



Du kommst hier nicht rein!  
Sicher programmieren



1. Sicher – warum?
2. Live Beispiele in echten T3 Extensions
  1. SQL Injection
  2. XSS (Cross Site Script)
3. Filtern der Usereingaben
4. Vorstellung von wt\_doorman
5. Allgemeine Links zum Thema



# Sicher – Warum?



**Es ist kein Problem eine unsichere Extension einzusetzen**

**Jedenfalls so lange nichts passiert!**



## Worst case für die Agentur:

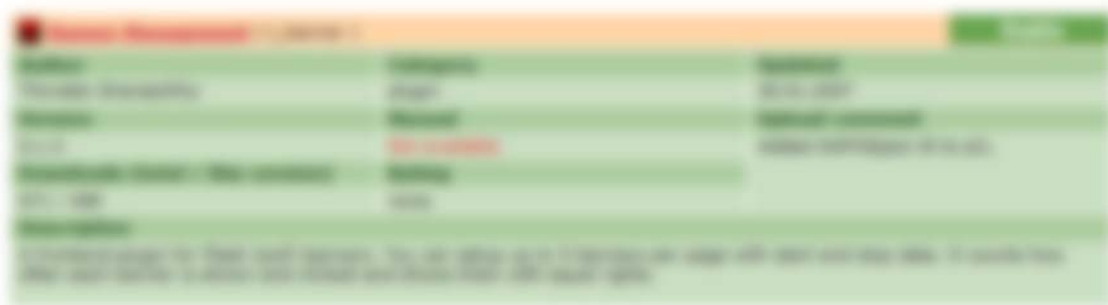
1. Datenverlust
2. Unmut des Kunden
3. Zeitverlust
4. Geldverlust
5. Mögliche Schadensersatzforderungen
6. Mögliche Folgeschäden



# Beispiele aus dem TER

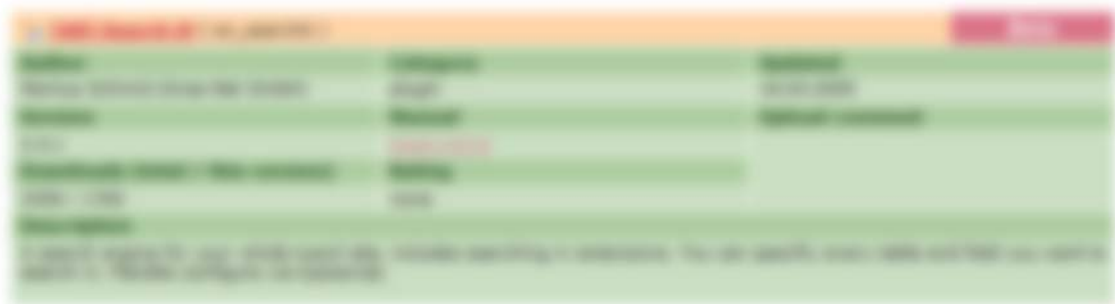


# SQL injection





# Cross Site Scripting





# Filtern der Usereingaben



## Umwandlung in Integer

*\$int = intval(\$string);*

Findet Einsatz vorwiegend bei Datenbank Aktionen  
(z.B. Zeige Datensatz mit uid = intval(\$uid) )

Bsp:

- „xxx“ zu 0

- „33“ zu 33



## String bei Datenbankaktionen

```
$string =  
$GLOBALS[TYPO3_DB]->fullQuoteString($string);
```

Findet Einsatz vorwiegend bei Datenbank Aktionen  
(z.B. Zeige Datensatz mit wert = „Usereingabe“)

Bsp:

- „x'xx“ zu „x\'xx“

- „3“3“ zu „3\“3“



## Ausgabe im FE

```
$string = htmlentities($string);
```

Ausgabe von Text (auch in HTML) – Wandlung der Sonderzeichen in ASCII Code

Bsp:

- „xßxx“ zu „x&szlig;xx“

- „3'>3“ zu „3&#039;&#062;3“



## Weitere Funktionen

1. `t3lib_div::removeXSS()`
2. `strip_tags()` (kein umfassender Schutz!)
3. `tslib_cObj::removeBadHTML()`
4. `Addslashes()`
5. Bzw. `t3lib_div::addSlashesOnArray()`



wt\_doorman



- Nutzung zur Filterung sämtlicher GET und POST Parameter einer TYPO3 Installation
- Nutzung in eigener Extension
  - wt\_directory
  - wt\_gallery



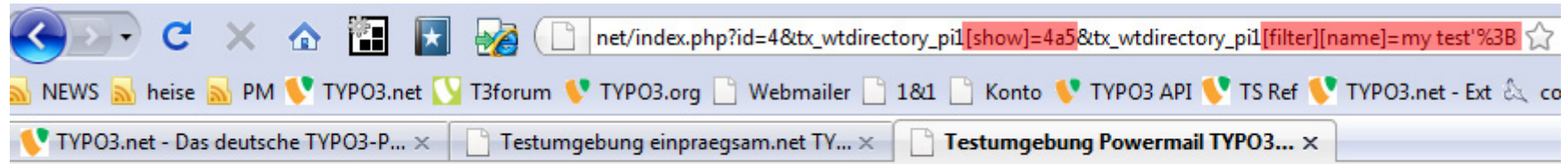
```
Adobe Dreamweaver CS3 - [...tions\1&1\typo3_powermail\typo3conf\ext\wt_directory\pi1\class.tx_wtdirectory_pi1.php (XHTML)]
Datei Bearbeiten Ansicht Einfügen Modifizieren Text Befehle Site Fenster Hilfe

class.tx_wtdirectory_pi1.php
Code Teilen Entwurf Titel:
↓ ↑ ↻ 🌐 🔍 📄 📄 Seite überprüfen

94 function secure() {
95     if (class_exists('tx_wtdoorman_security')) {
96         $this->sec = t3lib_div::makeInstance('tx_wtdoorman_security'); // Create new instance for security class
97         $this->sec->secParams = array ( // Allowed piVars type (int, text, alphanum, "value")
98             'show' => 'int', // show should be integer
99             'list' => '"all","none"', // list should be "all" or "none"
100            'vCard' => 'int', // vCard should be integer
101            'pointer' => 'int', // pointer should be integer
102            'catfilter' => 'int', // catfilter should be integer
103            'filter' => array (
104                '*' => 'text' // every filter should be text
105            )
106        );
107        $this->piVars = $this->sec->sec($this->piVars); // overwrite piVars piVars from doorman class
108    } else die ('Extension wt_doorman not found!');
109 }
```

6 K / 1 Sek

int, defined values, text, alphanum, htmlentities



show	4a5
filter	name my test';
show	4
filter	name my test\';

**before filtering**

**after filtering**



# Allgemeine Links

## Zum Thema



- wt\_doorman:  
[http://typo3.org/extensions/repository/view/wt\\_doorman/current/](http://typo3.org/extensions/repository/view/wt_doorman/current/)
- Wikipedia zu SQL Injection:  
[http://de.wikipedia.org/wiki/SQL\\_Injection](http://de.wikipedia.org/wiki/SQL_Injection)
- Wikipedia zu XSS:  
[http://de.wikipedia.org/wiki/Cross-Site\\_Scripting](http://de.wikipedia.org/wiki/Cross-Site_Scripting)
- typo3.org zum Thema security  
[http://typo3.org/teams/security/  
security@typo3.org](http://typo3.org/teams/security/security@typo3.org)
- Tutorial Henning Pingel:  
<http://www.slideshare.net/hepi/developing-extensions-with-security-in-mind-presentation>

Fragen, Wünsche oder  
Anregungen?



Vielen Dank für Ihre  
Aufmerksamkeit

