Vulnerability analysis
The tadasnippets application maintains a database of code snippets. It lets the user view existing code snippets (with view.php?name=...) and add a new code snippet to the database (with index.php and some POST parameters). The SELECT query performed by the view.php page is vulnerable to SQL injection by the GET parameter "name". We can confirm the presence of the vulnerability by requesting:
view.php?name=doesntexist'+OR+1=1+--+
And checking that the site returns the first snippet of the database instead of nothing. The "name" parameter is ineffectively protected with a string-based blackbox filter that strips the "select" and "union" strings in a case-insensitive fashion.