

# Wiki Security

Ofer Shezaf

Blog: [www.xiom.com](http://www.xiom.com),

LinkedIn: <https://il.linkedin.com/in/oshezaf>



[www.xiom.com](http://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.



Category:Israel - OWASP - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.owasp.org/index.php

category discussion view source history

## Category:Israel

(Redirected from Israel)

Contents [hide]

- 1 OWASP Israel Local Chapter
- 2 OWASP top 10 in Hebrew initiated
- 3 Next Meeting at Checkpoint on January 28th 2009
- 4 Upcoming meetings
- 5 OWASP Israel 2009 Road map
- 6 Previous OWASP Israel Conferences and Meetings

### OWASP Israel Local Chapter

Welcome to the local Israel chapter homepage. The chapter is currently in the process of being established.

### Participation

Local OWASP Chapter meetings are **FREE** and **OPEN** to all individuals interested in application security. We encourage individuals to provide knowledge and presentations of specific OWASP projects and research. We encourage vendor-agnostic presentations to utilize applicable and individual volunteerism to enable perpetual growth. We encourage association donations of meeting space or refreshments space. Please contact the local chapter leaders listed on this page to discuss. Please review the [Chapter Rules](#).

[Click here to join local chapter mailing list](#)

[Donate](#) funds to OWASP earmarked for Israel.

navigation

- Home
- News
- OWASP Projects
- Downloads
- Local Chapters
- Global Committees
- AppSec Job Board
- AppSec Conferences
- Presentations
- Video
- Get OWASP Books
- Get OWASP Gear
- Mailing Lists
- About OWASP
- Membership

reference

- How To...
- Principles
- Threat Agents
- Attacks
- Vulnerabilities
- Controls

# 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- ❑ The page is out-of-date: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:

## Restricted special pages

- [Block user](#)
- [Import pages](#)
- [Unwatched pages](#)
- [User rights management](#)
- [View deleted pages](#)

# 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**

[www.xiom.com](http://www.xiom.com)

# 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 forget to patch extensions.
- ❑ Install ModSecurity.
- ❑ Use SSL.

Vendor:

Title:

Version:

---

Search by CVE

CVE:

---

**MediaWiki Cross Site Scripting And Multiple HTML Injection Vulnerability**  
2008-12-31  
<http://www.securityfocus.com/bid/32844>

**MediaWiki 'useskin' Cross-Site Scripting Vulnerability**  
2008-10-07  
<http://www.securityfocus.com/bid/31540>

**MediaWiki '\$wgGroupPermissions' Configuration Security Bypass Vulnerability**  
2008-10-03  
<http://www.securityfocus.com/bid/31541>

**MediaWiki 'api.php' Cross-Site Scripting Vulnerability**  
2008-03-10  
<http://www.securityfocus.com/bid/28137>

**MediaWiki JSON Callback Information Disclosure Vulnerability**  
2008-03-03  
<http://www.securityfocus.com/bid/28070>

**MediaWiki Search Bar Cross-Site Scripting Vulnerability**  
2008-01-22  
<http://www.securityfocus.com/bid/27370>

**MediaWiki API Pretty-Printing Mode Cross-Site Scripting Vulnerability**  
2007-09-19  
<http://www.securityfocus.com/bid/25632>

# Education

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



QUESTIONS  
ANSWERS

Ofer Shezaf, [shezaf@xiom.com](mailto:shezaf@xiom.com)



[www.xiom.com](http://www.xiom.com)