Cross-Site Request Forgery (CSRF)

Utiliser les droits d'un utilisateur pour lui nuire

Accès simultané à deux sites différent Cas normal Session Site A Aucune interaction Site B Compromission du site B Session Site A Sous attaque Si accès à B durant connexion authentifiée à A, surf sur les droits de A Site B Forged request Commande vers site A Credentials sent automatically by browser 19

En pratique...

Cross-Site Request Forgery (CSRF)

Exemple : requête de transaction bancaire vulnérable Requête normale

http://example.com/app/transferFunds?amount=1500 &destinationAccount=4673243243

Requête du pirate sur un site infecté

<img src="http://example.com/app/transferFunds?
amount=1500&destinationAccount=attackersAcct#"
width="0" height="0" />

L'élément n'a pas besoin d'être visible!

Le pirate ne récupère pas les informations de l'utilisateur!

Cross-Site Request Forgery (CSRF)

| Cible | Risques | Conséquences |
|---|---|---|
| Utilisateur final, client du site d'origine | Exécution de commandes en exploitant les droits d'un utilisateur légitime | Usurpation d'identité Destruction de données Violation de confidentialité |

Défenses contre le CSRF

CSRF

Site A: authentification unique à l'instant T

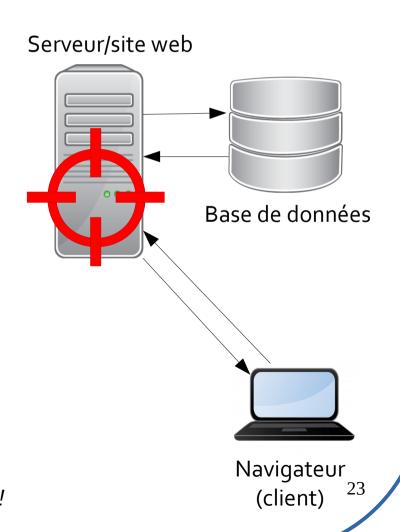
Navigateur : possibilité de surfer sur plusieurs pages à la fois

Pirate : connaissance de la structure des URL utilisées sur le site

- Authentifications répétées et ergonomie
- Vérification du chemin suivi vers la page demandée
 - Champ HTTP_REFERER de l'en-tête
 - Page de provenance
 - Inclusion d'un jeton aléatoire dans la page ou dans l'URL
 - ✓ Caché dans un champ invisible
 - ✓ Dans l'URI ...

Dépôt de fichier malicieux

- Propagation / impact
 - Serveur => autres nœuds du réseau
 - Serveur => base de données
 - Serveur => utilisateurs
- Pistes de protection
 - *Upload* vraiment indispensable ??
 - *Upload* si authentification
 - Liste blanche des extensions de fichier autorisées
 - Contrôle du nom de fichier par regex
 - Caractères interdits : «/», «\», «..», «\$»...
 - Dépôt dans un répertoire « non-executable »
 - Limitation de la taille de fichier (space DOS)
 - Scan des fichiers (antivirus)
 - Recommandations propres aux outils utilisés



Practice time!