

# FAILLES

Verrou par verrou et l'un après l'autre, aucun système ne résistera !



JUSTAL KEVIN

2014-2015

Justal Kevin - [justal.kevin@gmail.com](mailto:justal.kevin@gmail.com)

# Table des matières

<b>1</b>	<b>Ecrire des données par dessus une images - Caché du contenu</b>	<b>3</b>
1.1	Prérequis . . . . .	3
1.2	Etapes par Etape . . . . .	3
<b>2</b>	<b>Fonctions PHP</b>	<b>4</b>
2.1	Logique humaine . . . . .	4
2.1.1	L'ancrage du "str replace" ou le mauvais filtre . . . . .	4
2.1.2	Solutions . . . . .	4
<b>3</b>	<b>Directory transversal - Attaque sur le htaccess</b>	<b>5</b>
3.1	Explications . . . . .	5
3.1.1	Qu'est ce que la technologie htaccess ? . . . . .	5
3.1.2	Les directives htaccess . . . . .	5
3.1.3	Les directives htpasswd . . . . .	5
3.2	La navigation transversale ou Directory transversal . . . . .	5
3.3	Exploitation . . . . .	6
3.4	Variante . . . . .	7
3.5	Solutions . . . . .	7
<b>4</b>	<b>SMTP Injection - Injection dans la fonction php mail()</b>	<b>8</b>
4.0.1	Qu'est ce qu'un envoi de message ? . . . . .	8
4.0.2	La fonction mail() de php . . . . .	8
4.1	Qu'est ce qu'une injection de header . . . . .	9
4.2	Exemple . . . . .	9
4.3	Solutions . . . . .	11
<b>5</b>	<b>Attaque temporel - Attaque par Canaux cachés</b>	<b>12</b>
5.1	Qu'est ce qu'un canal caché ? . . . . .	12
<b>6</b>	<b>CSRF - Cross-site request forgery</b>	<b>13</b>
6.1	Qu'est ce qu'une attaque CRSF ? . . . . .	13
<b>7</b>	<b>XSS</b>	<b>14</b>
7.1	Simple XSS - balise script . . . . .	14
7.2	XSS Trick - Bypass htmlspecialchars in some cases . . . . .	14
7.3	XSS Trick - Bypass htmlspecialchars et htmlentities . . . . .	15
<b>8</b>	<b>Bibliographie</b>	<b>17</b>
8.1	SMTP Injection . . . . .	17

# **1 Ecrire des données par dessus une images - Caché du contenu**

## **1.1 Prérequis**

Pour réaliser cela, il faut impérativement avoir téléchargé et installé sur son ordinateur 7zip, un utilitaire de compression.

## **1.2 Etapes par Etape**

Le but ici est simplement de s'amuser à cacher des fichiers de tous genre dans une image. Cela ne semble pas avoir d'intérêt quelconque mais permet avec d'autres failles de faire télécharger à l'insu de l'utilisateur le malware et de le déclencher d'une autre méthode. Comment fais-t-on ?

## 2 Fonctions PHP

### 2.1 Logique humaine

#### 2.1.1 L'ancrage du "str replace" ou le mauvais filtre

Le filtre est un classique du WEB. Toutes les chaînes qui entrent doivent être analysées pour empêcher l'utilisateur d'entrer des choses à des fins malicieuses. Même ce principe de base qui consiste à simplement éliminer une chaîne dans une chaîne peut avec une simple erreur humaine permettre de faire un peu tout et n'importe quoi. Prenons l'exemple d'un simple formulaire :

```
<form method="POST" action="">
  <input type="text" name="secret"><br>
  <input type="submit" name="send" value="Envoyer">
</form>
```

Il s'agit d'un simple champ texte que j'envoie par une méthode POST sur la même page que ce bout de code. Si vous ne comprenez pas, ce n'est pas bien grave, ceci ne sert qu'à mettre un contexte. Maintenant imaginons que nous souhaitons récupérer la variable et filtrer tout Javascript :

```
$var=str_replace("<script>","",$_POST["secret"]);
```

J'ai retrouvé ce bout de code sur plusieurs sites et ceci m'a légèrement fait sourire. Comme on peut le voir sur cette ligne ci-dessus, nous remplaçons toutes les balises `<script>` par une chaîne vide. Il y a pourtant ici 2 erreurs flagrantes.

La première demande de connaître exactement ce que fait la balise `str_replace`. Dans le HTML, il est possible d'utiliser des balises écrites en minuscule ou en majuscule. Or, `str_replace` respecte la case, il m'est donc possible de rentrer une balise `<SCRIPT>` sans que le filtre ne s'alarme. La deuxième est simple d'ordre logique, que se passe-t-il si j'envoie ceci via mon script PHP :

```
<sc<script>ript>alert("HAHA")</sc<script>ript>
```

Dans cette chaîne, si nous remplaçons `script` par une chaîne vide nous obtenons :

```
<script>alert("HAHA")<script>
```

On réussit ainsi à bypasser le filtre de manière assez simple.

#### 2.1.2 Solutions

Pourquoi ne pas simplement utiliser les fonctions PHP : `htmlspecialchars()` et `htmlspecialchars()`.

## 3 Directory transversal - Attaque sur le htaccess

### 3.1 Explications

#### 3.1.1 Qu'est ce que la technologie htaccess ?

Les fichiers .htaccess sont des fichiers de configuration de Apache. Ils permettent de sécuriser via un mot de passe et un identifiant l'accès à une zone du serveur. Ils sont localisés et ne peuvent affecter que les répertoire où ils résident. La particularité d'une telle fonctionnalité apporte deux avantages. D'une part, on peut déléguer la gestion d'une partie du site sans donner le droit de gérer le serveur lui-même. D'autre part, les modifications sont prises en compte sans qu'il soit nécessaire de redémarrer le serveur HTML.

#### 3.1.2 Les directives htaccess

Un fichier htaccess prend la forme suivante :

```
AuthUserFile /var/www/.htpasswd
AuthName "Visiteur, vous pénétrez dans une section réservée aux membres, veuillez vous identifier"
AuthType Basic
require Admin
```

La première directive, **AuthUserFile**, est le lien entre le htaccess et le htpasswd. Cette simple directive indique simplement où se situe le fichier htpasswd. Le chemin inscrit ici est généralement le chemin d'accès absolue mais il est possible de trouver aussi un chemin relative mais cela reste tout de même relativement rare.

La directive **AuthName** permet de spécifier un titre à la fenêtre de connexion.

La directive **AuthType** indique le type d'authentification. Il n'existe que deux types possibles : Basic ou Digest. Le premier type indique simplement que le mot de passe lors de l'authentification sera transmise en clair du client au serveur. C'est pourquoi cette méthode n'est pas à utiliser pour un transfert de donnée sensible. Le type Digest est un soi-disant type améliorant la sécurité du transfert, cependant de nombreuses failles existent ici. Ce qui rend ce type inutile car plus lourd à mettre en place et pas vraiment sécurisé.

La directive **require** spécifie simplement qui est autorisé à accéder à cette partie du site. On ira donc chercher dans le fichier htpasswd l'utilisateur Admin pour comparer le mot de passe.

#### 3.1.3 Les directives htpasswd

Un fichier htpasswd prend la forme suivante :

```
admin1 :$apr1$Ikl22aeJ$w1uWlBGlbPnETT2XGx..
admin2 :$apr1$yJnQGpTi$WF5eCC/8lKsgBKY7fvag60
```

Un fichier htpasswd prend toujours la forme ci-dessus. Ce fichier lie un utilisateur à un password crypté via un algorithme comme SHA, DES, MD5...

### 3.2 La navigation transversale ou Directory transversal

Pour expliquer la faille, je prendrais un exemple. Le site w3challs.com dispose d'un exemple sur cette faille du système. Avant même de commencer l'expérimentation, il faut encore un peu d'explication pour comprendre la faille. Cette faille réside dans le PHP du site et en particulier dans la balise include.

```
$template = 'red.php';
if (isset($_COOKIE['TEMPLATE']))
    $template = $_COOKIE['TEMPLATE'];
include ("/home/users/phpguru/templates/" . $template);
```

Ici, le fait que dans l'include, on ne vérifie pas que le résultat attendu soit une page .html ou .php, on peut alors imaginer de modifier la variable \$template. Il y a plusieurs manières de procéder qui dépendent de la manière dont est implémenté le code du site que l'on souhaite attaquer : Par l'URL, Par la requête HTML...

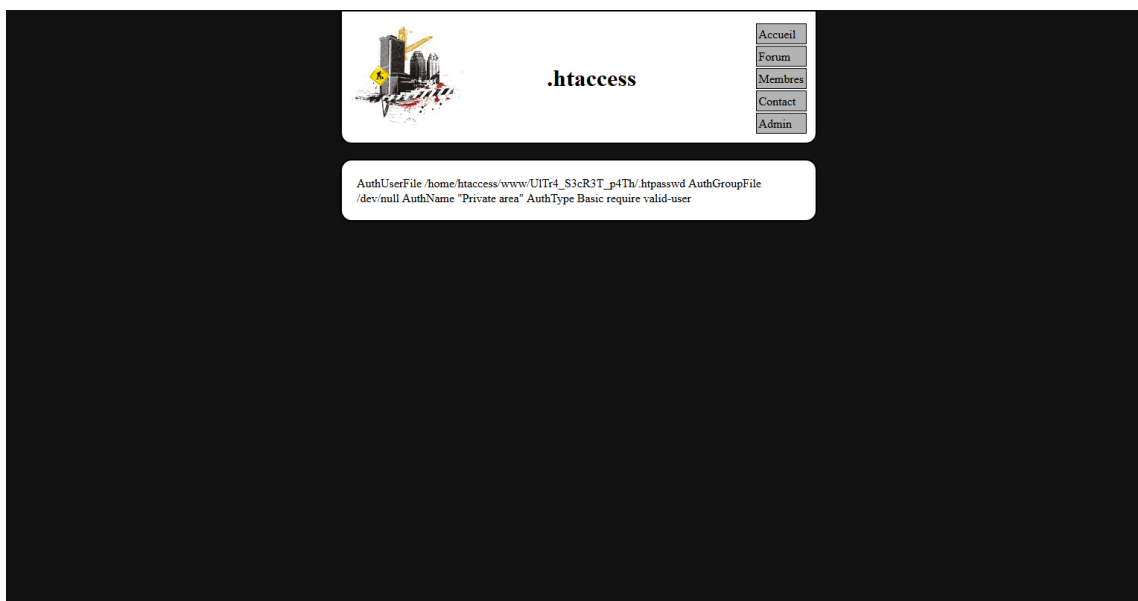
Dans le cas ci-dessus, on utilise \$\_COOKIE, on en retient donc que la page ou la destination vers où pointe \$template a été enregistré sur l'ordinateur de l'utilisateur. Il est donc possible de modifier la requête avant de l'envoyer au serveur.

Imaginons alors que la variable template soit ".././.htaccess", on remonte alors les répertoires jusqu'au root. Si le système de la machine est Linux, il existe alors forcément un répertoire etc/passwd. Maintenant, sur les serveurs en ligne, les développeurs posent généralement ces dossiers dans des répertoires comme admin/.htaccess ou encore pass/.htaccess. Il suffit de faire preuve d'un peu d'imagination pour trouver où pourrait se trouver le fichier.

### 3.3 Exploitation

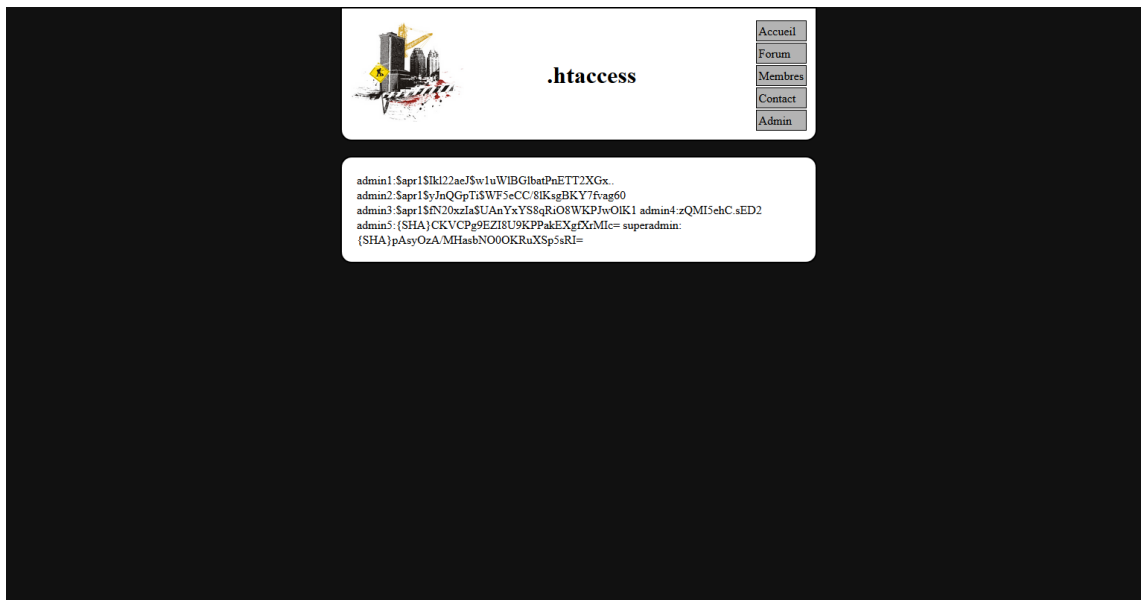
Sur w3chall.com, on trouve une page avec cette faille. La première chose à faire est donc de chercher le fichier .htaccess. En forçant, on trouve que le fichier assez rapidement. Dans la barre d'adresse, il suffit de finir l'adresse par :

```
/ ?page=../admin/.htaccess
```



Bien entendu, avant d'arriver à cela, j'ai tapé plusieurs autres chemins comme ../admin/.htaccess ou encore .htaccess. Une fois ici, on remarque la générosité du système qui nous donne l'emplacement exacte du fichier htpasswd. Il suffit alors de s'y rendre :

```
?page=../UITr4_S3cR3T_p4Th/.htpasswd
```



Et voila qu'apparaissent sous vos yeux les passwords et logins qui se trouvent dans le fichier httpasswd. Ils sont bien entendu crypté mais avec l'utilisation d'un logiciel tiers comme John the Ripper, la reconstitution du password d'origine n'est qu'une question de temps.

### 3.4 Variante

La première correction apportée par les développeurs furent d'ajouter l'extension du fichier à la fin de l'include. Ce qui donnait un lien finissant toujours par .html ou .php. Il devient alors théoriquement impossible de rentrer quelques choses finissant par aucune extension comme nous l'avons fait jusqu'à maintenant. Erreur ! Il est possible de terminer une chaîne à l'endroit où l'on souhaite en ajoutant le caractère de fin de chaîne : le null ou encore %00. Ce qui dans notre cas donnerais :

```
/?page=../admin/.htaccess%00.html
```

Cependant le serveur ne lira cette chaîne que jusqu'au caractère null, le reste sera ignoré.

### 3.5 Solutions

Pour se prémunir d'une telle attaque, pourquoi ne pas simplement escape tout les ../ ou %2e%2e/ (si encodé) lors des navigations.

## 4 SMTP Injection - Injection dans la fonction php mail()

### 4.0.1 Qu'est ce qu'un envoie de message ?

L'envoi de message sur le web se traduit par l'utilisation du protocole SMTP. La communication entre le client et le serveur qui va recueillir le message est la suivante :

```
S : 220 smtp.example.com ESMTP Postfix
C : HELO relay.example.org
S : 250 Hello relay.example.org, I am glad to meet you
C : MAIL FROM :<bob@example.org>
S : 250 Ok
C : RCPT TO :<alice@example.com>
S : 250 Ok
C : RCPT TO :<theboss@example.com>
S : 250 Ok
C : DATA
S : 354 End data with <CR><LF>.<CR><LF>
C : From : "Bob Example" <bob@example.org>
C : To : "Alice Example" <alice@example.com>
C : Cc : theboss@example.com
C : Date : Tue, 15 January 2008 16 :02 :43 -0500
C : Subject : Test message
C :
C : Hello Alice. C : This is a test message with 5 header fields and 4 lines in the message body.
C : Your friend,
C : Bob
C : .
S : 250 Ok : queued as 12345
C : QUIT
S : 221 Bye
The server closes the connection
```

Nous n'allons pas nous intéresser à tous le concept entre le client et le serveur (bien que cela tout aussi intéressant). La partie en bleu est la seule utile pour comprendre la faille. Comme on peut le voir, on retrouve ici toutes les informations composants un email.

### 4.0.2 La fonction mail() de php

Dans PHP, il existe une méthode pour envoyer un mail assez facile à utiliser. Comme on peut le voir ci-dessous, on retrouve la variable pour le destinataire, la variable pour le sujet du mail, la variable pour le corp du message et une variable pour les headers du mail. Cette dernière variable est celle qui nous intéresse le plus et c'est sur cette dernière que je vais agir.

```
mail($destinataire, $sujet, $message, $headers);
```

La variable header permet entre autre de rajouter un élément pour le mail. Dans le code en bleu précédemment, on retrouvait CC par exemple. Ci-dessous, je fais une liste des différents Header que l'on peut utiliser (non-exhaustive) :

- CC (Pour mettre quelqu'un en copie du message)
- BCC (Pour mettre quelqu'un en copie du message de manière invisible)



- FCC (Pour copier le message dans un fichier)
- Reply-To (L'adresse vers où diriger le message si le destinataire répond)

## 4.1 Qu'est ce qu'une injection de header

Lorsque l'on envoie un mail par la fonction `mail()` de php, l'envoi se transformera en ceci lors de la requête :

```
To : $destinataire  
Subject : $sujet  
$headers  
$message
```

Dans cette fonction, de nombreux filtres existent sur les variables `$destinataire`, `$subject` et `$message`. Cependant sur le champs `$header`, il est toujours possible d'agir et il le sera certainement toujours. Maintenant, il faut comprendre maintenant comment ce bout de texte est envoyé au serveur, ce n'est pas aussi beau qu'au dessus. Ces informations sont séparé par des `<LF>` afin que le serveur puissent différencier les différentes champs. Un `<LF>` est un passage à la ligne dont la traduction hexadécimale est `0x0A`. Cette information est très importante. Le but de la faille va être de surcharger le header avec des informations complémentaire pour obtenir par exemple une copie du message. Par exemple, si notre message est le suivant :

```
mail("lala@gmail.com", "Lala", "LalaLALA", "");
```

Cela se traduit par :

```
To : lala@gmail.com  
Subject : Lala  
  
LalaLALA
```

Maintenant, si l'on change le header par quelques choses comme ceci : `%0ABCC :lolo@gmail.com`

```
To : lala@gmail.com  
Subject : Lala  
  
BCC :lolo@gmail.com  
LalaLALA
```

On se retrouve alors à injecter un header qui n'était pas prévu à la base !

## 4.2 Exemple

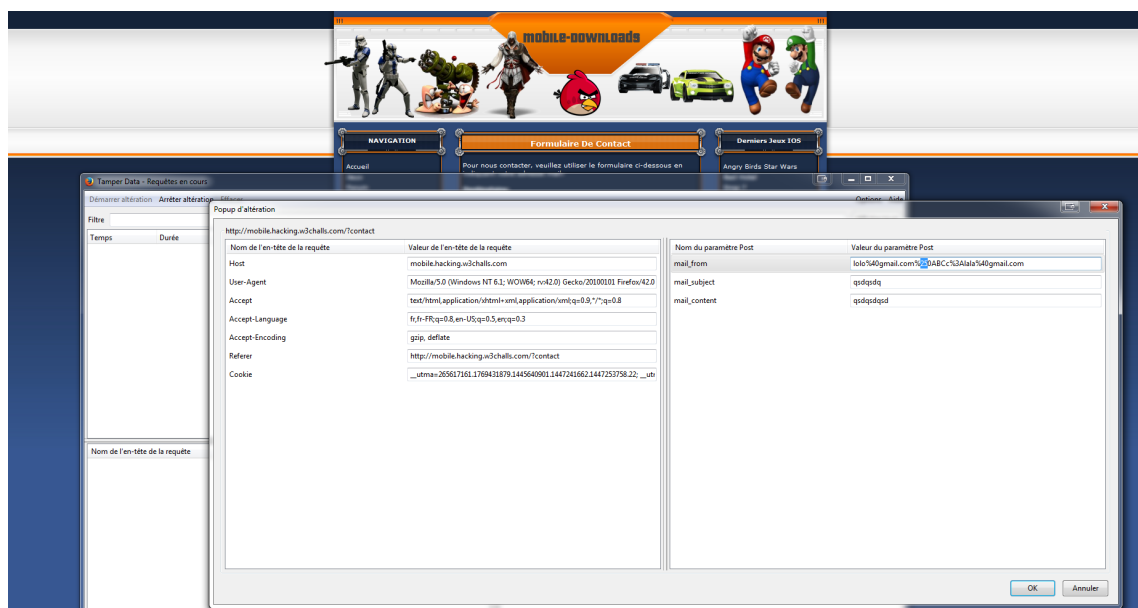
Pour expliquer la faille, je vais me servir du site de w3Challs. Sur ce dernier, il y a une page pour tester ce type d'injection. Pour commencer, il faut chercher un champ d'un formulaire qui pourrait utiliser cette fonction.



On trouve alors un très beau (et surtout moche) formulaire pour envoyer des messages aux créateurs du site. On remarque que le premier champ est très susceptible d'avoir une faille. On tente donc une injection de header. Je vais dans un premier temps créer ma petite injection dans le champ adresse mail en écrivant ceci : lala@gmail%0ABCC :lolo@gmail.com



En utilisant ensuite Tamper Data afin d'altérer la requête POST, on peut prévenir notre requête d'être encodé en format URL. Car dans notre cas, le symbole % est automatiquement transformé par Firefox en %25, ce qui n'est pas ce que l'on veut.



Enfin, on envoie la requête et pouvons maintenant consulter sur notre adresse un double du mail que l'admin a reçu :p Avec cette méthode, il est possible de spammer des personnes, de se faire passer pour certaines personnes...

### 4.3 Solutions

Pour se protéger contre ce type d'attaque, il suffit de vérifier que les informations entré par l'utilisateur ne contiennent pas les symboles `\n` ou `\r`. Par exemple, le bout de code suivant réalise cette opération :

```
if(ereg("\r",$from) or ereg("\n",$from)) {
    die("Why ?? :(");
}
```

## 5 Attaque temporel - Attaque par Canaux cachés

### 5.1 Qu'est ce qu'un canal caché ?

## 6 CSRF - Cross-site request forgery

### 6.1 Qu'est ce qu'une attaque CRSF ?

Pour expliquer cela, il est beaucoup plus intéressant de prendre un exemple. Imaginons la scène suivante :

- Une personne s'enregistre à sa banque normalement
- La banque donne un cookie a cette personne qui permet de définir session (Set-Cookie : SESSIONID=a804696f-93fc-48cf-9b02-267d9ed773c0)
- Puis sur d'autre onglet, cette personne navigue sur d'autres sites
- Et tombe sur un site, avec un code malicieux :

```
<form name="attack" enctype="text/plain" action="https://bank.example.com/api/transfer" METHOD="POST">  
<input type="hidden" name="'from" : "Savings", "to" : "00302319550440", "amount" : "100.00"'>  
</form>  
<script>document.attack.submit();</script>
```

- Lorsque l'utilisateur arrive sur la page, son navigateur lit la page et va exécuter le code. Ce qui va résulter à un transfert de 100 euros à un certain compte bancaire
- Comme l'utilisateur a un cookie avec une session valide, la requête émis via le formulaire va être accepté par le site de la banque

## 7 XSS

### 7.1 Simple XSS - balise script

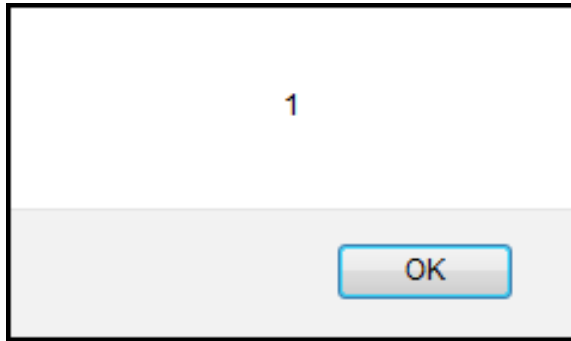
Prenons le script suivant sans aucune protection :

```
<?php
if(isset($_POST['XSS']))|
    echo $_POST['XSS'];
?>
<form action="" method="POST">
    XSS: <br><input type="text" input name="XSS"></br>
    <input type="submit">
</form>
```

Ici la moindre attaque XSS est possible, il est possible d'écrire directement du code dans les balises scripts. Par exemple, `<script>alert(1)</script>` :

XSS:

On obtient alors le résultat suivant qui nous montre qu'une faille XSS est possible ici :



### 7.2 XSS Trick - Bypass htmlspecialchars in some cases

Dans certains cas, la fonction htmlspecialchars est inutile comme on peut le voir ci-dessous :

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>Insert title here</title>
</head>
<body>
    <?php if(isset($_POST['XSS'])) { ?>
    <svg><script>var XSS = "<?php echo htmlspecialchars($_POST['XSS']); ?>"</script></svg>
    <?php } ?>
    <form action="" method="POST">
        XSS: <input type="text" name="XSS"><br />
        <input type="submit">
    </form>
</body>
</html>
```

On peut alors faire notre injection de la manière suivante : `xss";prompt(/XSS/);//`

XSS:

On obtient alors le résultat suivant qui nous montre qu'une faille XSS est possible ici :



### 7.3 XSS Trick avec les guillemets simples - Bypass htmlspecialchars et htmlentities

Si on se réfère à la documentation de PHP, par défaut sur la fonction htmlentities et/ou htmlspecialchars le flag ENT\_COMPAT est utilisé dans la fonction. Ce flag signifie que la fonction convertit les guillemets doubles et ignore les guillemets simples. Autrement dit, si le codeur en question a écrit une fonction comme :

```
echo '<a href="'.htmlspecialchars($_POST['XSS']).'">Test</a><br />';
```

Si on regarde attentivement, une injection XSS est donc ici possible avec par exemple la saisie suivante :

```
XSS' autofocus onfocus='alert(1)
```

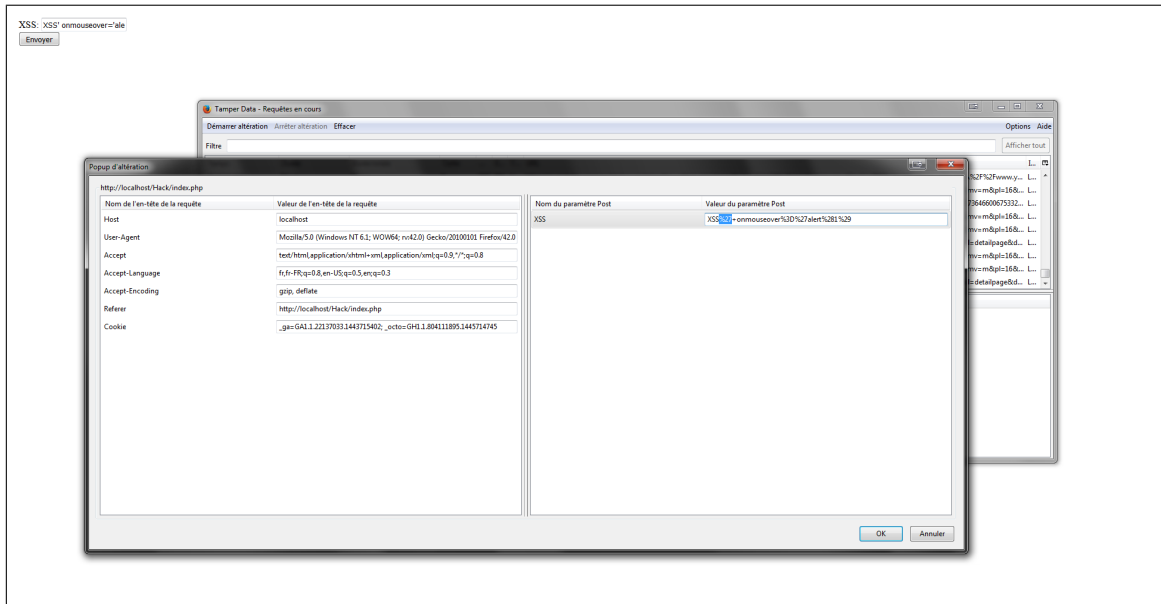
L'autofocus permet de mettre automatiquement le focus sur le lien dès le chargement de la page tandis que le onfocus sera la fonction appelé dès que le lien aura le focus. Autrement dit, la fonction à l'intérieur du onfocus sera automatiquement chargé au chargement de la page sur le PC du client.

Effectuons un petit test avec onmouseover pour voir le résultat cela dans un navigateur récent :

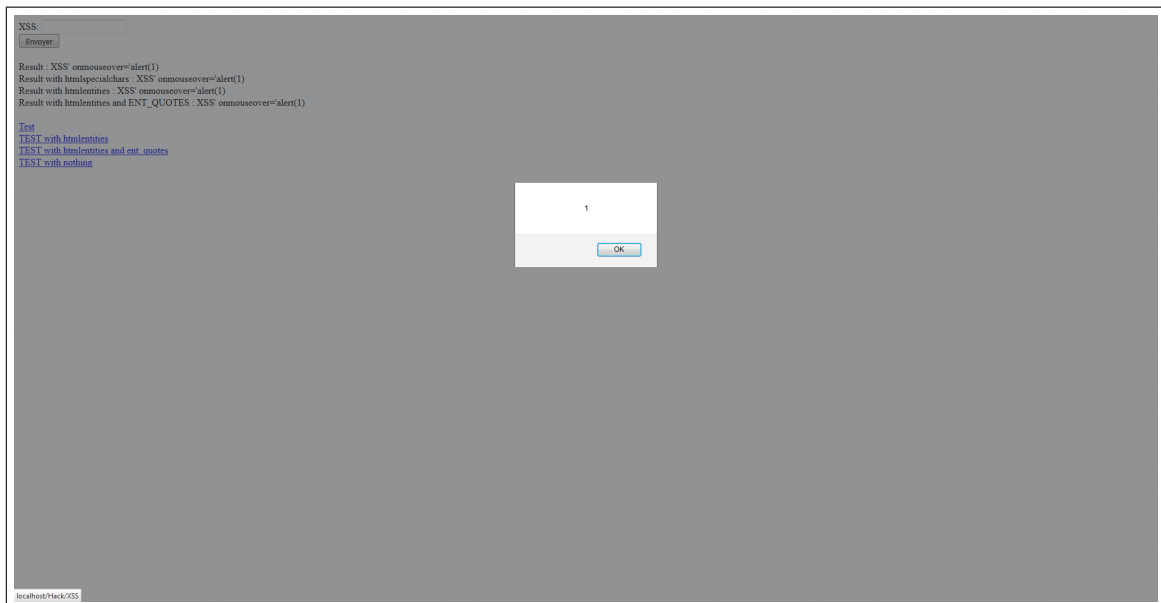
```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <meta charset="utf-8">
5 <title>Insert title here</title>
6 </head>
7 <body>
8 <form action="" method="POST">
9   XSS: <input type="text" name="XSS"><br />
10  <input type="submit">
11 </form>
12 <br />
13 <?php if(isset($_POST['XSS'])) { ?>
14   Result : <?php echo $_POST['XSS']; ?><br />
15   Result with htmlspecialchars : <?php echo htmlspecialchars($_POST['XSS']); ?><br />
16   Result with htmlentities : <?php echo htmlentities($_POST['XSS']); ?><br />
17   Result with htmlentities and ENT_QUOTES : <?php echo htmlentities($_POST['XSS'], ENT_QUOTES); ?><br /><br />
18   |
19   <?php
20     echo "<a href='".htmlspecialchars($_POST['XSS'])."'>Test</a><br />";
21     echo "<a href='".htmlentities($_POST['XSS'])."'>TEST with htmlentities</a><br />";
22     echo "<a href='".htmlspecialchars($_POST['XSS'], ENT_QUOTES)."'>TEST with htmlentities and ent_quotes</a><br />";
23     echo "<a href='".$_POST['XSS']."'>TEST with nothing</a><br />";
24   ?>
25 <?php } ?>
26 </body>
27 </html>
```

Je vais aussi utilisé Data Temper, un plugin de firefox, pour altérer ma requête POST afin de

bypasser l'encodage du navigateur.



On obtient alors le résultat suivant :





## 8 Bibliographie

### 8.1 SMTP Injection

— <http://www.phpsecure.info/v2/article/MailHeadersInject.php>