FAILLE XSS

C'est la faille de sécurité la plus exploité par les pirates.

Principe de base :

Une faille XSS consiste à injecter du code directement interprétable par le navigateur Web, comme, par exemple, du JavaScript ou du HTML. Cette attaque ne vise pas directement le site comme le ferait une injection SQL mais concerne plutôt la partie client c'est-à-dire vous (ou plutôt votre navigateur). Ce dernier ne fera aucune différence entre le code du site et celui injecté par le pirate, il va donc l'exécuter sans broncher. Les possibilités sont nombreuses : redirection vers un autre site, vol de cookies, modification du code HTML de la page, exécution d'exploits contre le navigateur : en bref, tout ce que ces langages de script vous permettent de faire.

Pour se protéger des XSS il faut remplacer les caractères qui pourraient éventuellement être compris par le navigateur comme des balises par leur entité HTML.

En faisant cela, le navigateur affichera textuellement le caractère et ne cherchera plus à l'interpréter.

`<h1>test</h1>` donnera donc le message `<h1>test</h1>` et non plus le mot « test » en tant que titre.

En PHP, vous pouvez utiliser les fonctions htmlentities ou htmlspecialchar

```
<!DOCTYPE html>
<html lang="fr">
    <head>
      <meta charset="utf-8" />
    </head>
    <body>
        <h1>Mon super moteur de recherche</h1>

        <?php
        if(!empty($_GET['keyword']))
        {
            echo "Résultat(s) pour le mot-clé : ".htmlspecialchars($_GET['keyword'], ENT_QUOTES);
        }
        ?>

        <form type="get" action="">
            <input type="text" name="keyword" />
            <input type="submit" value="Rechercher" />
```

```
        </form>
    </body>
</html>
```