# Core - Bug # 19831

| | | | |
|---|---|---|---|
| **Status:** | Resolved | **Priority:** | Must have |
| **Author:** | Marcus Krause | **Category:** | |
| **Created:** | 2009-01-15 | **Assigned To:** | Marcus Krause |
| **Updated:** | 2009-01-21 | **Due date:** | |

| | |
|---|---|
| **TYPO3 Version:** | 4.0 |
| **PHP Version:** | 5.2 |
| **Complexity:** | |
| **Is Regression:** | |
| **Sprint Focus:** | |

| | |
|---|---|
| **Subject:** | Session fixation vulnerability in user authentication |

**Description**

references TYPO3 Security Team OTRS issue #2008102610000015

Versions:
4.0 up to trunk (4.0, 4.1, 4.2, trunk)

Problem:
Session IDs are reused by TYPO3 even when they not yet exist in the db but are submitted by a client.

Solution:
Check if there's a session record in the database before using submitted session ids.

Provided by TYPO3 Security Team
(issue imported from #M10146)

**Related issues:**

| | | |
|---|---|---|
| related to Core - Bug # 19880: Patch 10146 in Version 4.2.4 does not work for... | **Resolved** | **2009-01-21** |
| related to Core - Bug # 19867: DB session records are only created when users... | **Resolved** | **2009-01-20** |
| related to Core - Bug # 19879: after upgrade from 4.1.7 to 4.1.8 feusers and ... | **Resolved** | **2009-01-21** |
| related to Core - Bug # 19874: Typo3 4.1.8: fe_session_data regression due to... | **Resolved** | **2009-01-21** |
| related to Core - Bug # 19908: session fixation fix avoid BE login | **Resolved** | **2009-01-25** |
| related to Core - Bug # 20424: Built In shopping basket is not working | **Closed** | **2009-05-14** |
| related to Core - Bug # 20290: Adding entries to recs[]-Array not working | **Resolved** | **2009-04-07** |

## History

**#1 - 2009-01-15 06:14 - Marcus Krause**

The first patch is for trunk only as it makes use of newly added function exec_SELECTcountRows(), the other one is for 4-0 up to 4-2 where the row counting is down the old way.

ready to be committed

**#2 - 2009-01-18 17:27 - Marcus Krause**

adding new patch 10146_trunk_v1.diff which replaces variablename $dbres by $count as requested by Francois

**#3 - 2009-01-20 13:12 - Ingmar Schlecht**

Committed to 4.0, 4.1, 4.2 and trunk.

**Files**

| | | | |
|---|---|---|---|
| 10146.diff | 1.4 kB | 2009-01-15 | Administrator Admin |
| 10146_trunk_v1.diff | 1.2 kB | 2009-01-18 | Administrator Admin |