XOOPS 2.0.10 BETA Released - XOOPS

NEWS_PDF_AUTHOR: Mithrandir

NEWS_PDF_DATE: 2005/3/26 15:39:57

The XOOPS Core Development Team brings you a beta version of the next step in XOOPS Development.

XOOPS version 2.0.10 beta is a security-improving release that lessens the use of fopen with URLs and brings a completely new tool for securing modules against CSRF attacks: The XoopsSecurity class.

This is just a beta for now, since the token system still needs some testing, but provided we get enough positive feedback, a final 2.0.10 release should be released within 1-2 weeks.

This release contains files for the core-included versions of News and Newbb (1.1 and 1, respectively). If you use Newbb 2 and/or News 1.2 or later, you should not upload the files in modules/news and modules/newbb as they will mess up these modules.

Xoops 2.0.10 Beta Full (.tar.gz)
Xoops 2.0.10 Beta Full (.zip)
Xoops 2.0.9.3 to 2.0.10 Beta Patch (.tar.gz)
Xoops 2.0.9.3 to 2.0.10 Beta Patch (.zip)

====
XoopsSecurity
====
The new class for handling security handles some routines including checking the HTTP REFERER and global variable contamination by request parameters.

It also introduces a token system for securing forms against CSRF attacks.

How does it work?
The token system is used in conjunction with input forms, where it generates a unique and practically un-guessable value that is saved in the user's session and as a hidden variable in the form. When the form is submitted, the receiving page can check if the token value provided via the form is also in the user's session. If not, the check will fail.

How do I use this in my module?
Depending on your module's implementation, there are several ways to implement the token system:

Form side
1) Add a 5th parameter to the XoopsForm-derived class constructor - true for adding a token and false (default) for not using the token system in this form

2) If not using XoopsForm classes but writing HTML directly in a PHP file or Smarty template, one can get the HTML for a token field with $GLOBALS['xoopsSecurity']->getTokenHTML() - this will return the result of a XoopsFormHiddenToken::render() call, ready to be used in a PHP file or assigned to $xoopsTpl for use in a template

Receiving side
On the receiving end, one must check the validity of the token by calling $GLOBALS['xoopsSecurity']->check() - which returns true or false - before authorising changes to the database or similar actions.

When should I use this?
You should use the token system whenever you have a form that makes changes to the database. Especially if the form is only available to certain privileged users.

I'm using module xxx on my site, it doesn't use tokens. Is it unsafe?
Not directly, no, although there is some discussion in this area (which is why we are making this token system altogether). If you are checking the HTTP REFERER (which XOOPS does by default) you are quite safe from the malicious attacks where your site admins are tricked into performing actions on your site by submitting forms on another site. However, checking the HTTP REFERER is not entirely friendly towards your users, who may have to configure their firewall for your site. The token system makes your site less vulnerable should you decide to disable the referer checking.

Who should I thank for making my XOOPS more secure
The Japanese XOOPS community should be the target for your praise, flowers, chocolate and whatever else, you would want to send their way.

The XOOPS Core Development Team brings you a beta version of the next step in XOOPS Development.

XOOPS version 2.0.10 beta is a security-improving release that lessens the use of fopen with URLs and brings a completely new tool for securing modules against CSRF attacks: The XoopsSecurity class.

This is just a beta for now, since the token system still needs some testing, but provided we get enough positive feedback, a final 2.0.10 release should be released within 1-2 weeks.

This release contains files for the core-included versions of News and Newbb (1.1 and 1, respectively). If you use Newbb 2 and/or News 1.2 or later, you should not upload the files in modules/news and modules/newbb as they will mess up these modules.

Xoops 2.0.10 Beta Full (.tar.gz)
Xoops 2.0.10 Beta Full (.zip)
Xoops 2.0.9.3 to 2.0.10 Beta Patch (.tar.gz)
Xoops 2.0.9.3 to 2.0.10 Beta Patch (.zip)

====
XoopsSecurity
====
The new class for handling security handles some routines including checking the HTTP REFERER and global variable contamination by request parameters.

It also introduces a token system for securing forms against CSRF attacks.

How does it work?
The token system is used in conjunction with input forms, where it generates a unique and practically un-guessable value that is saved in the user's session and as a hidden variable in the form. When the form is submitted, the receiving page can check if the token value provided via the form is also in the user's session. If not, the check will fail.

How do I use this in my module?
Depending on your module's implementation, there are several ways to implement the token system:

Form side
1) Add a 5th parameter to the XoopsForm-derived class constructor - true for adding a token and false (default) for not using the token system in this form

2) If not using XoopsForm classes but writing HTML directly in a PHP file or Smarty template, one can get the HTML for a token field with $GLOBALS['xoopsSecurity']->getTokenHTML() - this will return the result of a XoopsFormHiddenToken::render() call, ready to be used in a PHP

file or assigned to $xoopsTpl for use in a template

Receiving side
On the receiving end, one must check the validity of the token by calling $GLOBALS['xoopsSecurity']->check() - which returns true or false - before authorising changes to the database or similar actions.

When should I use this?
You should use the token system whenever you have a form that makes changes to the database. Especially if the form is only available to certain privileged users.

I'm using module xxx on my site, it doesn't use tokens. Is it unsafe?
Not directly, no, although there is some discussion in this area (which is why we are making this token system altogether). If you are checking the HTTP REFERER (which XOOPS does by default) you are quite safe from the malicious attacks where your site admins are tricked into performing actions on your site by submitting forms on another site. However, checking the HTTP REFERER is not entirely friendly towards your users, who may have to configure their firewall for your site. The token system makes your site less vulnerable should you decide to disable the referer checking.

Who should I thank for making my XOOPS more secure
The Japanese XOOPS community should be the target for your praise, flowers, chocolate and whatever else, you would want to send their way.