WF-Sections V2: New Exploits and Security Issues (Users MUST READ this) - Security

NEWS_PDF_AUTHOR: Mamba

NEWS_PDF_DATE: 2008/4/15 8:00:00

As always, XOOPS developers are committed to ensuring the highest security of XOOPS code. The message below comes from Catzwolf:

Quote:

> If you are still using WF-Sections v1+ and v2+ then I suggest that you read this please.
>
> It has come to my attention that there is a few very bad security exploits that some people could use to gain access to your website. I suggest that all users of this module should either:
>
> 1. Deactivate the module for the time being (recommended) or..
> 2. Renaming XOOPS_ROOT_PATH/modules/wfsections/ratefile.php and print.php.
>
> I am now in the process of doing a full audit of all the WF-Sections code and closing these and all possible security risks that may arise in the future.
>
> I will keep you all posted on an update.
>
> John (AkA Catzwolf)

To follow the story, please visit our discussion Forum.

As always, XOOPS developers are committed to ensuring the highest security of XOOPS code. The message below comes from Catzwolf:

Quote:

> If you are still using WF-Sections v1+ and v2+ then I suggest that you read this please.
>
> It has come to my attention that there is a few very bad security exploits that some people could use to gain access to your website. I suggest that all users of this module should either:
>
> 1. Deactivate the module for the time being (recommended) or..
> 2. Renaming XOOPS_ROOT_PATH/modules/wfsections/ratefile.php and print.php.
>
> I am now in the process of doing a full audit of all the WF-Sections code and closing these and all possible security risks that may arise in the future.
>
> I will keep you all posted on an update.
>
> John (AkA Catzwolf)

To follow the story, please visit our discussion Forum.