

2013/2014

M2-Informatique SSI

GULDNER Geoffrey

HURIER Médéric

LACAVE Valentin

SOIHILI Mouchtali



[Rapport d'Attaque n°A011]

SOMMAIRE

I. DESCRIPTION DE L'ATTAQUE.....	3
II. RESULTAT DE L'ATTAQUE.....	4

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

Exploitation de la faille

Date de l'attaque

27/03/2014

Catégorie d'attaque

Remplissage bd

Technique utilisée

« Afin d'accéder à cette page, il suffit à l'utilisateur de cliquer sur le bouton "Sauvegarder".

S'affiche alors un message de confirmation ainsi qu'un "loader" signifiant à l'utilisateur qu'il va être redirigé. Il lui suffit d'appuyer sur F5 afin de découvrir la faille : la page se rafraîchit et apparaît de nouveau le message de confirmation : une nouvelle occurrence est alors créée ! ».

Plugging Firefox IMACROS qui permet d'enregistrer une suite de commande comme un magnétoscope qui enregistre puis après on lance la macro qui le fera plusieurs fois automatiquement.

CID

L'intégrité.

II. Résultat de l'attaque

Description du résultat

Des articles on était créé à la suite mais cela a toujours était le meme a l'identique.

Preuve de l'attaque

Aucune preuve n'est disponible car leur serveur bug énormément et malgré les tentatives de reparations de Gorlt et Charlie rien n'as pu être fait. Gorlt me la fait testé sur le serveur de teste.

Information récupérée et/ou modifiées

Aucune

Comment s'en protéger?

?