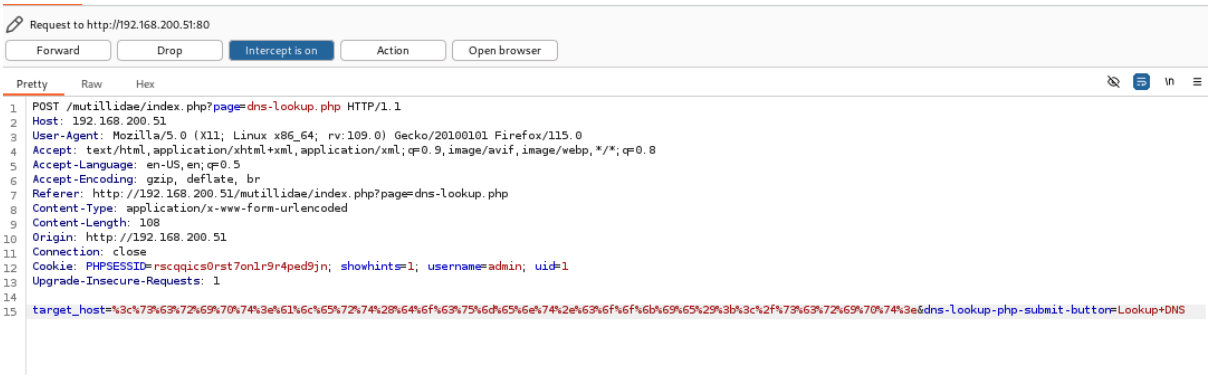
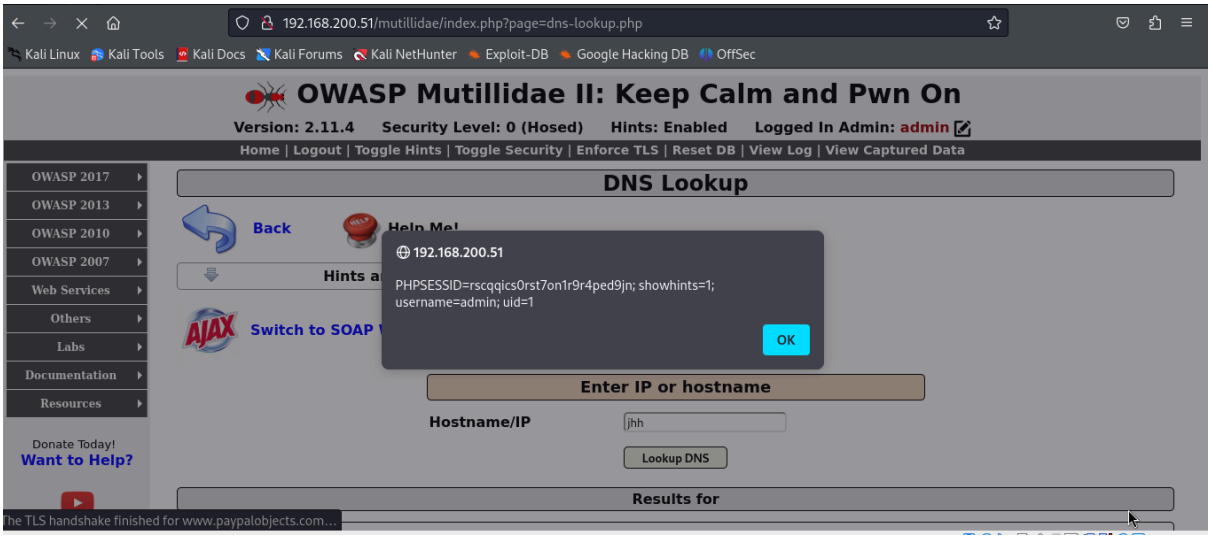


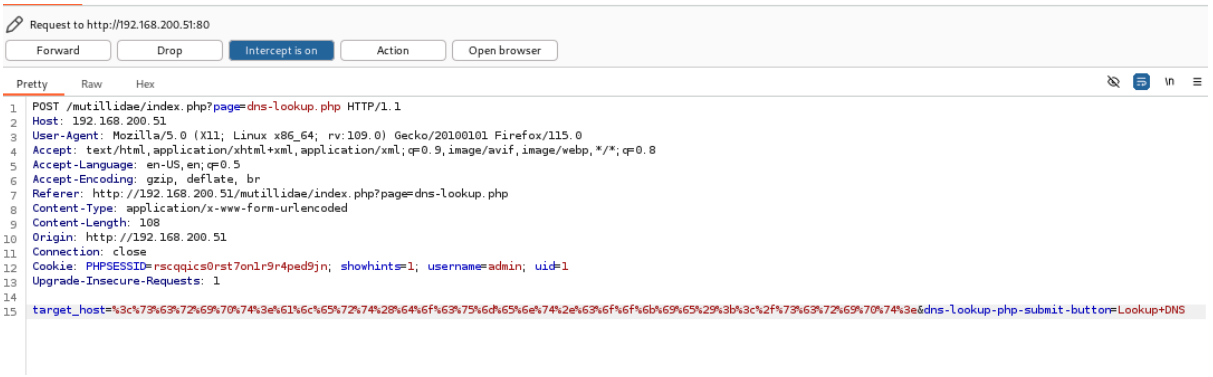


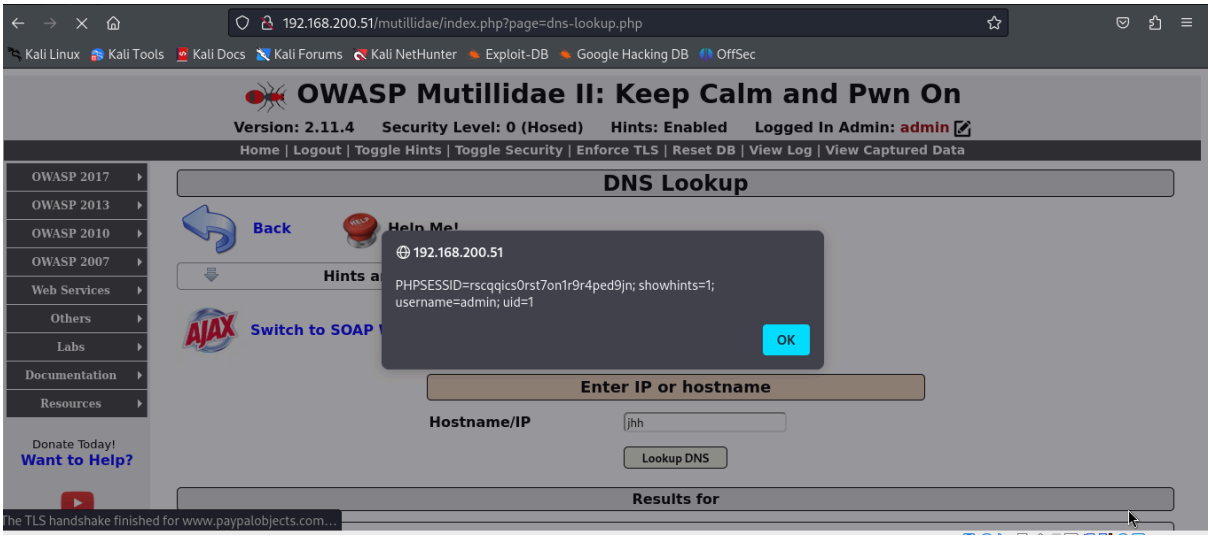
Travail à faire 2 Nouvelle tentative en mode sécurisé et analyse du code source
Le but de cette deuxième partie est de tester à nouveau l'attaque après activation du codage sécurisé
et de comprendre l'encodage mis en place.
Test du niveau 1 de sécurité :a
Q1. Est-ce que le niveau de sécurité 1 permet d'éviter l'attaque avec Burpsuite ?
Non il ne permet pas d'éviter l'attaque avec Burpsuite.
Q2. Est-il possible d'écrire le code malicieux directement dans le formulaire ?
Non ce n'est pas possible car la sécurité est trop faible.
Q3. En observant le code de la page dns-lookup.php, repérer les sécurités activées à ce niveau.
Comme sécurité,il y a la protection contre les injections de commandes,l'activation du contrôle HTML, activation de la validation de JavaScript, protection contre la méthode TAMPER et protection contre l'attaque XSS.
Q4. Quels sont les caractères typiques utilisés lors d'une attaque XSS ?
Test du niveau 5 de sécurité :

Oui le niveau 5 évite l'attaque en Burpsuite.

Q5. Est-ce que le niveau de sécurité 5 permet d'éviter l'attaque avec BurpSuite ?

Q6. En observant le fichier dns-lookup.php, repérer les variables spécifiques





Travail à faire 2 Nouvelle tentative en mode sécurisé et analyse du code source

Le but de cette deuxième partie est de tester à nouveau l'attaque après activation du codage sécurisé

et de comprendre l'encodage mis en place.

Test du niveau 1 de sécurité :a

Q1. Est-ce que le niveau de sécurité 1 permet d'éviter l'attaque avec Burpsuite ?

Non il ne permet pas d'éviter l'attaque avec Burpsuite.

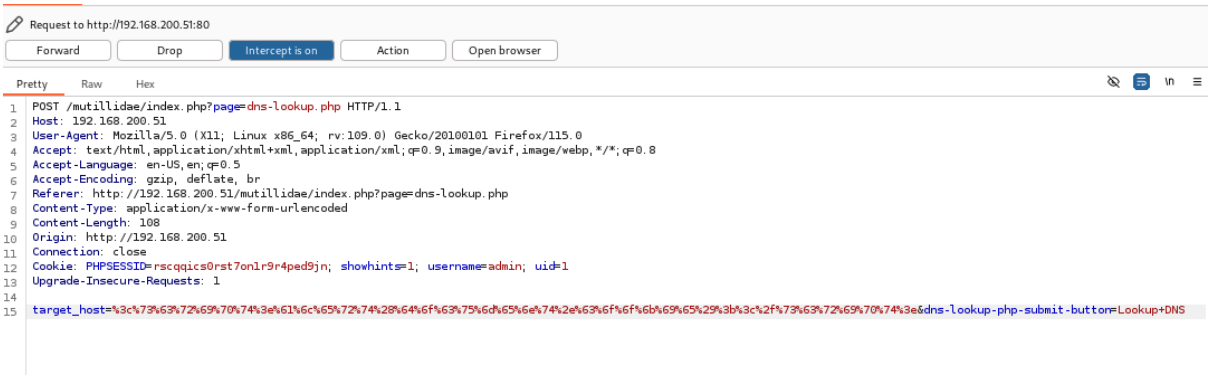
Q2. Est-il possible d'écrire le code malicieux directement dans le formulaire ?

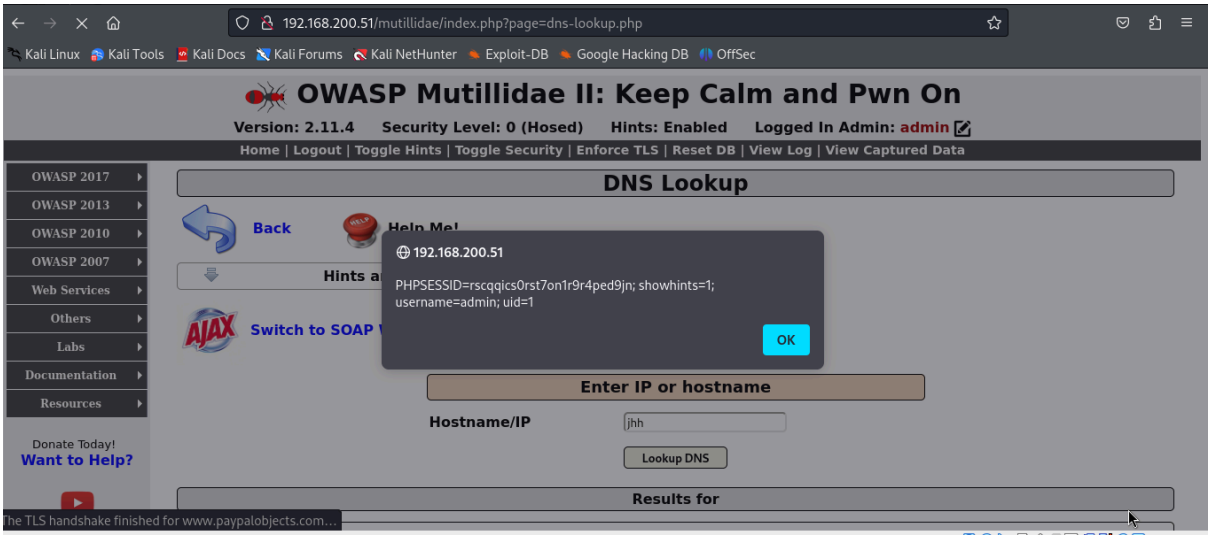
Non ce n'est pas possible car la sécurité est trop faible.

Q3. En observant le code de la page dns-lookup.php, repérer les sécurités activées à ce niveau.

Comme sécurité,il y a la protection contre les injections de commandes,l'activation du contrôle HTML, activation de la validation de JavaScript, protection contre la méthode TAMPER et protection contre l'attaque XSS.

Q4. Quels sont les caractères typiques utilisés lors d'une attaque XSS ?
Test du niveau 5 de sécurité :
Oui le niveau 5 évite l'attaque en Burpsuite.
Q5. Est-ce que le niveau de sécurité 5 permet d'éviter l'attaque avec BurpSuite ?
Q6. En observant le fichier dns-lookup.php, repérer les variables spécifiques





Comme sécurité,il y a la protection contre les injections de commandes,l'activation du ction contre l'attaque XSS.
Travail à faire 2 Nouvelle tentative en mode sécurisé et analyse du code source
Le but de cette deuxième partie est de tester à nouveau l'attaque après activation du codage sécurisé
et de comprendre l'encodage mis en place.
Test du niveau 1 de sécurité :a
Q1. Est-ce que le niveau de sécurité 1 permet d'éviter l'attaque avec Burpsuite ?
Non il ne permet pas d'éviter l'attaque avec Burpsuite.
Q2. Est-il possible d'écrire le code malicieux directement dans le formulaire ?
Non ce n'est pas possible car la sécurité est trop faible.
Q3. En observant le code de la page dns-lookup.php, repérer les sécurités activées à

Q4. Quels sont les caractères typiques utilisés lors d’une attaque XSS ?
Test du niveau 5 de sécurité :
Oui le niveau 5 évite l’attaque en Burpsuite.
Q5. Est-ce que le niveau de d