Start typing. This is crowdsourced note-taking!

Mika Epstein - Troubleshooting a Hacked Site

- Profiles/websites:
  - http://ipstenu.org/
  - http://profiles.wordpress.org/ipstenu
  - http://halfelf.org/
  - https://twitter.com/Ipstenu
  - https://www.facebook.com/ipstenu
  - http://www.slideshare.net/Ipstenu
  - https://plus.google.com/115931147765783348497/posts
  -
- Mika works for Dreamhost
- To clean up your site…
  - delete everything, reupload updated files?
  - knowing where to look and what to look for is the first step
- Demo site: http://meetwp.elftest.net
- examples of hacks & explanations http://breakfix.elftest.net
- if you see “base64_decode” in your site, it’s usually not a good thing
- don’t use your real username & pw in wp-config file for db settings
- Hackers will use normal wp filenames or minor variations as filenames for hacked files
- Themes from WP are reviewed and vetted
- If you don’t use a theme/plugin -> Delete it
- shell is important, if your host doesn’t offer it (or worse doesn't know what it is). move
- Don’t be stupid
- Check your DB as well as your files. Often a backdoor will be stored in wp_options - there’s a good guide to that here: http://smackdown.blogsblogsblogs.com/2010/06/14/rackspace-hacked-clients-check-your-databases-wordpress-wp_optimize-backdoor-in-wp_options-table/ (often the option_name is something to do with rss).