# TYPO3 Core - Bug #21336

## Encryption key can be recalculated when using normal mailform when [FE][strictFormmail] == 0

2009-10-22 11:11 - Ernesto Baschny

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 2009-10-22 |
| **Priority:** | Must have | **Due date:** | |
| **Assignee:** | Ernesto Baschny | **% Done:** | 0% |
| **Category:** | | **Estimated time:** | 0.00 hour |
| **Target version:** | | | |
| **TYPO3 Version:** | 4.3 | **Complexity:** | |
| **PHP Version:** | 5.2 | **Is Regression:** | |
| **Tags:** | | **Sprint Focus:** | |

**Description**

These settings required for being exploitable:
['TYPO3_CONF_VARS']['FE']['secureFormmail']  0
['TYPO3_CONF_VARS']['FE']['strictFormmail']  0

Reported by Stefan Schuler.

Security Team OTRS reference: 2009021010000086
(issue imported from #M12310)

### History

#### #1 - 2009-10-22 11:30 - Ernesto Baschny

Commited to:
trunk (rev.6255 = beta2)
TYPO3_4-2 (rev.6256 = 4.2.10)
TYPO3_4-1 (rev.6257 = 4.1.11)

#### #2 - 2010-06-30 10:28 - Helmut Hummel

Comments from Philippe Oechslin: ==========

Ok, I was looking at 4.3.1 but missed that sha1. But still:

- the ascii cleartext is xored with hex digits of the key, making only
16 possible ciphertexts for each character. For example, if the
cleartext is made only of 'a', '.' and '', you can decode it right
away, as the 16 possible encodings of these three characters never
overlap. Actually the '' doesn't overlap with any alphanumerical
character.

- the $key, even though it is a sha1 of the encryption key, is the same
for all encodings. If you know one cleartext that is long enough you can
decode other ciphertexts. It would be good to have something like

$key = sha1($this->TYPO3_CONF_VARS['SYS']['encryptionKey'] .':'. $string);

or even make that

$key = sha1($this->TYPO3_CONF_VARS['SYS']['encryptionKey'] .
':RoundTripKey:'. $string);

so that you can easily derive different keys for other purposes.