

## ***TP1 INFO 714***

# ***FAILLE SQL INJECTION, PLUGIN WORDPRESS ALLVIDEOGALLERY***

### ***TABLE DES MATIÈRES***

I ) Présentation du plugin.....	1
II ) Vulnérabilité du plugin.....	2
1 - Le code vulnérable.....	2
2 - Attaques réalisées.....	2
3 - Attaque sur un site tiers :.....	5
III ) Aller plus loin.....	9
1 - Que faire du mot de passe crypté récupéré ?.....	9
2 - Le système de sécurité de Wordpresse.....	9

## I) PRÉSENTATION DU PLUGIN

All Video Gallery est un plugin wordpress permettant de créer des galeries de vidéos. Il est actuellement disponible en version 1.2.

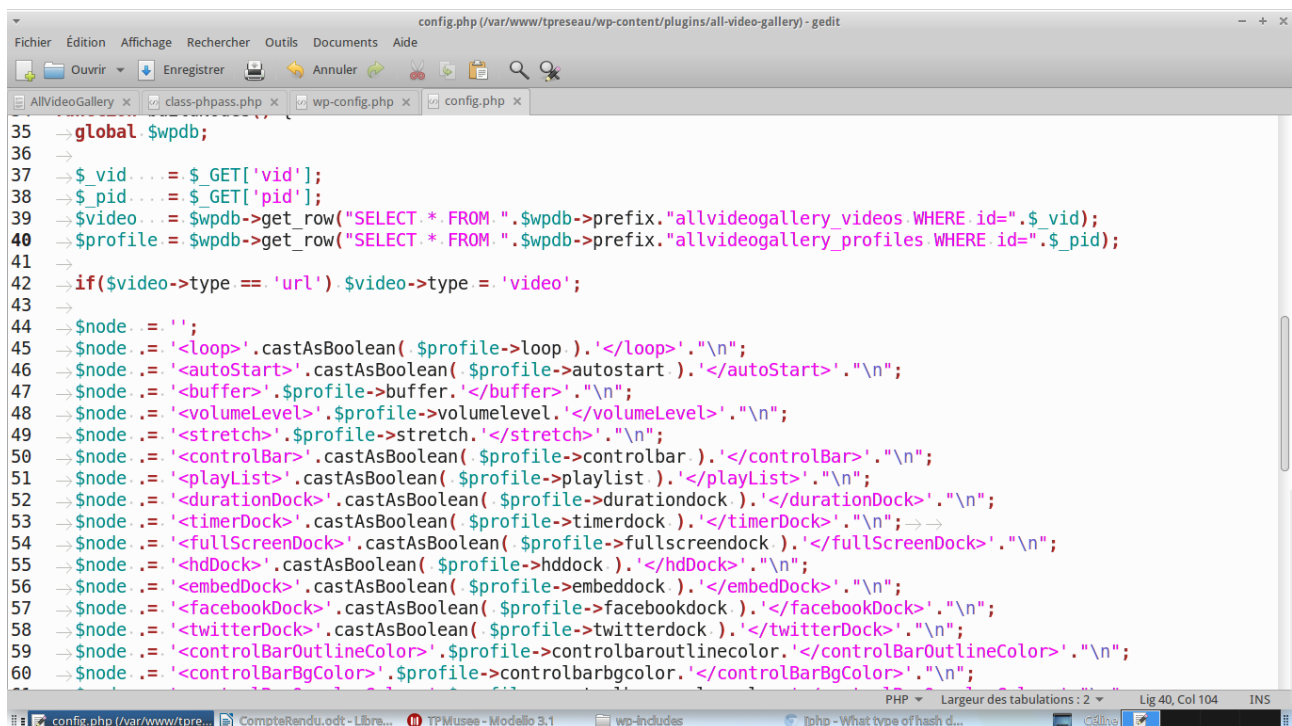
La version 1.1 présente une vulnérabilité à l'injection SQL, qui a été corrigée dans la version 1.2.

## II) VULNÉRABILITÉ DU PLUGIN

### 1 - Le code vulnérable

Dans le fichier config.php, qui rend un fichier xml donnant la configuration d'une vidéo et d'une galerie (répétition, dimensions etc), il y a un paramètre GET récupéré sans protection et utilisé dans une requête.

Code vulnérable dans le fichier wp-includes/plugins/all-video-gallery/config.php



```
35 → global $wpdb;
36 →
37 → $_vid = $_GET['vid'];
38 → $_pid = $_GET['pid'];
39 → $video = $wpdb->get_row("SELECT *. FROM ". $wpdb->prefix."allvideogallery_videos.WHERE id=".$_vid);
40 → $profile = $wpdb->get_row("SELECT *. FROM ". $wpdb->prefix."allvideogallery_profiles.WHERE id=".$_pid);
41 →
42 → if($video->type == 'url') $video->type = 'video';
43 →
44 → $node = '';
45 → $node .= '<loop>'.castAsBoolean( $profile->loop ).'</loop>'. "\n";
46 → $node .= '<autoStart>'.castAsBoolean( $profile->autostart ).'</autoStart>'. "\n";
47 → $node .= '<buffer>'. $profile->buffer . '</buffer>'. "\n";
48 → $node .= '<volumeLevel>'. $profile->volumeLevel . '</volumeLevel>'. "\n";
49 → $node .= '<stretch>'. $profile->stretch . '</stretch>'. "\n";
50 → $node .= '<controlBar>'.castAsBoolean( $profile->controlbar ).'</controlBar>'. "\n";
51 → $node .= '<playlist>'.castAsBoolean( $profile->playlist ).'</playlist>'. "\n";
52 → $node .= '<durationDock>'.castAsBoolean( $profile->durationdock ).'</durationDock>'. "\n";
53 → $node .= '<timerDock>'.castAsBoolean( $profile->timerdock ).'</timerDock>'. "\n";
54 → $node .= '<fullScreenDock>'.castAsBoolean( $profile->fullscreendock ).'</fullScreenDock>'. "\n";
55 → $node .= '<hdDock>'.castAsBoolean( $profile->hddock ).'</hdDock>'. "\n";
56 → $node .= '<embedDock>'.castAsBoolean( $profile->embeddock ).'</embedDock>'. "\n";
57 → $node .= '<facebookDock>'.castAsBoolean( $profile->facebookdock ).'</facebookDock>'. "\n";
58 → $node .= '<twitterDock>'.castAsBoolean( $profile->twitterdock ).'</twitterDock>'. "\n";
59 → $node .= '<controlBarOutlineColor>'. $profile->controlbaroutlinecolor . '</controlBarOutlineColor>'. "\n";
60 → $node .= '<controlBarBgColor>'. $profile->controlbarbgcolor . '</controlBarBgColor>'. "\n";
```

### 2 - Attaques réalisées

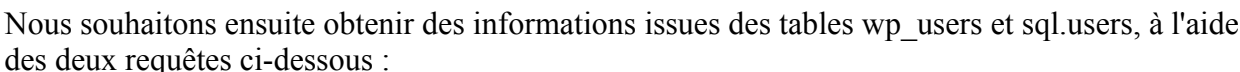
Nous avons donc essayé de placer une union dans cette requête de la façon suivante :

[http://tpreseau.localhost/wp-content/plugins/all-video-gallery/config.php?vid=1&pid=11+UNION+SELECT+version\(\),version\(\),version\(\),version\(\),version\(\),version\(\),version\(\),version\(\),...](http://tpreseau.localhost/wp-content/plugins/all-video-gallery/config.php?vid=1&pid=11+UNION+SELECT+version(),version(),version(),version(),version(),version(),version(),version(),...)

Explication :

- get\_row ne récupère qu'une seule ligne. Nous indiquons donc un pid inexistant afin que ce soit le résultat de la requête UNION SELECT qui arrive en première ligne.

- En observant le résultat, nous voyons également qu'une partie des réponses sont converties en booléens, nous laisserons donc des champs `version()` ou autres champs inutiles à ces emplacements.

[illegible]



### 3 - Attaque sur un site tiers :

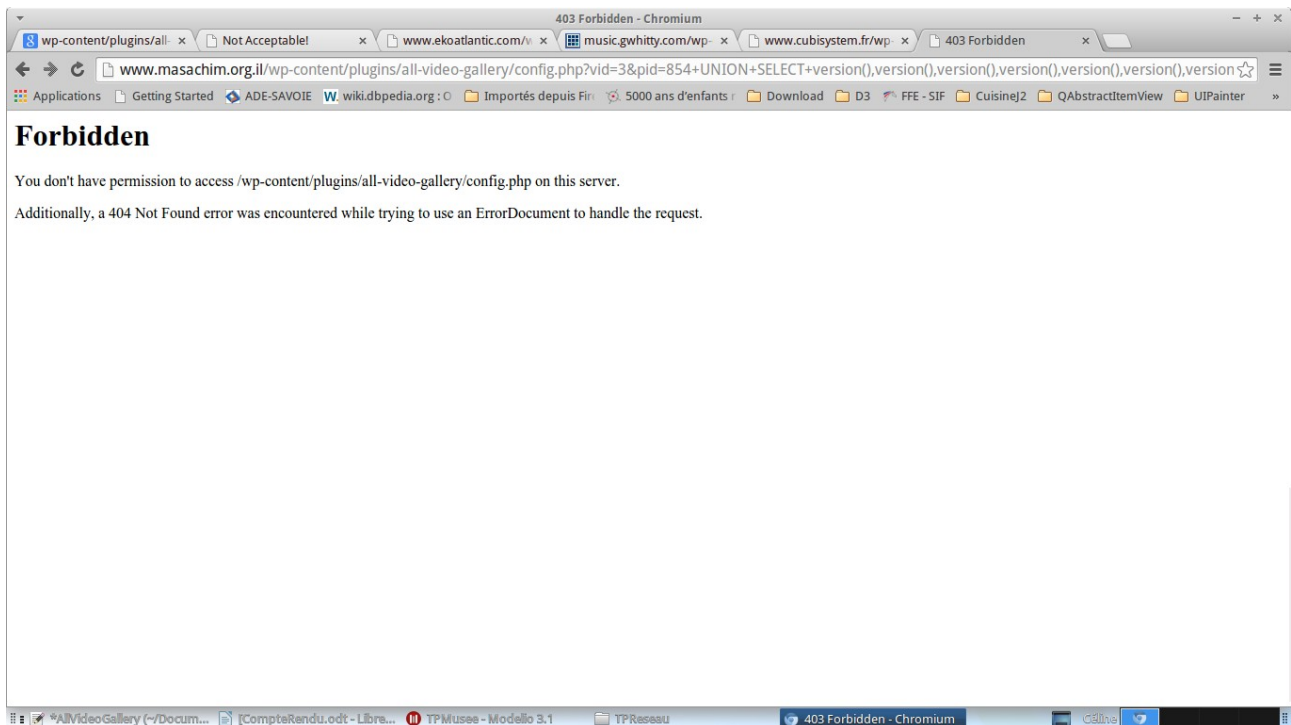
Nous avons effectué sur google la recherche « wp-content/plugins/all-video-gallery/config.php? » et tenté une injection sur les résultats de cette recherche. Nous pouvons déjà dire que les sites qui ont configuré correctement leur fichier robot.txt ont beaucoup moins de risques d'être attaqués par nous, même si ils sont vulnérables.

1. Le site utilise un module de sécurité supplémentaire qui a bloqué notre requête :

A screenshot of a Chromium web browser window. The address bar shows the URL: www.juangrial.com/wp-content/plugins/all-video-gallery/config.php?vid=1&amp;pid=854+UNION+SELECT+version(),version(),version(),version(),version(),version(),version(). The page title is "Not Acceptable! - Chromium". The main content area displays a large red "Not Acceptable!" heading, followed by the message: "An appropriate representation of the requested resource could not be found on this server. This error was generated by Mod\_Security." The browser's tab bar at the top shows several open tabs, including "wp-content/plugins/all...", "Not Acceptable!", "www.ekoatlantic.com/v...", "music.gwhitty.com/wp...", "www.cubisystem.fr/wp...", and "403 Forbidden". The taskbar at the bottom shows various application icons, including "AllVideoGallery (~/Docum...", "CompteRendu.odt - Libre...", "TPMuseum - Modello S.1", "TPReseau", and another instance of "Not Acceptable! - Chromium".

[illegible]

[rsion\(\),version\(\),version\(\),version\(\),version\(\),version\(\),version\(\),version\(\),version\(\),version\(\),versio](#)  
[n\(\),version\(\),version\(\),version\(\)](#)



3. Le site utilise la dernière version du plugin ou a modifié lui même le code vulnérable : le paramètre pid est converti en integer, aucun résultat n'est trouvé :

[illegible]





Nous voyons que notre attaque fonctionne sur ce site, nous essayons d'aller plus loin pour obtenir ses identifiants et empreintes de mot de passe.

[illegible]

Plus prudent que nous, il utilise un utilisateur différent de root, il y a donc peu de chances qu'on puisse accéder à la table mysql.users. Nous essayons quand même d'accéder à la table wp\_users, mais celle ci a du être renommée car nous n'obtenons pas de résultat.

1. Utilisation d'un module de sécurité reconnu
2. Mise à jour régulière des plugins utilisés
3. Bien configurer le fichier robots.txt
4. Bien configurer les droits sur les fichiers



5. Configurer mysql pour interdire les requêtes multiples
6. Ne pas utiliser l'utilisateur sql root dans nos sites web

### III ) ALLER PLUS LOIN

#### 1 - Que faire du mot de passe crypté récupéré ?

Nous pourrions essayer de retrouver le mot de passe, car il n'est pas vraiment crypté : en réalité, ce que nous obtenons est une empreinte calculée avec un algorithme du type sha ou md5. Il semble donc possible d'effectuer une attaque de type force brute : on utilise un logiciel tiers qui calcule l'empreinte de toutes les combinaisons possibles entre 1 et 10 caractères, jusqu'à trouver une empreinte égale à celle obtenue.

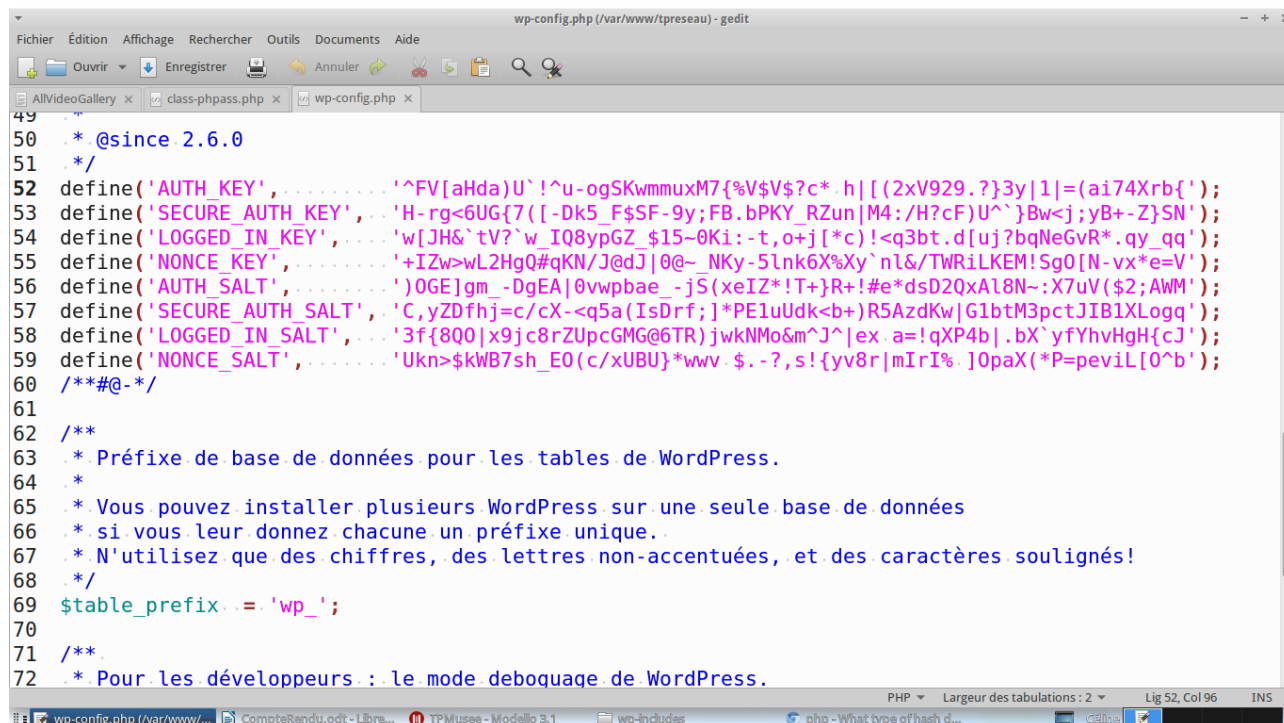
#### 2 - Le système de sécurité de Wordpress

Cependant, le système de sécurité de Wordpress nous en empêche : les développeurs de wordpress ont ajouté un « sel » sur l'algorithme de hashage.

Le sel est un mot choisi au départ, qu'on concatène au début du mot de passe avant de calculer l'empreinte. <http://md5live.com/decrypt-wordpress-passwords/>

Pour le décrypter, il faudrait donc plutôt chercher en force brute un mot de passe en 10 et 20 caractères (beaucoup plus long), puis essayer tous les suffixes possibles de cette chaîne.

Dans le fichier wp-config.php, nous voyons :



```
49
50 * @since 2.6.0
51 */
52 define('AUTH_KEY', ' ^FV[aHda)U`!^u-ogSKwmmuxM7{%V$V?$c*.h|[(2xV929.?}3y|1|=(ai74Xrb{');
53 define('SECURE_AUTH_KEY', 'H-rg<6UG{7([-Dk5_F$SF-9y;FB.bPKY_RZun|M4:/H?cF)U^` }Bw<j;yB+-Z}SN');
54 define('LOGGED_IN_KEY', 'w[JH&`tV?`w_IQ8ypGZ_$15~0Ki:-t,o+j[*c)!<q3bt.d[u]?bqNeGvR*.qy_qq');
55 define('NONCE_KEY', '+IZw>wL2HgQ#qKN/J@dJ|0@~_NKy-5lnk6X%Xy`nL&/TWRiLKEM!Sg0[N-vx*e=V');
56 define('AUTH_SALT', ' )OGE]gm_-DgEA|0vwpbae_-jS(xeIZ*!T+}R+!#e*dsD2QxAl8N~:X7uV($2;AWM');
57 define('SECURE_AUTH_SALT', 'C,yZDfhj=c/cX-<q5a(IsDrf;j*PEluUdk<b+)R5AzdKw|G1btM3pctJIB1XLogq');
58 define('LOGGED_IN_SALT', '3f{8Q0|x9jc8rZUpcGMG@6TR)jwkNM0&m^J^|ex.a=!qXP4b|.bX`yYhvHgH{cJ');
59 define('NONCE_SALT', 'Ukn>$kWB7sh_E0(c/xUBU}*wwv$.-?,s!{yv8r|mIrI%.]0paX(*P=peviL[0^b');
60 /**#@*/
61
62 /**
63  * Préfixe de base de données pour les tables de WordPress.
64  *
65  * Vous pouvez installer plusieurs WordPress sur une seule base de données
66  * si vous leur donnez chacune un préfixe unique.
67  * N'utilisez que des chiffres, des lettres non-accentuées, et des caractères soulignés!
68  */
69 $table_prefix = 'wp_';
70
71 /**
72  * Pour les développeurs : le mode débogage de WordPress.
```

Et dans le fichier wp-includes/class-phpass.php il y a toutes les fonctions qui ont permis de générer ces sels aléatoirement et d'encrypter le mot de passe (utilise les fonctions de hashage MD5 fournies par php).

En conclusion, l'utilisation d'un framework reconnu est également une barrière de sécurité qui permet de limiter les effets d'une vulnérabilité dans le code.