En quoi consiste une faille xss ?

Définition
L'attaque XSS (pour Cross Site Scripting) est une attaque très populaire presque au même titre que l'injection SQL. Elle est également présente dans le podium (à dix marches) d'OWASP en 2017.

L'attaque XSS vise comme cible le client plutôt que le serveur. Elle se sert d'un script Javascript qui sera exécuté chez le client pour détourner le fonctionnement de son navigateur. En effet, le pirate développe un script Javascript selon ses attentions, il soumet ensuite ce script comme étant une chaine de caractères à un serveur via une de ses entrées (formulaire, URL...). Si le serveur présente une vulnérabilité vis-à-vis du XSS, alors le script sera accepté et probablement déposé dans la base de données (ou autre forme de source de données). Jusqu'ici il ne se passe rien de spécial. Mais imaginez qu'à un certain moment un client se connecte sur le serveur et demande une page qui affiche les entrées de la base de données, et par hasard c'est le contenu Javascript qui sera envoyé au navigateur. Puisque Javascript est un langage coté client, alors il sera aussitôt exécuté sur le navigateur du client et fera ce qui a été demandé par le pirate.

Dans ce cas de figure, n'importe quel client peut être victime de cette attaque. Tout dépend de qui a demandé l'affichage du contenu de la base de données qui coïncide avec le script. Par contre, si le pirate veut viser un client en particulier alors il peut lui envoyer un message privée encapsulant une attaque XSS via un site Web (présentant la vulnérabilité) comme un forum de discussion ou autre.

Une attaque XSS peut également provoquer des dommages parfois conséquents comme par exemple:
Rediriger un utilisateur à son insu vers un site pirate ou site compromettant
Afficher des messages indésirables sur le navigateurs du client
Empêcher l'exécution normale des scripts embarqués dans la page
Ordonner le déclenchement de périphériques sur l'ordinateur de la victime comme la Webcam

Comment détourner une faille xss ?

Pour vous protéger des XSS, vous devez remplacer les caractères pouvant être compris par le navigateur comme des balises par leur entité HTML. En procédant ainsi, le navigateur affichera mot à mot le caractère et ne cherchera plus à l'interpréter. En PHP, vous pouvez utiliser les fonctions htmlentities ou htmlspecialchar.

Détection d'une faille xss ?

La détection de la faille se fait simplement en essayant d'injecter des donnée arbitraire dans un site web, par le remplissage d'un formulaire, ou en modifiant les paramètres d'URL. Si ces données sont transmise sans avoir été vérifiées par le serveur, alors il existe une potentiel faille : on peut s'en servir pour faire exécuter du code malveillant en JavaScript par le navigateur web d'un utilisateur cible.

Il existe trois formes basiques de vulnérabilités XSS:

Le reflected XSS (XSS refléchi) : C'est la vulnérabilité la plus connue. Pour faire simple, en suivant une url piégée l'utilisateur arrivera sur une page dont le hacker contrôle le contenu. Si celui-ci a modifié des fonctionnalités de la page il pourra alors récupérer les données partagées par le visiteur (identifiant de connexion et mot de passe pa r exemple).

Le stored XSS (XSS stocké) : Le XSS stocké est une saisie (input) utilisateur stockée dans l'application. Si les finali tés
d'attaques sont les mêmes que pour le XXS réfléchi, le stored XSS distribue l'attaque beaucoup plus largement. Cett

e faille
est donc critique sur les sites à fort trafic.

Le DOM XSS : C'est la modification du DOM ("Document Object Model", la représentation d'une site web dans un navigateur) qui permet aux
hackers de récupérer les données des utilisateurs. De plus, les attaques DOM n’ayant pas besoin de passer par le serv eur web, elles
rendent les moyens de défense traditionnels, comme les pare-feux, inutiles.

Les pratiques a prendre pour éviter une injection xss ?

Vous pouvez contrer cette attaque en utilisant des caractères spéciaux HTML & ENT_QUOTES dans vos codes d'ap plication.
En utilisant ENT_QUOTES, vous pouvez supprimer les options de guillemets simples et doubles, ce qui vous perme t d'éliminer
toute possibilité d'attaque de script intersite.

Ou se mettre a jour ?

Undernews.fr (https://www.undernews.fr/)