

Joomla! Security: Avoid Getting Hacked

Northern Virginia Joomla Users Group

April 21, 2016

Dorothy Firsching, Ursa Major Consulting, LLC

dfirsching@ursamajorconsulting.com

Agenda

- Joomla! News and Plans
 - Joomla! Updates
 - Joomla! Certification
 - Our JUG
- How to Avoid Getting Hacked

Joomla! News

- Joomla! 3.5 bug regarding e-mails
 - Joomla! will fail catastrophically when trying to send an email, including from Akeeba
 - If the From Email or From Name in Global Configuration are Empty
 - Invalid e-mail addresses in user accounts
- <https://www.akeebabackup.com/home/news/1664-major-joomla-3-5-bug-regarding-e-mails.html>

Joomla! 3.6+ plans

- ❑ As of 4/16/2016:
- ❑ Features currently being worked on:
 - Custom Fields (Allon Moritz): progressing well, can use testing
 - New media manager: needs testing
 - New router (Hannes Papenberg): ready for testing
 - Service layer (Chris Davenport): probably later
 - Web services (Chris Davenport): probably in 3.7
 - Mobile app (Matias Aguirre): not sure of status
 - Admin template (Cliff Pfeifer): scheduled for 3.7
- ❑ Tentative aim: Late June 2016 for at least some features (depends when ready)
- ❑ See Google Joomla! CMS Development group for latest
- ❑ Alpha release soon

Joomla! Certification

□ Joomla! Certification

- Establish a standard
- Ensure competence and develop a qualified workforce
- Provide a documented measurement of knowledge
- Important role in choosing a Joomla! service provider

□ First certification: Joomla! 3.x Administrator

- The badge received is valid for the lifetime of that major version that it covers
- Computer based, 60 questions - 90 minutes, multiple choice, in US \$75
- How to Prepare:
<https://certification.joomla.org/exams/joomla-administrator>
- Where:
At a JLP, Joomla!Day, or JUG

□ Our JUG

- Application to administer certification test is pending our certification as a JUG
- Need to submit photo of testing location and names of proctors / supervisors
for testing

Our JUG Status

- ❑ New website at www.novajoomla.com
 - Register or update your listing in the members directory!
- ❑ JUG was dropped by Joomla! But now re-approved.
 - <http://community.joomla.org/user-groups/north-america/united-states/virginia.html> "Joomla! Community Portal"
 - There are now no JUGs in Virginia
 - Wanted us to change our name to include a city, e.g., Fairfax or Kings Park, and not a state. Answered: No. We are officially organized in Virginia with that name and have IRS tax exempt 501(c)(6) status!
 - Wanted us to create a new logo that does not include the clover Joomla! logo
 - It is OK now, under "fair use".

Upcoming NoVA JUG events

- ❑ May 19, 2016: Steve Burge, Best Joomla! Tips and Techniques
- ❑ June 16 – open
- ❑ July 21 – open
- ❑ What would you like to present or hear about?

Other Upcoming Joomla Events

- New York: May 15, 2016
 - JoomlaCamp 2016
 - Joomlausersnj.com
- Minneapolis: July 17-18, 2016
Web and Marketing Conference
 - 2 days, at Mall of America
 - www.joomladay.mn
- Denver: October 1, 2016
- Chicago: September 17, 2016
 - Joomladaychicago.com

How to Avoid Getting Hacked

1. Update Joomla! to Current Version

- Outdated Joomla! 2.5.14, 3.5.1 code allow anybody to upload php scripts to your site via media manager.
- Remote code execution vulnerability: all versions up to 3.4.5 (December 15, 2015)

2. Upgrade Extensions

- Upgrade extensions all the time
- Use Tools like managemyjoomla.com or watchful.li

How to Avoid Getting Hacked

3. Upgrade Templates

- Templates, modules, frameworks
- E.g., RocketTheme SQL injection in sliders affected several hundred templates

4. Avoid Weak passwords

- Brute force attacks break weak passwords, e.g., pass123
- Change username from "admin" or "admin2"
- Allow access only from certain IP addresses
- Password protect the administrator folder
- Use secret URL parameters (Akeeba Admin Tools)

How to Avoid Getting Hacked

5. Avoid Outdated or Poorly Configured Server Software

- Php before 5.3.12, running as CGI: remote execution exploit
 - Can see the passwords, etc. in configuration.php
- Apache Symlinks Bug: Lets Hackers access other accounts on shared servers
 - add `SymLinksIfOwnerMatch` to `.htaccess`

How to Avoid Getting Hacked

6. Check for Bad File Permissions

- 755 for folders
- 644 for files
- Use Akeeba Admin Tools to Fix

7. Have account isolation!

- Watch out for test accounts and update or remove them, too!

8. Keep Malware off Your PC

How to Avoid Getting Hacked

9. Configure Akeeba Admin Tools to Harden Joomla!

- Restrict editing user accounts
- Creating a custom .htaccess to stop various login and hack attempts
- Email you upon successful/unsuccessful administrator logins
- Etc.

How to Avoid Getting Hacked

10. Scan for File Changes

- PHP file scanner in Akeeba Admintools

11. Scan for Hacks

- Managemyjoomla.com
- Check for good practices you forgot
- Scan for potential hacks
- Update or remove bad files
- Manage extensions
- Schedule backups

Try a Content Delivery Network (CDN)

- ❑ <http://myawesomejoomlawebsite.com/the-complete-guide-to-using-cloudflare-with-joomla.html>
- ❑ A CDN can handle IP blocking also
- ❑ (Note: added by Thomas at the meeting)

Set up your site to use SSL

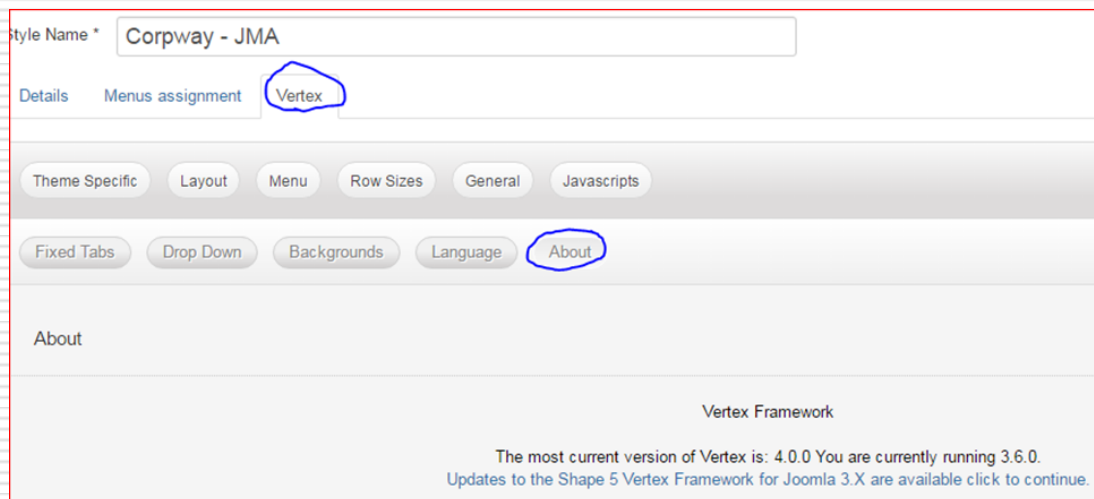
- ❑ Note that Google gives ranking preference to sites using SSL
- ❑ <https://www.simbunch.com/products/free-extensions/cloudflare-for-joomla>
- ❑ Or investigate getting your own certificate
- ❑ (Note: added by Thomas at the meeting)

Read Joomla! Security News

- ❑ [https://docs.joomla.org/Security Checklist](https://docs.joomla.org/Security_Checklist)
- ❑ <http://feeds.joomla.org/JoomlaSecurityNews>
- ❑ <http://feeds.joomla.org/JoomlaSecurityVulnerableExtensions>
- ❑ Sucuri:
- ❑ <Http://blog.sucuri.net/?s=joomla>

Example of Template Framework Update: Shape5


- ❑ Template Framework is Vertex
- ❑ Current Version may be hard to notice on existing templates



Shape5 Vertex Upgrade

- ❑ Log in and download the upgrade patch.
http://www.shape5.com/component/option,com_docman/Itemid,96/task,cat_view/gid,307/
 - Extract the files
 - Upload the extracted files and folders to the template's root folder.
 - Go to Extensions/Template Manager and then open your templates configuration link. Save any changes that you wish and the upgrade is complete!
 - Don't overlay Yourtemplate/index.php – adjust positions
 - Don't overlay css/custom.css – adjust css
- ❑ Much easier to forget to do, if it does not appear in the control panel!
- ❑ Why isn't this using the Joomla! upgrade process?

Upgrade to Widgetkit Current Version? Potential Pitfall...



The screenshot shows the Yootheme website interface. At the top right, there is a user profile for 'dorothy.firsching' with a 'Logout' link and a shopping cart icon showing '€0,00 (0 Items)'. Below this is a navigation menu with links for 'Themes', 'Widgetkit', 'ZOO', 'Icons', 'Support', 'Company', and 'Blog'. The 'Widgetkit' link is highlighted. Below the navigation, there are links for 'Demo', 'Downloads', 'Documentation', and a blue 'Buy Now' button. The main content area is titled 'How to Migrate from Widgetkit 1' and contains the following text:

Widgetkit 2 has a new approach to widget management compared to Widgetkit 1. Content and widgets have been decoupled completely, which resulted in a new back end. That is why there is no possible upgrade path from Widgetkit 1.x to Widgetkit 2.

Unfortunately, it is also NOT possible to run both Widgetkit 1.x and 2 at the same time. You have to decide which version you want to use. If you are satisfied with Widgetkit 1.x, there is no need to move to the new version. If you start with a new site, we recommend using Widgetkit 2.

If you still want or need to migrate your content from Widgetkit 1.x to 2, a possible solution is to get a full dump of your current website on your local system. There you can remove Widgetkit 1, install the new version and recreate your widgets one by one. When you are done, you can update the online version with your prepared offline version. That way, you limit downtime of your live site to a minimum.

Note that the best upgrade for Joomla! 3.x is called widgetkit_j25.zip!

Widgetkit_j25.zip does run on Joomla! 3.x despite its name.
Widgetkit_2.6.5_j3.zip is "Widgetkit 2". You can't run both.

Discussion
