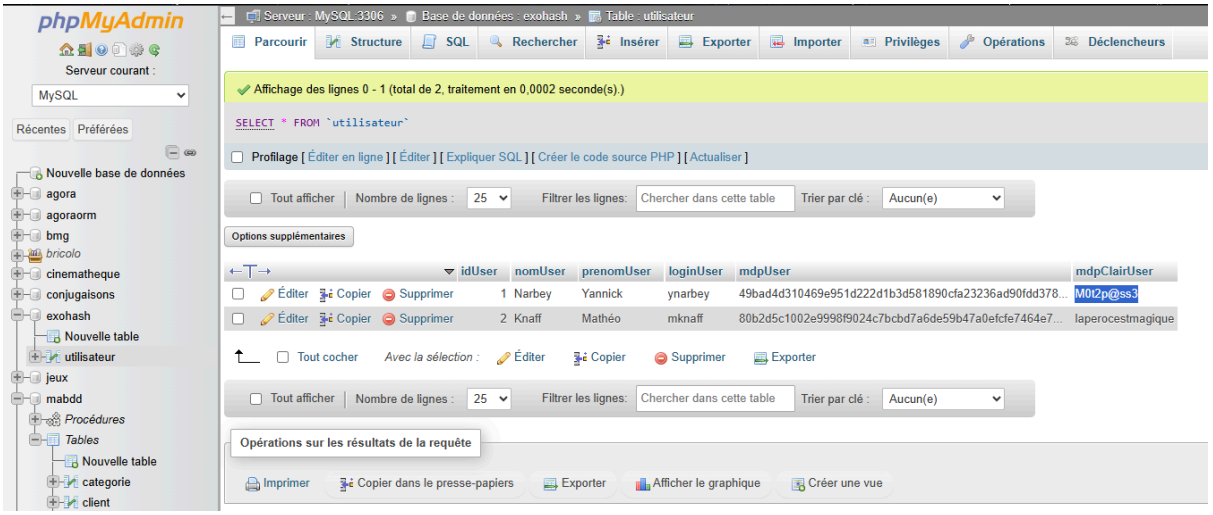
Compte-Rendu HASH

Pour commencer il faut importer la BDD “exohash” et ajouter un nouvel utilisateur :



Il faut ensuite ajouter quelques lignes dans le code afin de pouvoir prendre en compte le hashage (les lignes jaunes). Cela nous permets de hasher le mdp que va récupérer le formulaire :

```php
try {
    $requete_prepare = $db->prepare(query: 'SELECT idUser, loginUser, mdpUser, prenomUser, nomUser FROM utilisateur WHERE loginUser = :loginBindParam AND mdpUser = :passwordBindParam');
    $requete_prepare->bindParam(param: ':loginBindParam', var: &$_POST['login'], type: PDO::PARAM_STR);
    $motDePasseHash = hash(algo: "sha512", data: $_POST["password"]);
    $requete_prepare->bindParam(param: ':passwordBindParam', var: &$motDePasseHash, type: PDO::PARAM_STR);
    $requete_prepare->execute();
```

MAIS il faut également penser à aller modifier notre requête, car pour le moment elle ne gère que les mot de passes en clair :

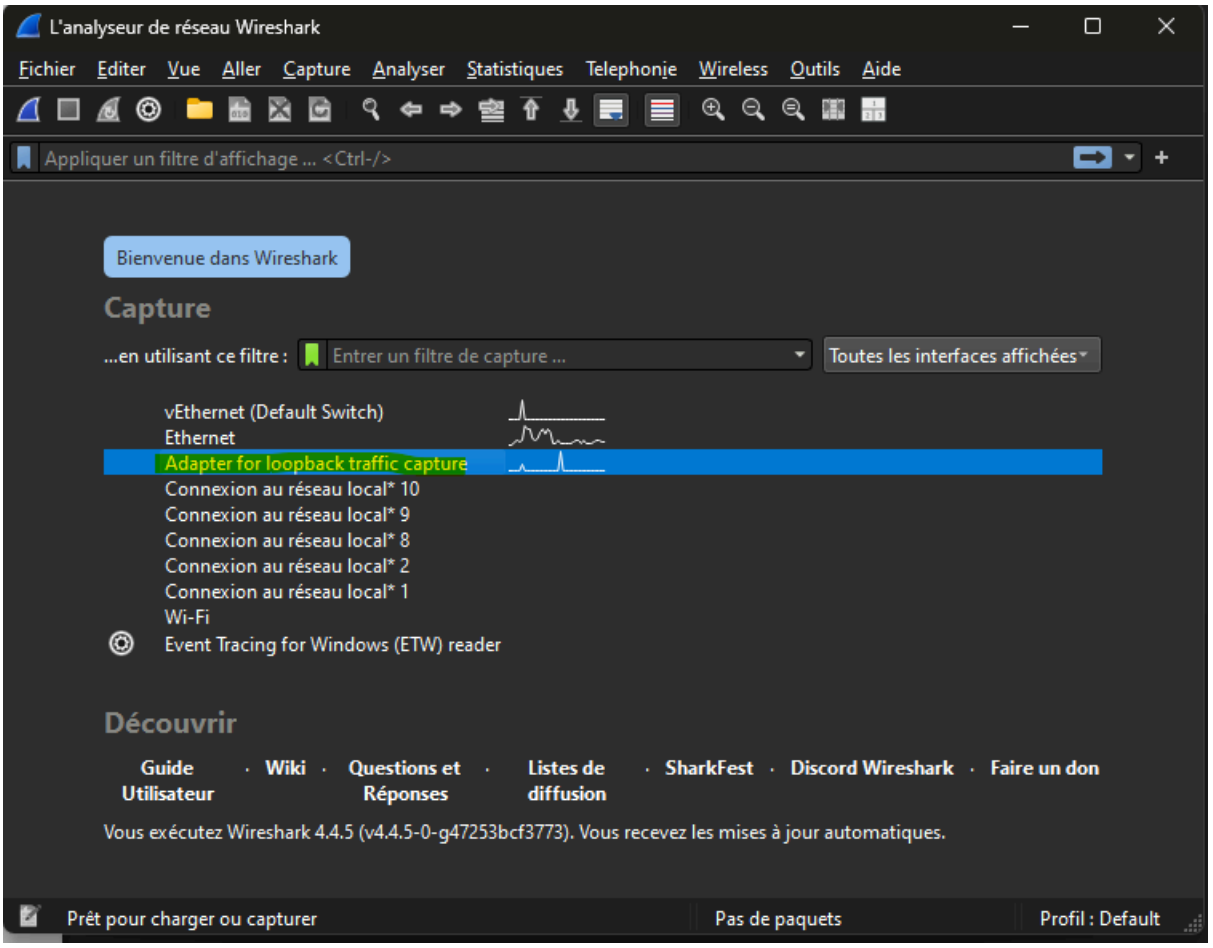
```php
try {
    $requete_prepare = $db->prepare(query: 'SELECT idUser, loginUser, mdpUser, prenomUser, nomUser FROM utilisateur WHERE loginUser = :loginBindParam AND mdpUser = :passwordBindParam');
    $requete_prepare->bindParam(param: ':loginBindParam', var: &$_POST['login'], type: PDO::PARAM_STR);
    $motDePasseHash = hash(algo: "sha512", data: $_POST["password"]);
    $requete_prepare->bindParam(param: ':passwordBindParam', var: &$motDePasseHash, type: PDO::PARAM_STR);
    $requete_prepare->execute();
```

Ensuite on test :

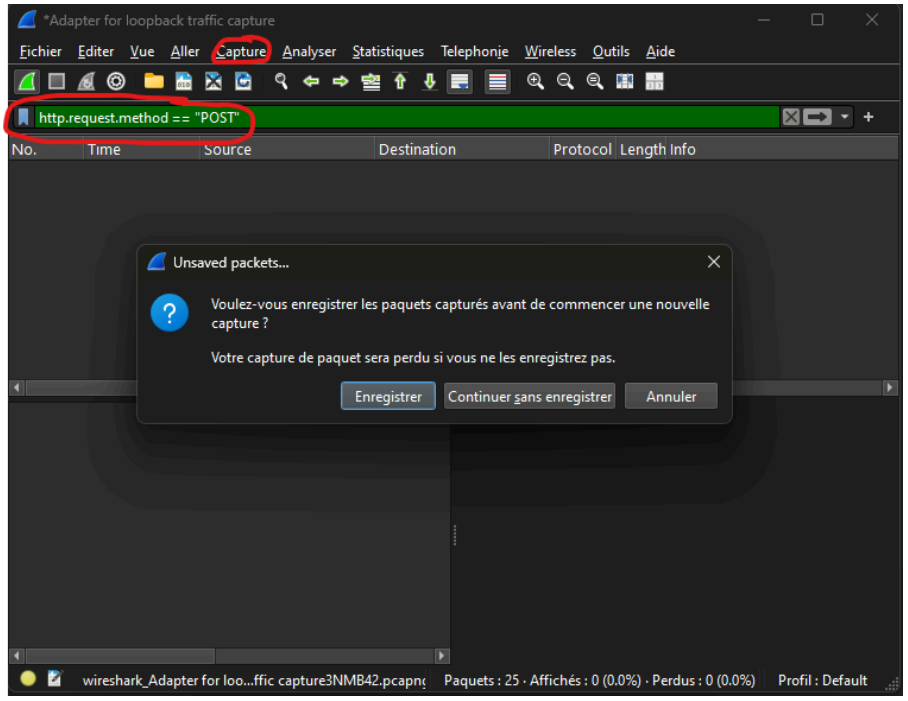
Résultat :

bienvenue Mathéo Knaff.

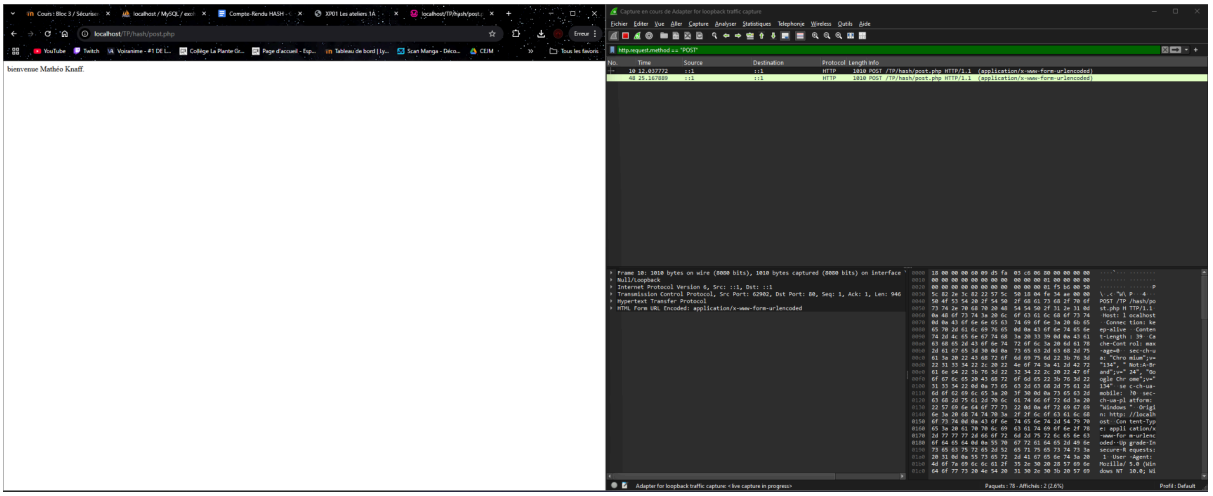
Ensuite il faut installer et lancer Wireshark et choisir la connexion “loopback” :



Il faut ensuite ajouter un filtre et démarrer la capture pour pouvoir enregistrer les méthodes “POST” :



Cela nous permet d’avoir ceci une fois le formulaire exécuter de nouveau :



On peut remarquer que Wireshark arrive à avoir le mot de passe alors qu’il est censé être hashé. Et ceux car dans le formulaire il est entrer de manière clair ainsi que dans la requête donc une personne attaquant le trafic verra tout de suite le mot de passe si on ne fait rien, hachage ou non :