Wiki Security

Ofer Shezaf

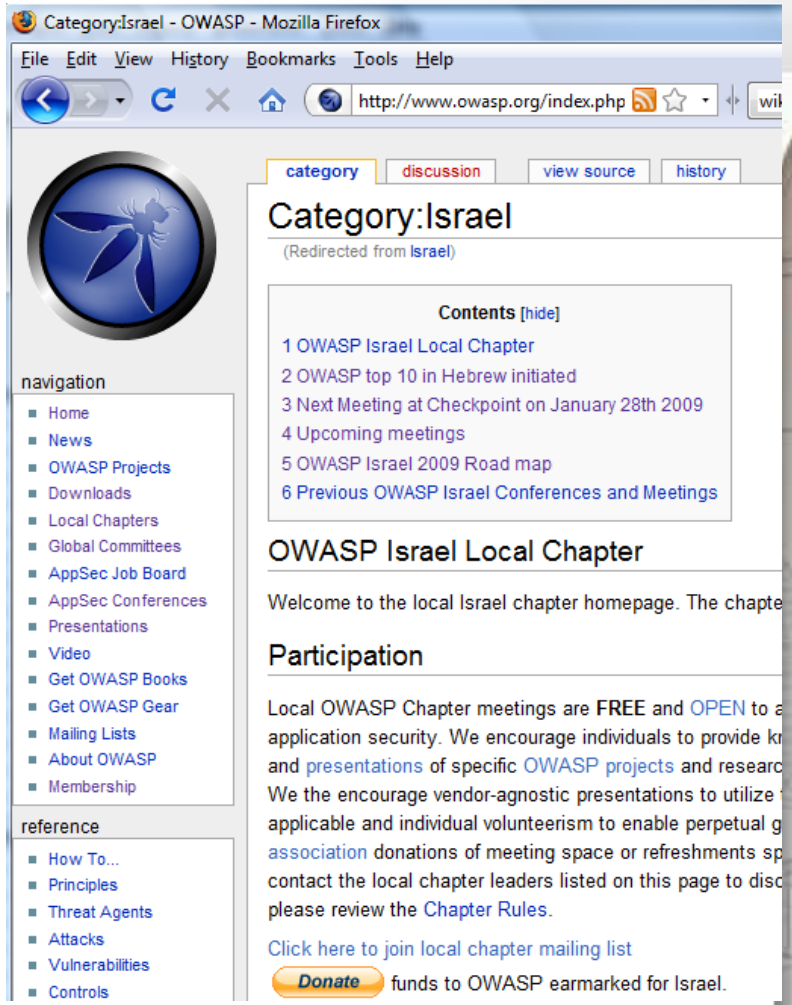
Blog: www.xiom.com,
LinkedIn: https://il.linkedin.com/in/oshezaf

www.xiom.com

About Wiki

Wiki Basics

- A content management system model.
- Most well known for running Wikipedia.
- Used internally by organization for knowledge management.



Wiki Philosophy

A wiki invites all users to create and edit any page.

Wiki promotes associations between different pages.

A wiki is not a carefully crafted site.

Did you know? "Wiki" (/wi:ki:/) is a Hawaiian word for "fast"

Wiki does not have a “delete”!

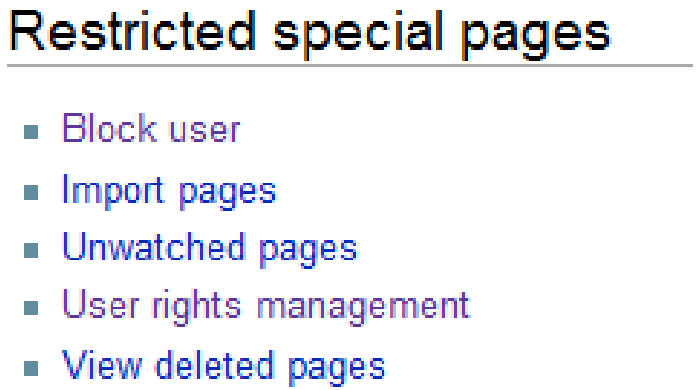
According to Wiki philosophy, “delete” really means that:

- A page should have a different title:
  - Use move.
- The contents should have been placed on a different page:
  - Merge & redirect.
- The contents is already on a different page:
  - Remove content and redirect.
- The page is out-of-date:
  - Re-word as an historical record.

Wiki Security Challenges

Security? Wiki? Are you joking?

- Limited roles and no access control.
- No release workflow process.
- The only “admin” features are:

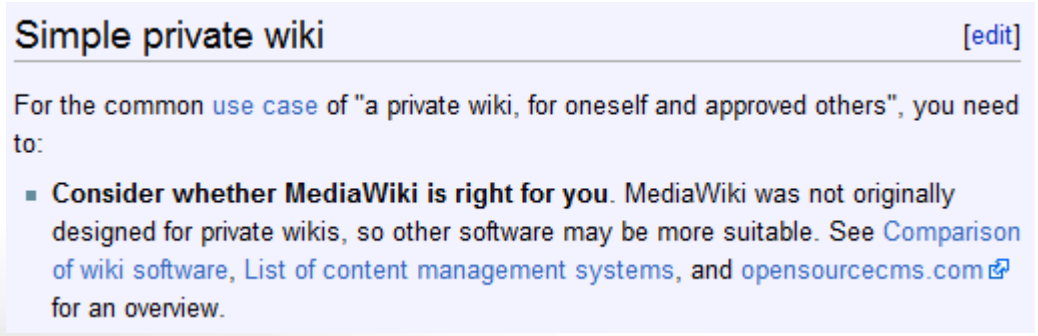


A Different Approach to Security

- Based on trust and audit rather than authorization.
- (Authenticated) users can modify (nearly) every page
- Wiki provides tools to manage these changes:
  - Keeps all versions
  - Enables to easily obtain a diff
  - Enables regressing to any version
  - Discussion page to “talk about this”
- Rudimentary protection provided by:
  - One level authorization with two roles: Administrator and user.
  - Capability to lock certain pages or name spaces
  - Capability to limit pages only to registered user.

Public vs. Private

- Even so, Wikis are used a lot for private groups, for example for corporate wikis.
- The challenge is often departmentalizing – even using some access control tool, many features such as search are not supported.
- There is no turning back. Due to lack of control over content, a top secret Wiki cannot be unclassified.



Simple private wiki [edit]

For the common use case of "a private wiki, for oneself and approved others", you need to:

- **Consider whether MediaWiki is right for you**. MediaWiki was not originally designed for private wikis, so other software may be more suitable. See Comparison of wiki software, List of content management systems, and opensourcecms.com for an overview.

Wiki Security Challenges

- Control over Content:
  - Vandalism and defacement & Fraud
  - Wiki spam
  - Low content quality
- Focus on client side attacks such as XSS as user content is displayed to other users.
- Lack of access control makes stealing of login credentials and session hijacking major problems.
- Extensions - Prone to application layer vulnerabilities.

SOLUTIONS

Authentication

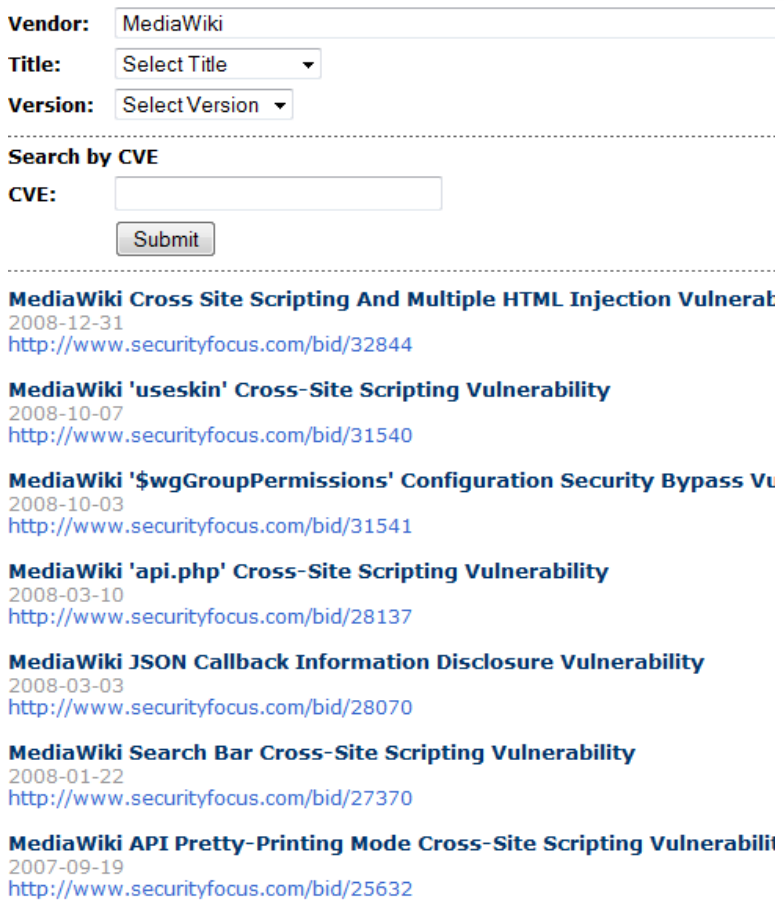
- Ensure password strength
- Force periodical password expiration.
- Consider 2 factor authentication, certainly for administrators.
- Detect and block brute force attacks.
- Usage audit and fraud detection.

Anti Automation

- Avoid defacement & wiki spam.
- Use:
  - Captcha
  - Rate limiting
  - User level fraud and anomaly detection

Hardening & Common Sense

- Host on a different domain to avoid same origin violation risk to your other sites.
- Patch, Patch, Patch. And don’t forger to patch extensions.
- Install ModSecurity.
- Use SSL.



Education

- Explain to users the security limitations and rules regarding content.
- Audit usage and let people know that you caught them.

Ofer Shezaf, shezaf@xiom.com

www.xiom.com