2013/2014

M2-Informatique SSI

GULDNER Geoffrey
HURIER Médéric
LACAVE Valentin
SOIHILI Mouchtali

[Rapport d'Attaque n°A010]

SOMMAIRE

I. Description de l'attaque

Groupe ciblé
Pour le groupe ciblé on a : le groupe 3
Adresse(s) IP cible : 172.24.141.211
Propriétaires du serveur (les 4 noms)

- HEYD
- CONTAL
- GORLT
- KONE

Nom de l'attaque
Attaque par Injection SQL

Date de l'attaque
21/03/2014

Catégorie d'attaque
Injection SQL

Technique utilisée
Première étape : recherche de champs vulnérables à l'injection sql (on met ' dans un champ et on regarde)
Deuxième étape : une fois un champ trouvé on essaye différentes injections (ici la mienne est très basique : '#).

CID
La confidentialité est touchée.

II. Résultat de l'attaque

Description du résultat

Sur la page d'accueil du site, il y a un champ de recherche concernant les articles. Le fonctionnement normal est celui-ci : on cherche un mot clé et il nous affiche tous les articles (les dernières versions !) en rapport avec ce mot clé. Avec l'injection, il est possible de faire afficher tous les articles avec toutes leurs versions, ce qui ne se produit pas en temps normal.

Malheureusement, pour remettre le site en marche, clément a du restaurer une machine virtuelle qui ne contenait aucun article. De plus, il m'est impossible de me connecter sur leur application pour en créer car mon compte n'existe plus, il m'est aussi impossible d'en recréer un car leur formulaire d'inscription ne fonctionne plus (le captcha ne peut pas se connecter au serveur des captcha et renvoie une erreur : depuis quelques jour le réseau de la fac a été modifié, les mails ne passent plus avec Thunderbird, certains services sont bloqués dont les captcha (notre serveur souffre aussi de ce problème.))

Preuve de l'attaque

Information récupérée et/ou modifiées

Versions non visible des articles

Comment s'en protéger?

Filtrer les caractères spéciaux coté serveur