CMS-Sicherheit

Problemstellung

- sicherer Betrieb von CMSystemen gewinnt zunehmend an Bedeutung.
- Angriffspotenzial durch Quasi-Monokultur von Opensource-Systemem wie drupal, Typo3, Joomla usw.
- Sichheitskonzept muss schon bei der Planung berücksichtigt werden.
- Was-wäre-wenn-Szenario.
- Regelung der Verantwortlichkeiten.
- Patch-Strategie
- Regelung und Verfahrensweise von Major-Minor-Updates
- regelmäßiges Monitoring hinsichtlich Sicherheit nötig
- Problem Funktionserweiterung durch Module vs. selbstprogrammiert.

Typische Angriffsvektoren

Angriffsart	Kurzbeschreibung	Beschreibung
DOS	todo	todo
Code Execution	todo	todo
Overflow	todo	todo
Memory Corruption	todo	todo
Sql Injection	todo	todo
XSS	todo	todo
Directory Traversal	todo	todo
Http Response Splitting	todo	todo
Bypass something	todo	todo
Http Response Splitting	todo	todo
Gain Information	todo	todo
Gain Privileges	todo	todo
CSRF	todo	todo
File Inclusion	todo	todo

Meldungen von Schwachstellen

- http://cvedetails.com/
- http://nvd.nist.gov/
- https://portal.cert.dfn.de/adv/archive/