Joomla Security Basics

SIMPLE TIPS AND ADVICE FOR RUNNING SECURE JOOMLA WEBSITES

PRESENTED BY: NICK MARTINELLI
@SHREDDEMON
NICK.MARTINELLI@SOURCEBOOKS.COM
JUNE 2013 @ JOOMLA CHICAGO PALATINE

Who, What, Why

- You don't have to be a server admin or have a deep knowledge of web servers to run secure Joomla sites
- We'll cover basic knowledge that you can go back to work today and start applying
- Keep your website safe and protected from nefarious people and malicious software

Why take security seriously?

- The obvious…
  - Cleanup from an intrusion can be a headache and time consuming
  - Cause you grief from clients
  - Hurt you or your clients brand
  - Ever heard of credit card or personal data theft?
  - Repercussions: Loss of trust, PR nightmare, $$$ fines
  - Customers computers could be infected with viruses directly from your website
  - If you don't take it seriously you could lose work easily

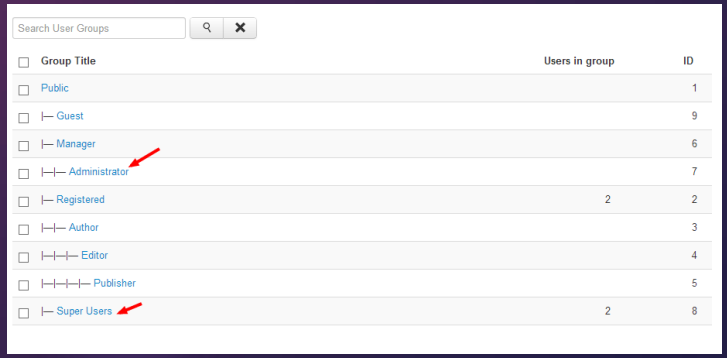
Scared a little… You should be!

Recent real world example

- Drupal.org hacked!
  - Due to a vulnerability from third-party software installed on the Drupal.org server infrastructure, and was not the result of a vulnerability within Drupal itself.
  - Information exposed included usernames, email addresses, and country information, as well as hashed passwords.
  - https://drupal.org/news/130529SecurityUpdate

User Basics

- Limit the amount of Joomla super admins and 2nd level admins
- Only give users that need Super and admin rights that privilege
- Super Administrators have full control over Joomla
- Administrators cannot change, edit or install Site Templates or make any changes to the sites Global configuration options. Some extensions might limit configuration options as well. Treats as publishers on the front end



User Basics Continued…

- Take advantage of Joomla ACL levels
- Create business roles that match up with ACL groups to restrict who has access to what controls
- Great explanation of Joomla ACL Groups: http://docs.joomla.org/User_Group_Access_levels_explained_in_simple_terms
- Globally disable the text editor, manually assign text editor to the user account itself

Passwords

- Use strong passwords!!!
- The more random the better
- Avoid using plain English words
- Avoid keystroke patterns (circles, squares, etc)
- Mix case, numbers and special characters
- More than 8 characters
- Bad password example: bella47
- Strong password example: !j0m$06o13%$#
- Use a random password generator tool.
  - CPanel has random password generator tool that can be used when creating user accounts

Passwords Continued…

- Cpanel, FTP and MySql accounts passwords should use a minimum of 12 characters (more is better). You should have to cut and paste them in because they are difficult to recall!
- Joomla Super admin and administrator accounts should have extremely difficult passwords. Follow strong password rules when installing Joomla from the start
- The harder the password schema the more difficult time hackers and brute force tool to crack in
- Be smart about storing your passwords locally. Avoid plain text files or word docs.
- Keep your passwords secure by using an encrypted password database like KeePass www.keepass.info
- Never give out passwords over Skype or instant messengers
- When emailing clients, create password protected documents or use drop box (remove files after transfer). Send two part emails with login credentials
- Only provide your hosting company passwords via help desk systems
- Password protect dev enviroments i.e. www.site.com/dev

MySQL Security Tips

- Use strong passwords for user accounts
- Get creative with database names
  - Bad database name: joomla31
  - Good example: sourceprod, sourcedev
- Use random table name prefixes
  - Bad table prefix: joomla_, jom_
  - Good examples: source_, prod_, dev1_
- Newer versions of Joomla installer created random table prefixes
- Protects from injections that target generic Joomla tables

Patching Joomla

- Keep Joomla sites updated at all times
- Don't let your site go unpatched for an extended period of time
- Patch regularly
- If you don't you run the risk of being susceptible to known security exploits
- Patching tip: Wait a couple days after a patch is released. There have been buggy patches released in the past. ALWAYS BACKUP FIRST!

Helpful Links:

- http://feeds.joomla.org/JoomlaSecurityNews
- http://developer.joomla.org/security.html
- http://www.joomla.org

Joomla Extensions

- Keep extensions updated as possible
- Joomla core extensions will get patched with regular releases
- Update 3rd party extensions often
  - Including: Components, Plugins, Modules and templates
    - Examples: RS Form, sh404SEF, EasyBlog, gantry template framework
- Not only will you get new features, but security fixes and enhancements might also go along with it
- Get on developer email lists to be notified of new releases. A sign of a good developer is one who communicates with customers often.

Helpful Vulnerability Links

Helpful Links:

- http://feeds.joomla.org/JoomlaSecurityNews
- http://developer.joomla.org/security.html
- http://feeds.joomla.org/JoomlaSecurityVulnerableExtensions
- **http://secunia.com/search/?search=joomla**
- http://www.frsirt.com/english/
- **http://www.milw0rm.com/**

Global Configuration

- Set "Show Joomla Version" = Off
  - No need to advertise what you're running in meta tags
  - Also make sure your templates meta tags don't blurt out what you're using either.
- Set default editor to none (control editor at user level)
- Disable Joomla FTP layer. Its only for hosts with challenging setups.
- Enable SEF Urls using .htaccess (preferred without /index.php/)
- Helpful link http://docs.joomla.org/J3.1:Global_configuration

Obtaining Extensions

Common sense approach – DON'T BE A PIRATE!

- Never torrent Joomla extensions or templates
  - Just asking for files to be infected with malware
- Avoid websites claiming to sell cheap Joomla software!
  - Software is being sold without knowledge or approval of developers
- Trustworthy developers don't distribute their software through other sites.
- It will end up costing you more in the long run to recover from corrupted and infected software.
- Your hurting the community you are thriving from
- Stick with extensions listed on extensions.joomla.org.

Public Service Announcement

- Avoid www.joomlacheap.net
- They are reselling stolen extensions at a deep discount and not sharing a cent with original developers
- They are using developer's branding to build up your trust and fool you.
- Tell them how you feel on twitter @Joomlacheap and lets spread the word

SEF URLS

- SEF urls add a great layer of protection to Joomla
- Hides the long query string thus adding an extra layer of security
- Use in conjunction with .htaccess
- Avoid /index.php/ in the url
- SEO benefits
- Core SEF urls are ok for smaller sites
- Recommend sh404SEF for more freedom over url structure

Hosting

- Stick with reputable hosts. Cheapest isn't always the best and most secure
- Make sure you can actually call someone, online only help can be challenging in an emergency situation
- Request a list of their server hardening techniques
  - Ask what firewall's they have in place as far as hardware and also software firewall layers at the server level.
  - Are they using a software firewall like ConfigServer
  - Ask if use protection like cphulk (brute force attack protection) and suPHP (hosting account permission control)
- Use php version 5.3+
- Helpful Link: http://www.webhostingtalk.com/ - Community website for reviews and forums about hosting companies and technology

Firewalls within Joomla

- Add your own software firewall into Joomla itself
- Good choices:
  - sh404SEF – has a built in security layer with honey pot support. Also logs hack attempts http://anything-digital.com/sh404sef/seo-analytics-and-security-for-joomla.html
  - JomDefender – remove joomla identifiers from code, backend IP ban/blocking, extra admin login page and more http://www.corephp.com/joomla-products/jomdefender.html
  - RS Firewall – permission checker, password protect admin folder, block brute force attacks, database checks and moer. http://www.rsjoomla.com/joomla-extensions/joomla-security.html
  - Akeeba Admin tools, application firewall, block lists, permission checks, honeypot support and more https://www.akeebabackup.com/products/admin-tools.html
  - HoneyPot – real time RBL (real-time black list of IPS) http://extensions.joomla.org/extensions/access-a-security/site-security/site-protection/17919

File Permissions

- Folders 755
- Files 644
- Configuration.php 640
- Never have 777 that's full access
- Ask your host to run a perm check to make sure files and folders are set to the right permissions. They should be able to run a script and set a global server parameter to ensure files are set that way.
- If a host doesn't follow those parameters…RUN AWAY!

Use .htaccess and SSL

- Joomla provide some basic exploit blocks inside .htacccess
- Can add other rules to block bad bots

- Secure pages that pass personal information
  - Login
  - Account management pages
  - Components that have access to sensitive data
  - Ecommerce

Backups / DR

- Create a backup schedule. Daily, weekly, monthly.
- Off load backups to multiple locations
  - Local with redundancy or cloud
- Use Joomla based tools like Akeeba Backup or Xcloner to create off-site backups
- Create a DR plan and test it quarterly
- Some hosts offer online backups like R1Soft. Be sure to be aware of the frequency and how long they store backups for.
- Perform restore tests to ensure your backups are working
  - You need to know if your backups will actually allow you to restore a site quickly

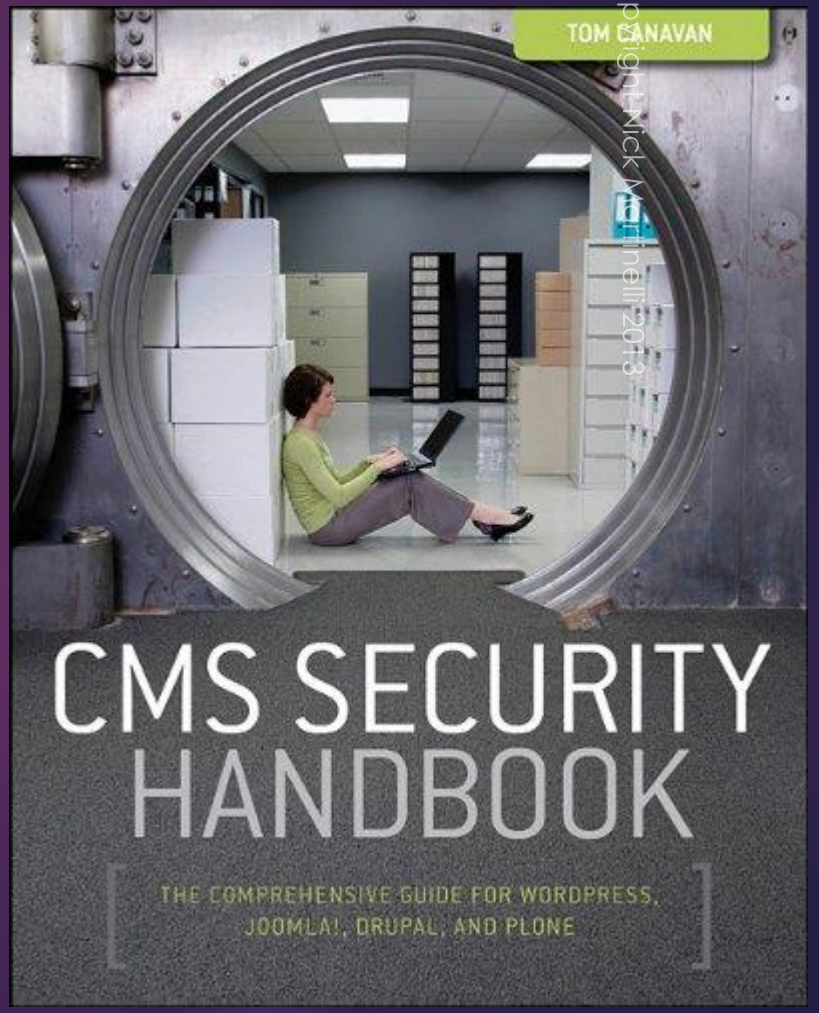
Security Reviews

- Create a review process and perform it regularly
- Monthly / quarterly (depends on your biz needs)
- Document your plan and train your team members to perform
- Patch, Patch, Patch
- Practice restoring sites

Helpful link
http://docs.joomla.org/Joomla_Administrators_Security_Checklist

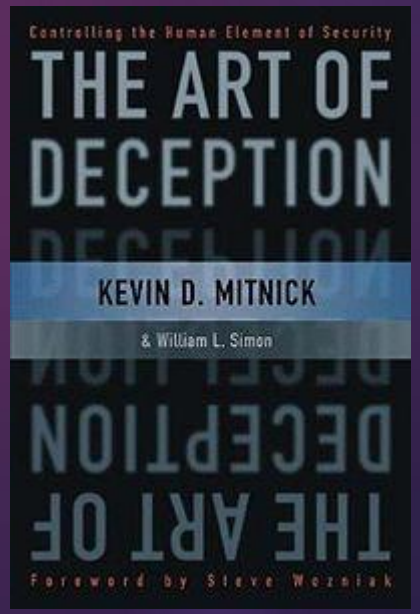
Great Reference Book

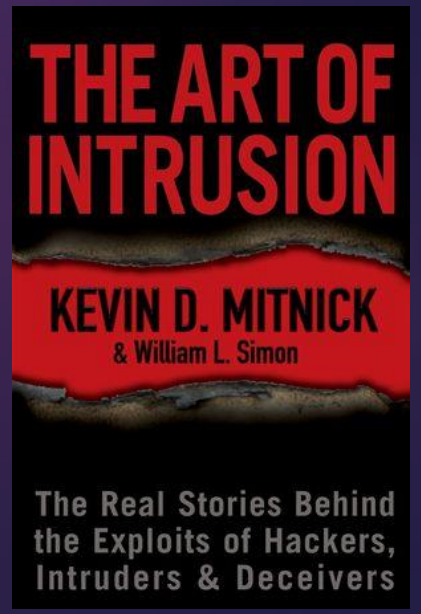
- All in one guide
- Covers hosting, installation security issues, hardening servers against attack, establishing a contingency plan, patching processes, log review, hack recovery, wireless considerations, and infosec policy
- http://www.amazon.com/CMS-Security-Handbook-Comprehensive-WordPress/dp/0470916214



Don’t be socially hacked

- Don’t be a victim of social engineering
- Safeguard sensitive information and passwords
- Be cautious of who and how you give out sensitive information





Final Thoughts

- Patch, Patch, Patch
- Backup and test them often
- Work closely with your host to enforce security
- Safe guard your sensitive info
- Be proactive
- Security is an ongoing process so keep up

```
# ADD the below code to your .htaccess file to block bad bots from accessing your site
# Block Bad bots
RewriteCond %{HTTP_USER_AGENT} ^BlackWidow [OR]
RewriteCond %{HTTP_USER_AGENT} ^Bot\ mailto:craftbot@yahoo.com [OR]
RewriteCond %{HTTP_USER_AGENT} ^ChinaClaw [OR]
RewriteCond %{HTTP_USER_AGENT} ^Custo [OR]
RewriteCond %{HTTP_USER_AGENT} ^DISCo [OR]
RewriteCond %{HTTP_USER_AGENT} ^Download\ Demon [OR]
RewriteCond %{HTTP_USER_AGENT} ^eCatch [OR]
RewriteCond %{HTTP_USER_AGENT} ^EirGrabber [OR]
RewriteCond %{HTTP_USER_AGENT} ^EmailSiphon [OR]
RewriteCond %{HTTP_USER_AGENT} ^EmailWolf [OR]
RewriteCond %{HTTP_USER_AGENT} ^Express\ WebPictures [OR]
RewriteCond %{HTTP_USER_AGENT} ^ExtractorPro [OR]
RewriteCond %{HTTP_USER_AGENT} ^EyeNetIE [OR]
RewriteCond %{HTTP_USER_AGENT} ^FlashGet [OR]
RewriteCond %{HTTP_USER_AGENT} ^GetRight [OR]
RewriteCond %{HTTP_USER_AGENT} ^GetWeb! [OR]
RewriteCond %{HTTP_USER_AGENT} ^Go!Zilla [OR]
RewriteCond %{HTTP_USER_AGENT} ^Go-Ahead-Got-It [OR]
RewriteCond %{HTTP_USER_AGENT} ^GrabNet [OR]
RewriteCond %{HTTP_USER_AGENT} ^Grafula [OR]
RewriteCond %{HTTP_USER_AGENT} ^HMView [OR]
RewriteCond %{HTTP_USER_AGENT} HTTrack [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Image\ Stripper [OR]
RewriteCond %{HTTP_USER_AGENT} ^Image\ Sucker [OR]
RewriteCond %{HTTP_USER_AGENT} Indy\ Library [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^InterGET [OR]
RewriteCond %{HTTP_USER_AGENT} ^Internet\ Ninja [OR]
RewriteCond %{HTTP_USER_AGENT} ^JetCar [OR]
RewriteCond %{HTTP_USER_AGENT} ^JOC\ Web\ Spider [OR]
RewriteCond %{HTTP_USER_AGENT} ^larbin [OR]
RewriteCond %{HTTP_USER_AGENT} ^LeechFTP [OR]
RewriteCond %{HTTP_USER_AGENT} ^Mass\ Downloader [OR]
RewriteCond %{HTTP_USER_AGENT} ^MIDown\ tool [OR]
RewriteCond %{HTTP_USER_AGENT} ^Mister\ PiX [OR]
RewriteCond %{HTTP_USER_AGENT} ^Navroad [OR]
RewriteCond %{HTTP_USER_AGENT} ^NearSite [OR]
RewriteCond %{HTTP_USER_AGENT} ^NetAnts [OR]
RewriteCond %{HTTP_USER_AGENT} ^NetSpider [OR]
RewriteCond %{HTTP_USER_AGENT} ^Net\ Vampire [OR]
RewriteCond %{HTTP_USER_AGENT} ^NetZIP [OR]
RewriteCond %{HTTP_USER_AGENT} ^Octopus [OR]
RewriteCond %{HTTP_USER_AGENT} ^Offline\ Explorer [OR]
RewriteCond %{HTTP_USER_AGENT} ^Offline\ Navigator [OR]
RewriteCond %{HTTP_USER_AGENT} ^PageGrabber [OR]
RewriteCond %{HTTP_USER_AGENT} ^Papa\ Foto [OR]
RewriteCond %{HTTP_USER_AGENT} ^pavuk [OR]
RewriteCond %{HTTP_USER_AGENT} ^pcBrowser [OR]
RewriteCond %{HTTP_USER_AGENT} ^RealDownload [OR]
RewriteCond %{HTTP_USER_AGENT} ^ReGet [OR]
RewriteCond %{HTTP_USER_AGENT} ^SiteSnagger [OR]
RewriteCond %{HTTP_USER_AGENT} ^SmartDownload [OR]
RewriteCond %{HTTP_USER_AGENT} ^SuperBot [OR]
RewriteCond %{HTTP_USER_AGENT} ^SuperHTTP [OR]
RewriteCond %{HTTP_USER_AGENT} ^Surfbot [OR]
RewriteCond %{HTTP_USER_AGENT} ^tAkeOut [OR]
RewriteCond %{HTTP_USER_AGENT} ^Teleport\ Pro [OR]
```

```
RewriteCond %{HTTP_USER_AGENT} ^VoidEYE [OR]
RewriteCond %{HTTP_USER_AGENT} ^Web\ Image\ Collector [OR]
RewriteCond %{HTTP_USER_AGENT} ^Web\ Sucker [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebAuto [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebCopier [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebFetch [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebGo\ IS [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebLeacher [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebReaper [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebSauger [OR]
RewriteCond %{HTTP_USER_AGENT} ^Website\ eXtractor [OR]
RewriteCond %{HTTP_USER_AGENT} ^Website\ Quester [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebStripper [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebWhacker [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebZIP [OR]
RewriteCond %{HTTP_USER_AGENT} ^Widow [OR]
RewriteCond %{HTTP_USER_AGENT} ^WWWOFFLE [OR]
RewriteCond %{HTTP_USER_AGENT} ^Xaldon\ WebSpider [OR]
RewriteCond %{HTTP_USER_AGENT} ^Zeus
RewriteRule ^.* - [F,L]
```