TYPO3 Core - Bug #29693

Respect HTTP_X_FORWARDED_PROTO in SSL check

2011-09-12 14:57 - Michael Stucki

Status:	Rejected	**Start date:**	2011-09-12
Priority:	Should have	**Due date:**	
Assignee:	Michael Stucki	**% Done:**	0%
Category:	Backend API	**Estimated time:**	0.00 hour
Target version:			
TYPO3 Version:	4.5	**Complexity:**	
PHP Version:		**Is Regression:**	No
Tags:		**Sprint Focus:**	

Description

If the webserver runs behind a proxy server which takes care of the SSL encryption, it may forward the HTTP_X_FORWARDED_PROTO header.
However, TYPO3 ignores the header when checking for SSL using t3lib_div::getIndpEnv('TYPO3_SSL').

The header value seems to be a de-facto-standard according to Wikipedia (similar to HTTP_X_FORWARDED_FOR):
http://en.wikipedia.org/wiki/List_of_HTTP_header_fields

Related issues:

Related to TYPO3 Core - Bug #16395: There is a error in detecting the ssl page	**Closed**	**2006-07-22**
Related to TYPO3 Core - Bug #32341: $_SERVER['HTTPS'] vs. $_SERVER['HTTP_HTTP...	**Closed**	**2011-12-06**
Related to TYPO3 Core - Bug #32999: Cannot properly handle reverse-proxy as S...	**Rejected**	**2012-01-05**
Related to TYPO3 Core - Feature #39016: Hook to modify t3lib_div::getIndpEnv ...	**Closed**	**2012-07-17**
Related to TYPO3 Core - Bug #37467: Change in class.t3lib_div.php may break t...	**Closed**	**2012-05-24**
Related to TYPO3 Core - Bug #65334: SSL detection: better support for reverse...	**Rejected**	**2015-02-25**
Related to TYPO3 Core - Bug #81837: SSL mixed content issues in backend when ...	**Closed**	**2017-07-11**
Related to TYPO3 Core - Bug #86264: Trusted hosts pattern mismatch with Nginx...	**Accepted**	**2018-09-15**
Related to TYPO3 Core - Bug #92187: HTTP/HTTPS not correctly determined behin...	**Under Review**	**2020-09-03**
Has duplicate TYPO3 Core - Feature #35723: Improvement for SSL detection behi...	**Closed**	**2012-04-05**

History

#1 - 2011-09-12 14:58 - Michael Stucki

- Status changed from New to Accepted

- Assignee set to Michael Stucki

#2 - 2011-09-12 15:12 - Mr. Hudson

Patch set 1 of change I3db6cf6faab11718083709cfe6fc9b5df71812b4 has been pushed to the review server.
It is available at http://review.typo3.org/4913

#3 - 2011-09-12 15:20 - Mr. Hudson

Patch set 1 of change I3db6cf6faab11718083709cfe6fc9b5df71812b4 has been pushed to the review server.
It is available at http://review.typo3.org/4916

#4 - 2011-09-12 15:23 - Mr. Hudson

Patch set 1 of change Id248bf4a9b83703f3a8cdc4df6c43c1c8a7ec105 has been pushed to the review server.
It is available at http://review.typo3.org/4921

#5 - 2011-09-12 16:54 - Andreas Wolf

- Category set to Backend API

- Status changed from Accepted to Under Review

#6 - 2011-09-13 21:56 - Mr. Hudson

Patch set 2 of change I3db6cf6faab11718083709cfe6fc9b5df71812b4 has been pushed to the review server.
It is available at http://review.typo3.org/4913

#7 - 2011-09-19 13:29 - Michael Stucki

- Status changed from Under Review to Rejected

This feature should not be used because the HTTP_X_FORWARDED_PROTO header can be forged by clients. The solution is to use "HTTPS=on" instead.
Won't fix.

#8 - 2013-07-14 12:11 - Christian Kuhn

This was discussed and denied again with https://review.typo3.org/#/c/21853/

#9 - 2013-07-14 12:17 - Christian Kuhn

The only way to support this for people who know what they are doing is a possible hook in getIndPEnv, see issue #39016 ... I would suggest such a patch now.

#10 - 2013-07-17 01:24 - Christian Ludwig

Adding a hook (only) seems to me more risky because there will be an extension soon, that handles HTTP_X_FORWARDED_PROTO without any extra checks. And this will make TYPO3 more insecure than offering the right solution with the core (and making such an extension dispensable).

Please see my comment at https://review.typo3.org/#/c/4913/ on how to make this patch secure!

At the moment the only dirty (and insecure) workaround seems to me in adding these lines to index.php (due to Issue #37467)

```
if ($_SERVER['X-Forwarded-Proto'] == 'https') {
    $_SERVER['HTTPS'] = 'on';
}
```

#11 - 2013-07-18 19:36 - Helmut Hummel

Christian Ludwig wrote:

> Adding a hook (only) seems to me more risky because there will be an extension soon, that handles HTTP_X_FORWARDED_PROTO without any extra checks. And this will make TYPO3 more insecure than offering the right solution with the core (and making such an extension dispensable).

I totally agree!

> At the moment the only dirty (and insecure) workaround seems to me in adding these lines to index.php (due to Issue #37467)

You can simply configure your web server correctly for example like this in case it's an apache with mod_env:

```
SetEnvIf HTTP_X_FORWARDED_PROTO "^https$" HTTPS=on
SetEnvIf HTTP_X_FORWARDED_PROTO "^http$" HTTPS=off
```

All problems solved transparently for all applications in this virtual host configuration. Ano specific patch or software needed. The idea to do it this way is mentioned in the abandoned patch : http://www.fabrizio-branca.de/nginx-varnish-apache-magento-typo3.html

> Please see my comment at https://review.typo3.org/#/c/4913/ on how to make this patch secure!

your suggestion does not make anything more secure. The reason is that it cannot be reliably secured on application level in such a scenario because the terminating proxy **must** set the HTTP_X_FORWARDED_PROTO header for every request making sure to overwrite all requested variants (case insensitively). If that is not the case, the application can be tricked to act like a https request has been sent.

We decided to not handle this scenario on application side (TYPO3) because:

1. It can be more elegantly solved with server configuration
2. It would introduce unneeded complexity (getIndpEnv already is too complex which leads to bugs you mentioned above)
3. Leave all configuration for such a scenario in one "domain" which is the domain of the server admin. This makes the bahviour clearer and avoids misunderstandings between people of different domains.

But I agree that we should add this to our documentation. Feel free to add a ticket in the according tracker and contribute different configurations for different web servers running TYPO3 (e.g. Nginx)

Hope that makes the reasoning a bit clearer. Feel free to add further comments. Thank you.

#12 - 2013-09-11 16:46 - Philipp Müller

Hi Helmut

The "SetEnvIf"-solution does not run with fcgi and suexec (http://bit.ly/14LtRMH). That means we need any other solution, maybe in TYPO3. You have an idea?

Philipp

#13 - 2013-09-13 16:32 - Michael Stucki

- Is Regression set to No

Hi Philipp,

> The "SetEnvIf"-solution does not run with fcgi and suexec (http://bit.ly/14LtRMH). That means we need any other solution, maybe in TYPO3. You have an idea?

Try this instead:

```
SetEnvIf X-Forwarded-Proto "^https$" HTTPS=on
```

I prefer to refer to the port instead (needs nginx adjustment):

```
SetEnvIf X-Forwarded-Port "443" HTTPS=on
```

#14 - 2017-08-12 10:13 - Sybille Peters

- Related to Bug #81837: SSL mixed content issues in backend when HTTPS server var is not set added

#15 - 2018-09-21 09:15 - Susanne Moog

- Related to Bug #86264: Trusted hosts pattern mismatch with Nginx and HTTP_X_FORWARDED_PORT 443 added

#16 - 2020-09-03 21:22 - Christian Kuhn

- Related to Bug #92187: HTTP/HTTPS not correctly determined behind reverseProxy added