

CMS-Sicherheit

Problemstellung

- sicherer Betrieb von CMS-Systemen gewinnt zunehmend an Bedeutung.
- Angriffspotenzial durch Quasi-Monokultur von Opensource-Systemen wie Drupal, TYPO3, Joomla usw.
- Sicherheitskonzept 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

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/>

From:
<https://g6r.de/dw/> - g6r

Permanent link:
<https://g6r.de/dw/webdev:cmssec?rev=1372077930>

Last update: 2014-05-07 10:53



