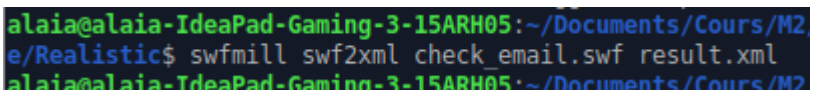


Entrer le mail de notre victime ne fonctionne pas :

On découvre un fichier flash dans le code source, on clique dessus pour le télécharger :



On le convertit en fichier XML :



On affiche son contenu :

```
<Dictionary>
  <strings>
    <String value="check_enabled"/>
    <String value="./check_email.php?auth=true&amp;id=63a4bf12cd&amp;email="/>
    <String value=""/>
  </strings>
</Dictionary>
```

On copie ce qu'on vient de trouver dans l'URL et on complète avec le mail de Jenn :