

Request to http://192.168.200.51:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
2 Host: 192.168.200.51
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://192.168.200.51/mutillidae/index.php?page=dns-lookup.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 108
10 Origin: http://192.168.200.51
11 Connection: close
12 Cookie: PHPSESSID=rscqqjics0rst7on1r9r4ped9jn; showhints=1; username=admin; uid=1
13 Upgrade-Insecure-Requests: 1
14
15 target_host=%3c%73%63%72%69%70%74%3e%61%6c%65%72%64%28%64%6f%63%75%6d%65%6e%74%2e%63%6f%6b%69%65%29%3b%3c%2f%73%63%72%69%70%74%3e%6dns-lookup.php-submit-button=Lookup+DNS

```

The screenshot shows the OWASP Mutillidae II interface. A modal dialog box is open, displaying the result of a DNS lookup for the IP address 192.168.200.51. The modal contains the session ID (PHPSESSID=rscqqjics0rst7on1r9r4ped9jn), hints status (showhints=1), and user information (username=admin, uid=1). Below the modal, there is a form with a placeholder 'Enter IP or hostname' and a 'Hostname/IP' input field containing 'jhh'. A 'Lookup DNS' button is visible next to the input field. The main page has a navigation menu on the left and various links at the top.

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.

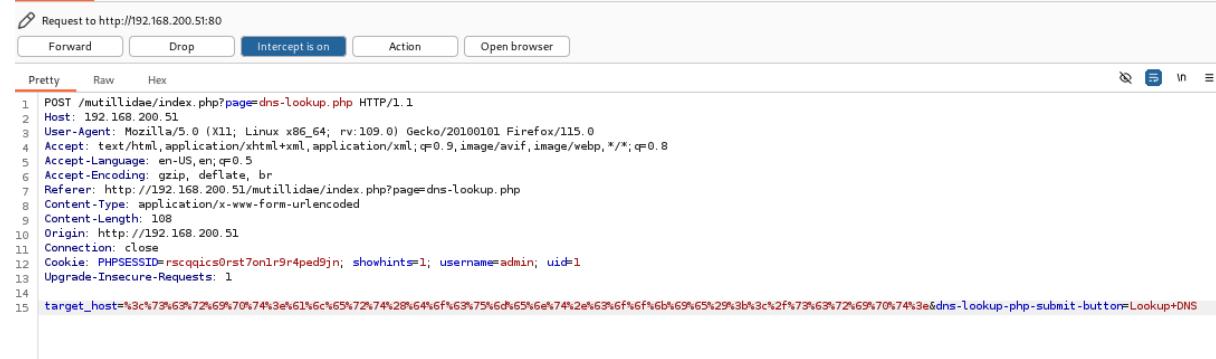
Q4. Quels sont les caractères typiques utilisés lors d'une attaque XSS ?

Test du niveau 5 de sécurité :

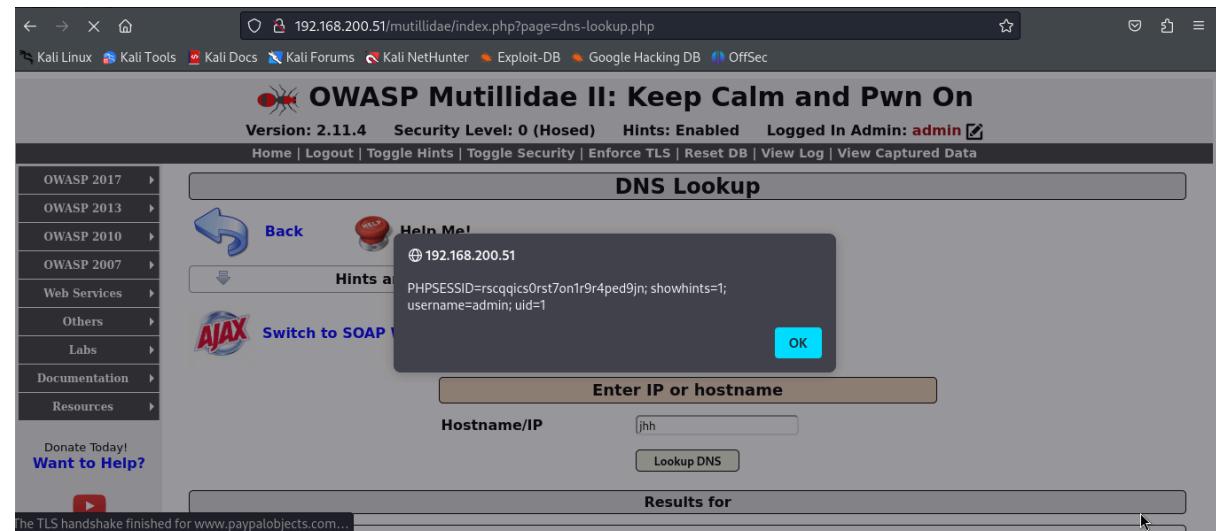
Oui le niveau 5 évite l'attaque en Burpsuite.

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



```
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 192.168.200.51
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://192.168.200.51/mutillidae/index.php?page=dns-lookup.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 108
Origin: http://192.168.200.51
Connection: close
Cookie: PHPSESSID=rscqqics0rst7on1r9r4ped9jn; showhints=1; username=admin; uid=1
Upgrade-Insecure-Requests: 1
target_host=%3c%73%63%72%69%70%74%3e%61%6c%65%72%74%28%64%6f%63%75%6d%65%6e%74%2e%63%6f%6f%6b%69%65%29%3b%3c%2f%73%63%72%69%70%74%3e&dns-lookup-php-submit-button=Lookup+DNS
```



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.

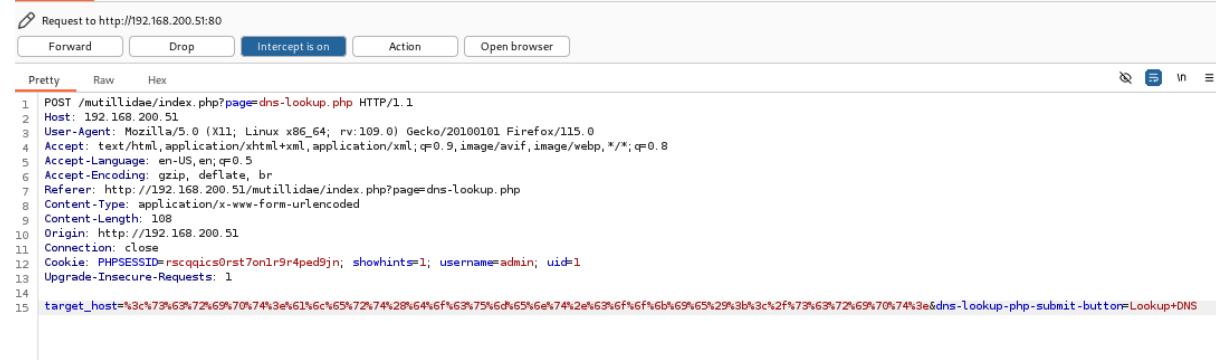
Q4. Quels sont les caractères typiques utilisés lors d'une attaque XSS ?

Test du niveau 5 de sécurité :

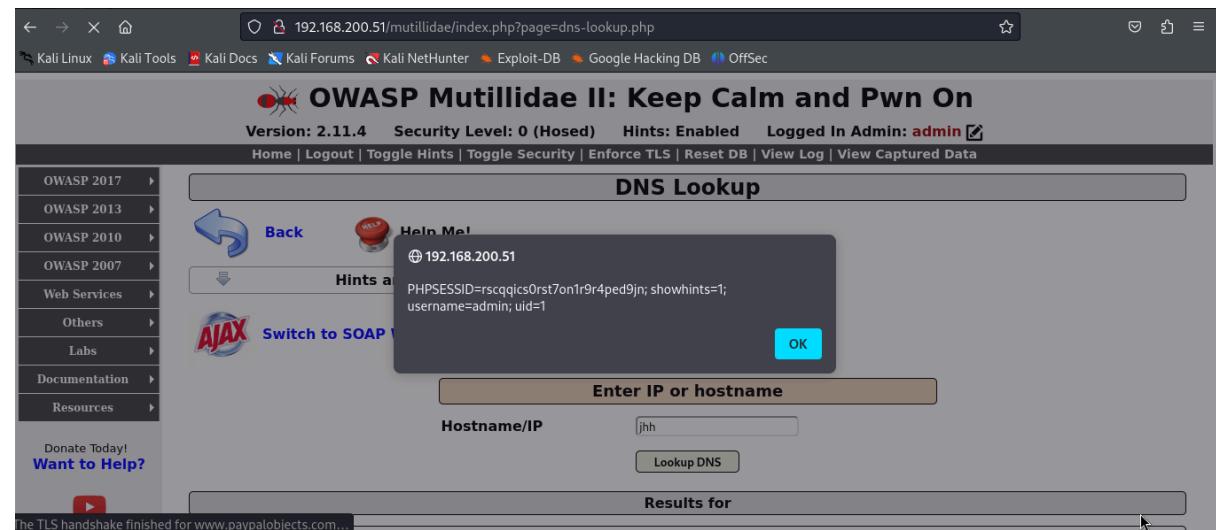
Oui le niveau 5 évite l'attaque en Burpsuite.

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



```
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 192.168.200.51
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://192.168.200.51/mutillidae/index.php?page=dns-lookup.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 108
Origin: http://192.168.200.51
Connection: close
Cookie: PHPSESSID=rscqqjics0rst7on1r9r4ped9jn; showhints=1; username=admin; uid=1
Upgrade-Insecure-Requests: 1
target_host=%3c%73%63%72%69%70%74%3e%61%6c%65%72%74%28%64%6f%63%75%6d%65%6e%74%2e%63%6f%6b%69%65%29%3b%3c%2f%73%63%72%69%70%74%3e&dns-submit-button=Lookup+DNS
```



Comme sécurité, il y a la protection contre les injections de commandes, l'activation du codage 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