- En 2011, le PlayStation Network (PSN) de Sony a subi une violation de données massive qui a entraîné le vol des informations personnelles de millions de clients

- En 2018, Marriott International a révélé qu'elle avait été victime d'une violation de données qui a exposé les informations personnelles de près de 500 millions de clients

- En décembre 2020, SolarWinds a subi une injection sql qui a compromis SolarWinds orion un logiciel de surveillance et de gestion des réseaux largement utilisé par les entreprises et les agences gouvernementales

Les failles de sécurité

Sommaire

- Cross-Site Scripting (XSS)
- Injection sql
- Cross-Site Request Forgery (CSRF)
- Inclusion de fichier
- Guide de survie sur internet

Les attaques xss

Les attaques xss machin truc c’est quoi ?

- Envoi de code malveillant (ex: javascript) en passant par les formulaires
- Survient lorsque les information envoyer par l’utilisateur ne sont pas contrôlé
- Permet à l’attaquant de dérober les données d’autres utilisateurs

Exemple d’attaques

- Xss stocké :

  Envoi de code malveillant en base de données

- Xss réfléchi :

  Envoi d’un lien malveillant qui sera exécuté par le navigateur de la victime

Objectif : Voler les données de la victime comme par exemple les cookies de session

Bonne pratiques

- NE JAMAIS FAIRE CONFIANCE À L'UTILISATEUR !

  - Vérifier les données envoyer, coté client et surtout coté serveur en utilisant par exemple un strip_tag() en php.

  -S'assurer que les données respectent bien le format attendu

Les injections sql

Les injection sql machin truc c’est quoi ?

- Langage de base de données

- Survient lorsque que l'attaquant envoi du code sql en passant par nos formulaires `SELECT nom_du_champ FROM nom_du_tableau WHERE nom = :nom`

- Permet de manipuler la base de données || Effectuer des actions non autorisés

Exemple

- SELECT * FROM utilisateurs WHERE nom_utilisateur='$nom_utilisateur' AND mot_de_passe='$mot_de_passe'

- Si l’utilisateur ajoute' OR '1'='1 à la requète ça lui permettra de se connecter sans utiliser de mot de passe

Bonne pratiques

- NE JAMAIS FAIRE CONFIANCE À L'UTILISATEUR !

  - Vérifier les données envoyer

  - S'assurer que les données respectent bien le format attendu

  - Faire des requêtes préparées

    query("SELECT * FROM utilisateurs WHERE nom_utilisateur='$nom_utilisateur' AND mot_de_passe='$mot_de_passe'")

  Devient

    prepare("SELECT * FROM utilisateurs WHERE nom_utilisateur='?' AND mot_de_passe='?'")

Les attaque CSRF

Les injection CSRF machin truc c’est quoi ?

- Egalement connu sous le nom d'attaque "sea surf" ou "session riding"

- Attaque qui exploite la confiance accordée par un site à un utilisateur authentifié pour exécuter des actions non autorisées

- Dans une attaque CSRF, un attaquant force un utilisateur authentifié à exécuter des actions sur un site web sans son consentement

Comment ça marche ?

- L’attaquant crée un lien qui correspond au site ou la victime est connecté
  - Lien contenant une image comme celle ci :

```
<img src="https://www.sitecible.com/changepassword?newpassword=123456" style="display:none">
```

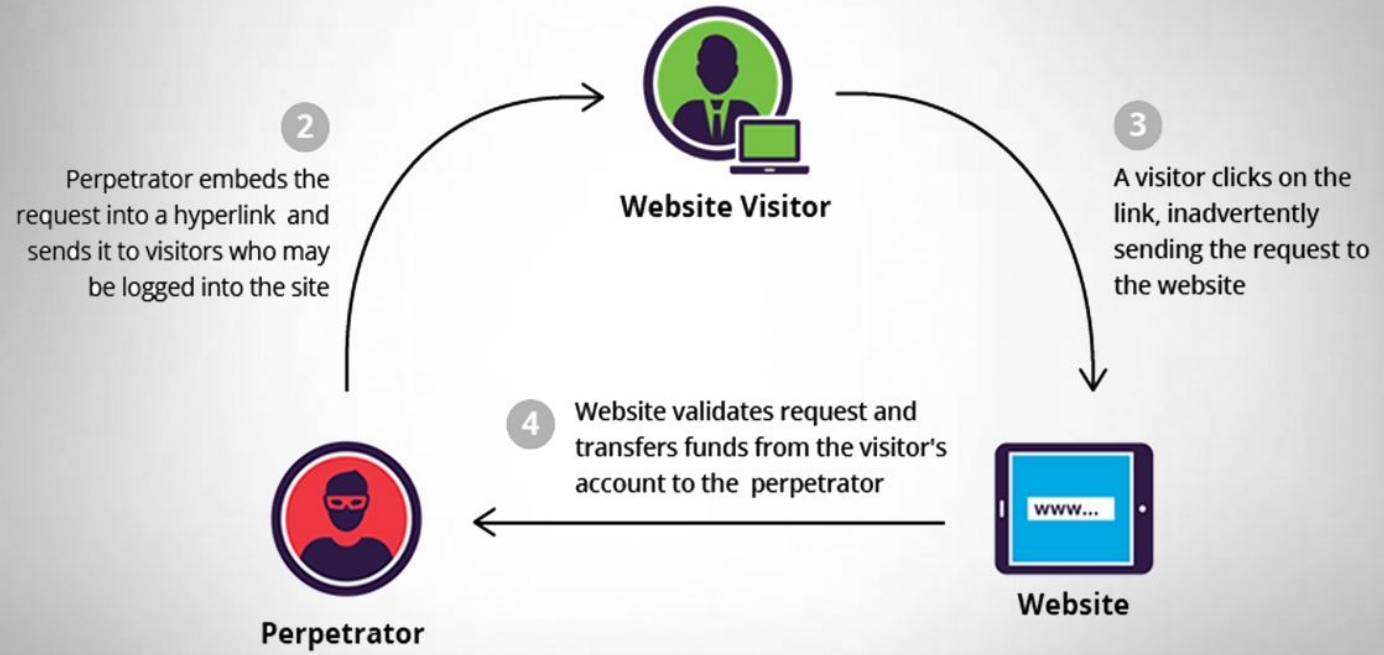
- L’attaquant envoi le lien à la victime

- Le lien envoi une requête au site

- Le site valide la requête et envoi les données à l’attaquant sans que la victime ne soit au courant

CSRF Attacks

(Cross Site Request Forgery)



Comment ont lutte ?

- Token anti csrf synchronisé :
  - On génère des token aléatoire, unique à chaques sessions pour ensuite vérifier l'authenticité du token à chaque requêtes.

L’inclusion de fichier

C’est quoi ?

- RFI (Inclusion de fichier arbitraire)

  - Quand on permet à l’utilisateur d’envoyer un fichier sur le site, l’utilisateur en profite donc pour envoyer un fichier malveillant

- LFI (inclusion de fichier locaux)

  - Permet à l’utilisateur d'accéder à des fichier contenant des information sur l’application

Comment ça marche ?

- RFI

  - L’attaquant fournit un lien qui redirige vers le fichier malveillant qu’il a implémenter dans l’application qui lui permet d'exécuter ensuite du code malveillant sur le serveur.

- LFI
  - L’attaquant exploite les données récoltées

Exemple : Les données d'authentification à la base de données

Comment ont lutte ?

- Limiter l’accès au répertoire contenant le fichier envoyé

- Vérifier le mime type Mime des fichiers envoyés
  - Attention le nom ne correspond pas au type de l’image

    Exemple : uneVrailmage.exe.jpeg n’est pas une image

Guide de survie

- Ne pas cliquez sur les liens qu’on ne connaît pas (même par curiosité)
- Ne pas télécharger des logiciel qu’on ne connaît pas
- Ne pas brancher de clé usb qui ne nous appartient pas
- Ne pas scanner n’importe quel qr code
- Utiliser un vrai mot de passe (Bernard1995 n’est pas un mot de passe)
- Ne faites confiance en personne

0,50€ la question