WordPress
Security Implementation Guideline

Good practices and
epic fails of WordPress implementations

OWASP
The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Information Security Consultant
  - Application Security
  - Secure SDLC

Canon®

Dan VASILE

http://www.pentest.ro




dan@pentest.ro

@DanCVasile

Why do I talk about **WordPress**?

OWASP
The Open Web Application Security Project

- I use WordPress
- Previous talk @OWASP Ro InfoSec Conf 2013
- Working with 3rd parties on secure WordPress implementation

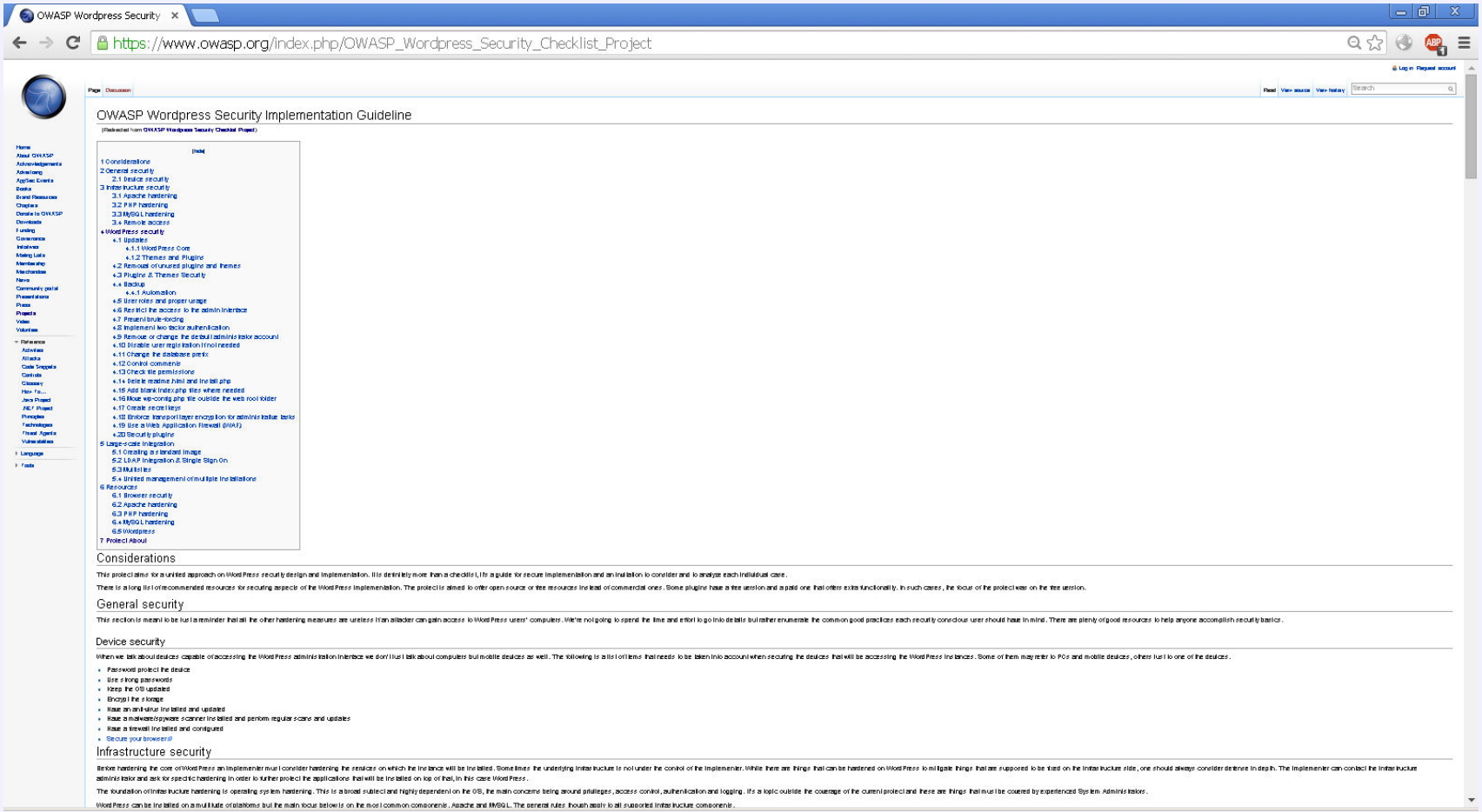
- The project:

WordPress Security Implementation Guideline

Why do I talk about **WordPress**?

OWASP
The Open Web Application Security Project

WordPress Security Implementation Guideline



Scope

OWASP
The Open Web Application Security Project

- Not just WordPress but Open Source adoption
- Framework for secure implementation
- Large scale integration

Scope

OWASP
The Open Web Application Security Project

- General security
- Infrastructure security
- WordPress security
- Large-scale integration

OWASP
The Open Web Application Security Project

- **General security**
- Infrastructure security
- WordPress security
- Large-scale integration

OWASP
The Open Web Application Security Project

General security

OWASP
The Open Web Application Security Project

- General security
- **Infrastructure security**
- WordPress security
- Large-scale integration

OWASP
The Open Web Application Security Project

Infrastructure security

Scope

OWASP
The Open Web Application Security Project

- General security
- Infrastructure security
- **WordPress security**
- Large-scale integration

OWASP
The Open Web Application Security Project

WordPress Security Implementation Guideline

20 subjects

3 main components:

- Core
- Plugins
- Themes

Manual activities & plugin alternatives

OWASP
The Open Web Application Security Project

Updates

3 main types of updates:

- Core
- Minor
- Major

WordPress > v3.7 – automatic updates for Minor

OWASP
The Open Web Application Security Project

Updates

Turn on auto-updates for Major/Core

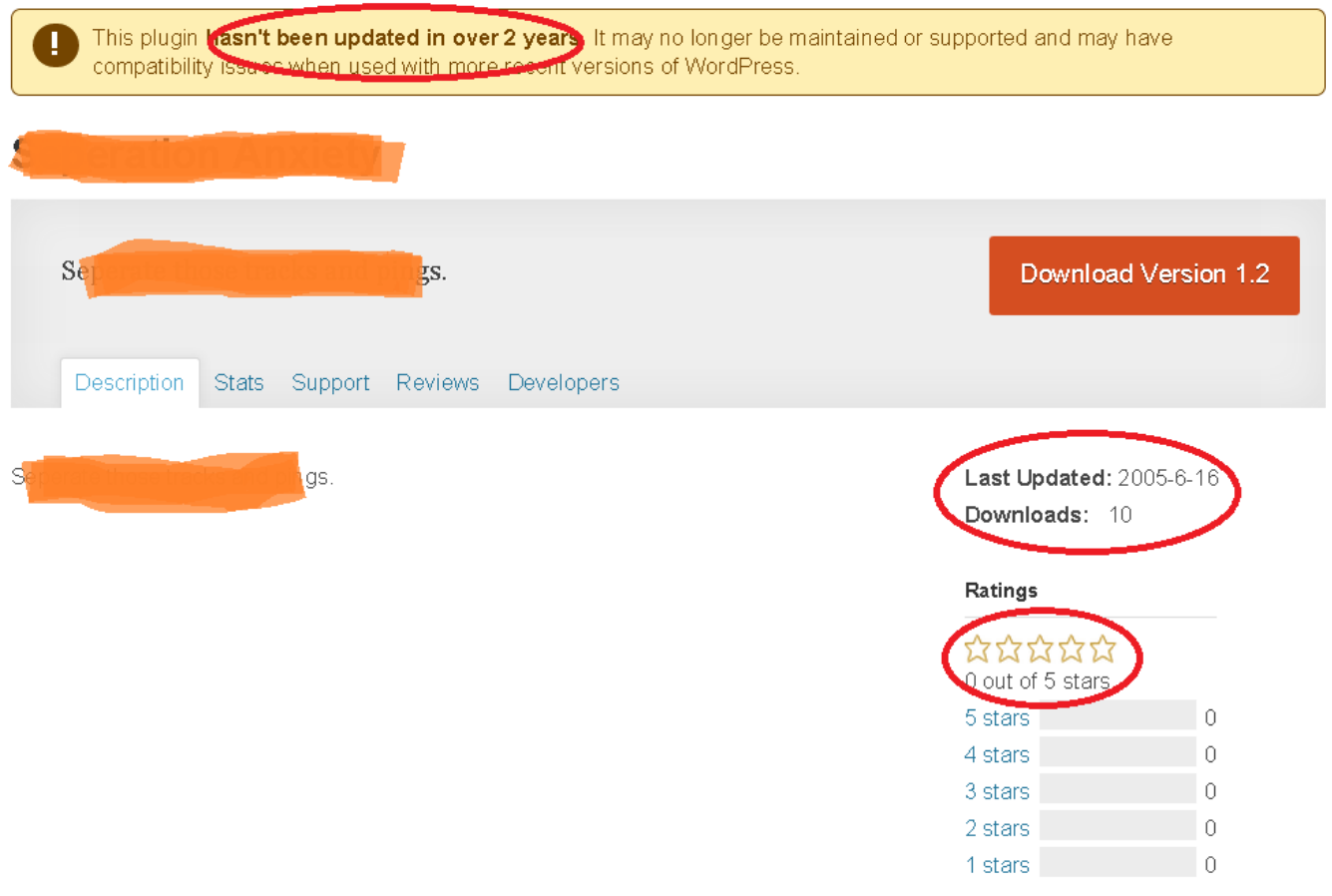
```
define( 'WP_AUTO_UPDATE_CORE', true );
```

For plugins and themes add a filter

```
add_filter( 'auto_update_plugin', '__return_true' );
add_filter( 'auto_update_theme', '__return_true' );
```

OWASP
The Open Web Application Security Project

Choose plugins carefully



OWASP
The Open Web Application Security Project

Backup

What?

- *Files*
  - Core installation, plugins, themes, images & files
- *Database*

How?

Manual vs Automatic

OWASP
The Open Web Application Security Project

Backup horror story 1

The good

- Daily backup, files & database, 365 days retention policy

The bad

- No geographical redundancy, no disaster recovery plan

The ugly

- HDD fail on main machine, faulty HDD on the backup machine
- Missing data and database structure

OWASP
The Open Web Application Security Project

Backup horror story 2

The good

- Proper backup to the cloud

The bad

- Backup credentials stored in clear text

The ugly

- Attacker compromising site and deleting backups

OWASP
The Open Web Application Security Project

User roles

- Super Admin
- Administrator
- Editor
- Author
- Contributor
- Subscriber

OWASP
The Open Web Application Security Project

Restricting access

Sensitive areas of the application must be protected from unauthorized access.

.htaccess

```
Order Deny,Allow
Deny from all
Allow from 127.0.0.1
```

OWASP
The Open Web Application Security Project

Prevent brute-forcing

- Add CAPTCHA
- Blacklist attackers
- Lock accounts

Write a plugin that will lock an account for a predefined period of time after a number of failed attempts.

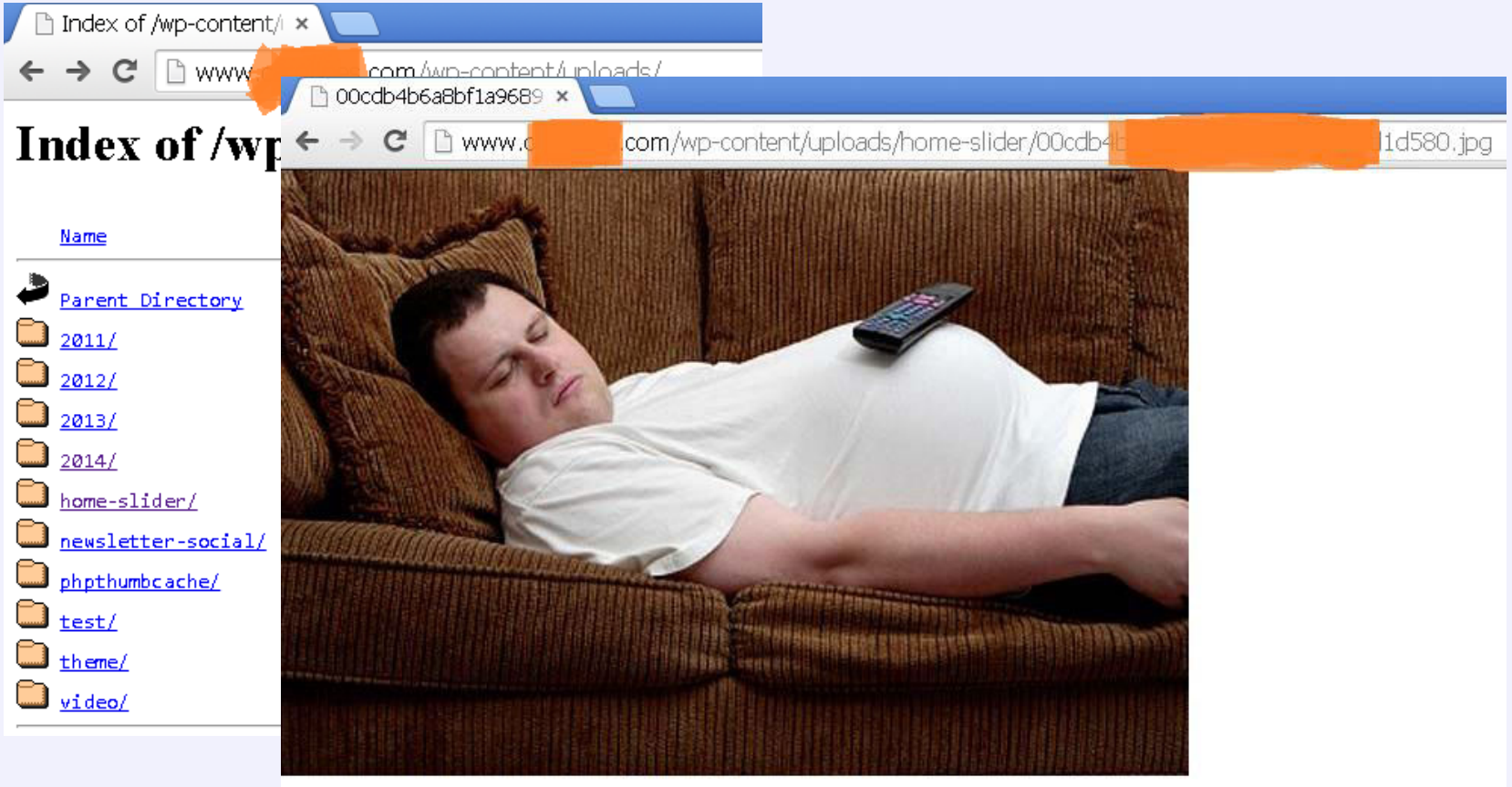
OWASP
The Open Web Application Security Project

Add blank index.php

This should be covered by Apache configuration, but it’s not always the case.

OWASP
The Open Web Application Security Project

Missing blank index.php



OWASP
The Open Web Application Security Project

Force encryption on data in transit

There are cases where both port 80 and 443 are used.

Sensitive operations must use SSL:

```
define('FORCE_SSL_LOGIN', true);
define('FORCE_SSL_ADMIN', true);
```

Scope

OWASP
The Open Web Application Security Project

- General security
- Infrastructure security
- WordPress security
- **Large scale integration**

OWASP
The Open Web Application Security Project

Large scale integration

- Creating a standard image
- LDAP integration & Single Sign On
- Multisites
- Unified management of multiple installations

OWASP
The Open Web Application Security Project

Creating a standard image

- Blank image (no data)
- All the updates
- All the basic shared plugins and themes (&data?)

Purpose:

- Testing ground for new stuff
- Create new instances, secure by default

OWASP
The Open Web Application Security Project

LDAP integration & Single Sign On

- Integration with Active Directory
- Single Sign On (SSO)

Why?

- Centralized user management
- Use existing hierarchy

Multisites

- Built-in WordPress functionality
- End users can create their own sites on demand

Downside

- Shared components (plugins)

OWASP
The Open Web Application Security Project

Unified management of multiple installations

- Self-hosted and cloud solutions

Why?

- Centralized login and management
- Push updates to all instances

OWASP
The Open Web Application Security Project

Next steps

- Contribute to the project

  Wordpress Security Implementation Guideline
- Share the knowledge
- Write secure code for WordPress
- Help others

Q&A

OWASP
The Open Web Application Security Project