Security Guide - Task # 59398

Task # 60744 (Closed): Raise version of TYPO3 Security Guide to 1.0.6

Status:	Closed	**Priority:**	Should have
Author:	Michael Schams	**Category:**	Guidelines for Integrators
Created:	2014-06-07	**Assigned To:**	Michael Schams
Updated:	2014-08-04	**Due date:**	
Subject:	Executable binaries shipped with extensions		

Description

A few TYPO3 extensions in TER contain binaries, e.g. Unix/Linux ELF files (compiled executables). Using these is a security risk, because it can not be verified what these files really do (unless they are reverse-engineered or dissected likewise).

Add a section to the Security Guide that explains the risks and recommends to build binaries from trusted sources and from scratch only (which often requires the source code) and **not** use binaries, where you do not know (and you can not verify) it's functionality under the hood.

History

#1 - 2014-06-23 14:06 - Michael Schams

- Status changed from New to Accepted

- Assigned To set to Michael Schams

- Priority changed from Could have to Should have

- Target version set to 1.0.6

#2 - 2014-06-23 14:12 - Michael Schams

- Category set to Guidelines for Integrators

#3 - 2014-08-02 12:52 - Michael Schams

- File task59398-1.patch added

- Status changed from Accepted to Under Review

- % Done changed from 0 to 80

- File task59398-1.patch added

- Remaining (hours) deleted (1.0)

My suggestion:

> TYPO3 extensions (.t3x files) are packages, which may contain any kind of data/files. This can not only be readable PHP or Javascript source code, but also binary files, e.g. Unix/Linux ELF files or Microsoft Windows .exe files (compiled executables).
>
> Executing these files on a server is a security risk, because it can not be verified what these files really do (unless they are reverse-engineered or dissected likewise). Thus it is highly recommended **not** to use any TYPO3 extensions, which contain executable binaries. The only way binaries should be installed on a server is to compile them from scratch (and review the source code before use).

Requires review from Security Team.

#4 - 2014-08-02 14:42 - Michael Schams

- Parent task set to #60744

#5 - 2014-08-04 11:04 - Michael Schams

- Status changed from Under Review to Needs Feedback

- Assigned To changed from Michael Schams to Helmut Hummel

Updated wording based on a suggestion by Helmut:

> TYPO3 extensions (.t3x files) are packages, which may contain any kind of data/files. This can not only be readable PHP or Javascript source code, but also binary files, e.g. Unix/Linux ELF files or Microsoft Windows .exe files (compiled executables).
>
> Executing these files on a server is a security risk, because it can not be verified what these files really do (unless they are reverse-engineered or dissected likewise). Thus it is highly recommended **not** to use any TYPO3 extensions, which contain executable binaries. Binaries should only come from trusted and/or verified sources such as the vendor of your operating system - which also ensures, these binaries get updated in a timely manner, if a security vulnerability is discovered in these components.

Requires review from Security Team (Helmut?).

#6 - 2014-08-04 11:05 - Michael Schams

- File task59398-2.patch added

- File task59398-2.patch added

#7 - 2014-08-04 13:04 - Helmut Hummel

nice, thanks!

#8 - 2014-08-04 13:58 - Michael Schams

- Status changed from Needs Feedback to Closed

- Assigned To changed from Helmut Hummel to Michael Schams

- % Done changed from 80 to 100

TYPO3 Security Guide v1.0.6 published - closing ticket as resolved.

Files

task59398-1.patch	1.2 kB	2014-08-02	Michael Schams
task59398-2.patch	1.3 kB	2014-08-04	Michael Schams