Defending Web Applications with PHPSecInfo

Ed Finkler
coj@cerias.purdue.edu

20070320

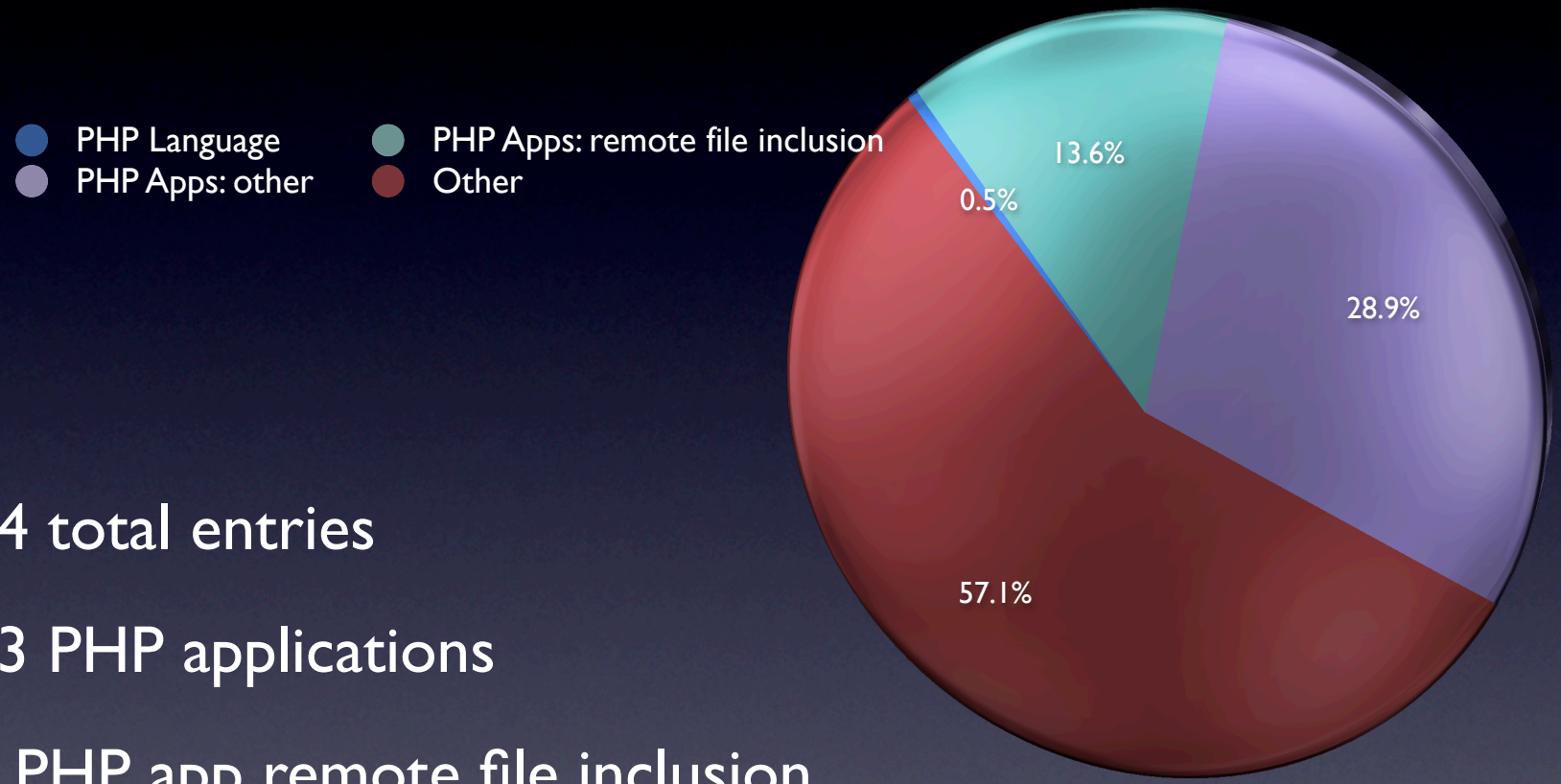
The ubiquity of PHP

- PHP is very, very popular
  - Nearly impossible to find a hosting service that doesn't support PHP in some form
  - About 34% of all domains report using PHP
- PHP is very easy to learn
- PHP provides results quickly
  - Time between setup and seeing results is very short

The ubiquity of PHP

- PHP powers many busy, high-profile sites
  - Wikipedia
  - Facebook
  - Wordpress.com
  - Digg
  - Flickr
  - Yahoo (presentation layer)

NIST NVD: 2006 data



- 6604 total entries
- 2803 PHP applications
- 895 PHP app remote file inclusion
  - Almost blocked by disabling allow_url_fopen

Ed Finkler <coj@cerias.purdue.edu>

What does this mean?

- PHP is very popular
- How much a target web apps are
- How many PHP developers are incapable of writing secure apps
- How many sysadmins don't secure their PHP environments

The parties involved

The System Administrator

The PHP Developer

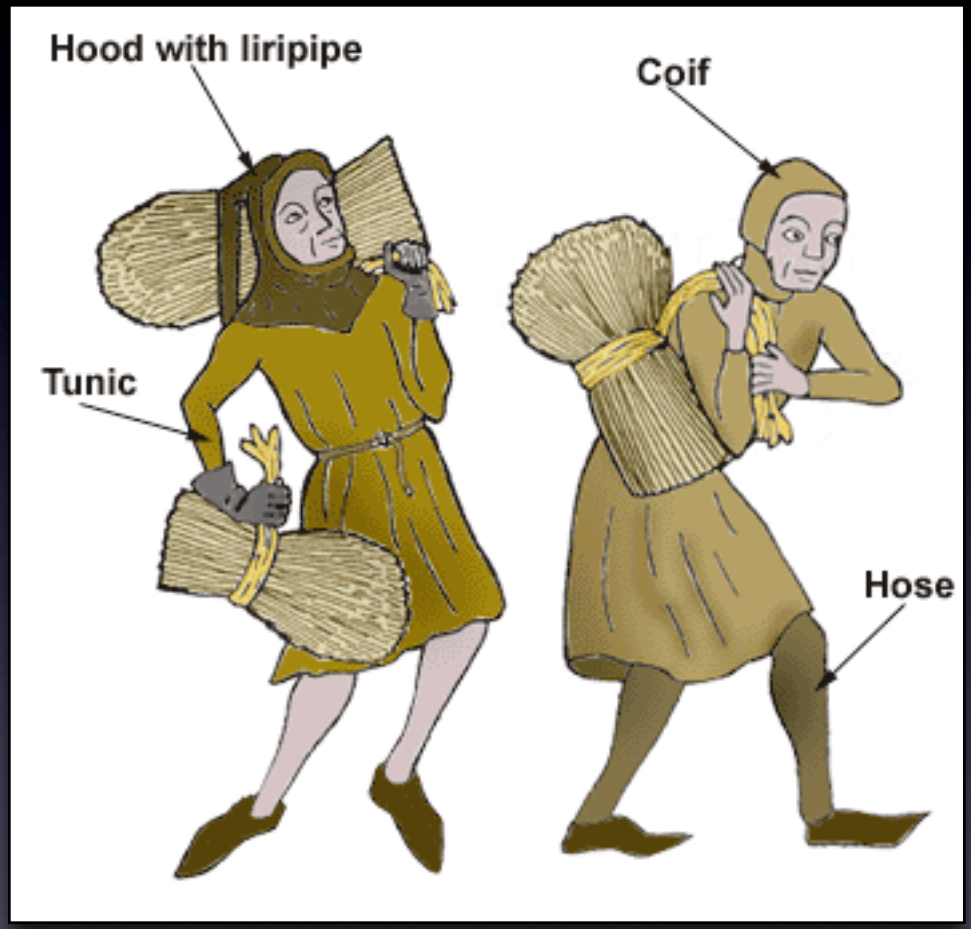
Ed Finkler <coj@cerias.purdue.edu>

The parties involved

- The System Administrator
  - Directly responsible for PHP environment security
  - Tendency to lower security of environment to reduce application compatibility complaints
- The PHP Developer
  - Must be aware of the environment and how it impacts app development
  - Will write apps assuming certain features are enabled, despite security risks

The parties involved

- The PHP "Deployer"
  - By far the largest portion of the audience
  - Uses PHP apps on a web site, but not a coder
  - Not capable of assessing security of an app
  - At the mercy of the SysAdmin and Developer



Ed Finkler <coj@cerias.purdue.edu>

Requirements of PHPSecInfo

- A security auditing tool accessible to the "Deployer"
  - Compatible
    - Support PHP4 (85%) and PHP5 (15%)
  - Easy to install
    - Unzip and Upload
  - Easy to execute (little or no config)
    - Runs upon upload; single function call

Requirements of PHPSecInfo

- Easy to understand
  - Clear, unambiguous results; color coding
- Encourage further exploration
  - Offer extended explanations with links to more info

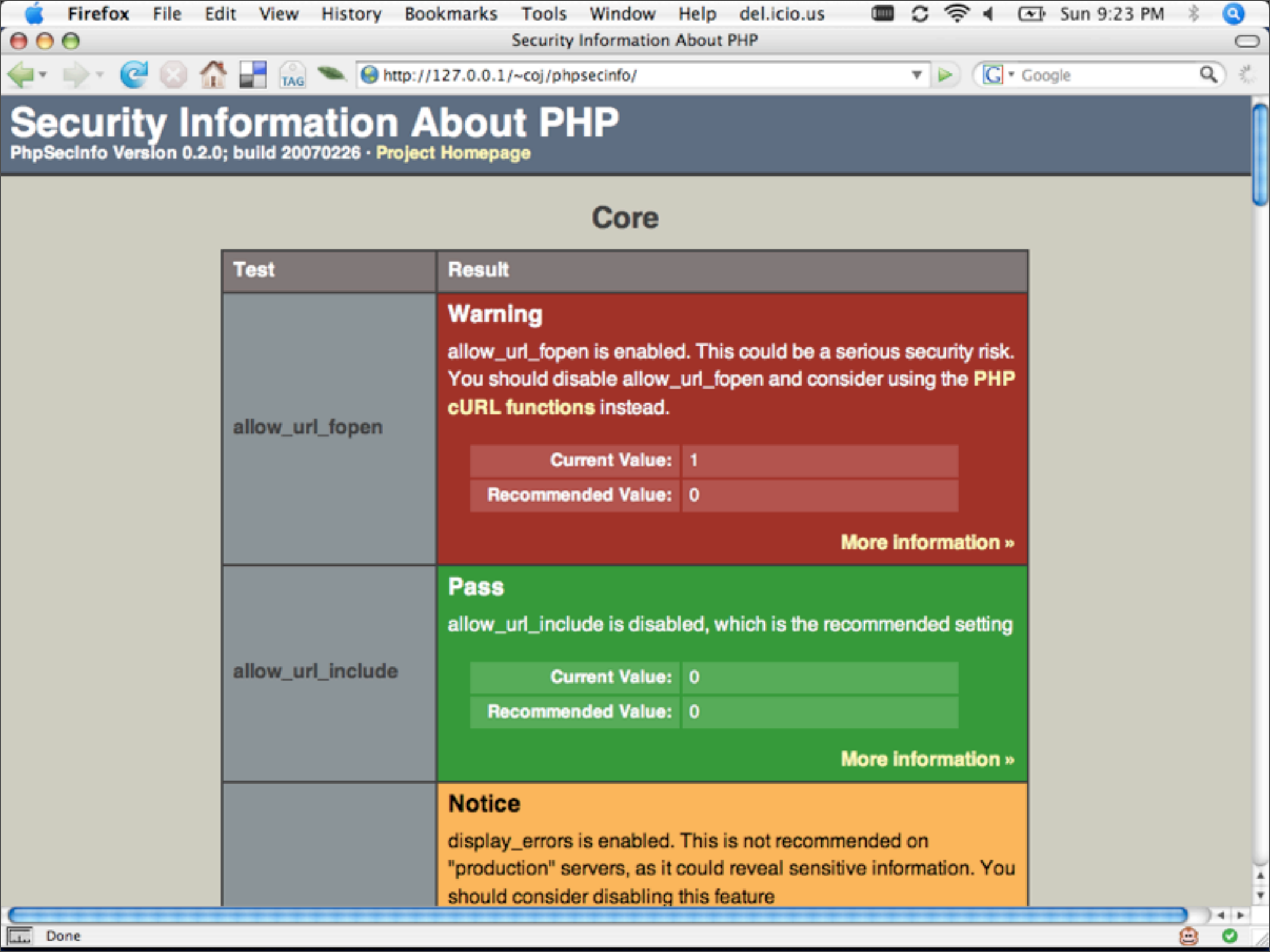
Ed Finkler <coj@cerias.purdue.edu>

Executing PHPSecInfo

1. Unzip
2. Upload
3. View in Browser

```
<?php require_once('PhpSecInfo/PhpSecInfo.php'); ?>
<?php phpsecinfo(); ?>
```

Ed Finkler <coj@cerias.purdue.edu>


Firefox File Edit View History Bookmarks Tools Window Help del.icio.us
Sun 9:23 PM
Security Information About PHP
http://127.0.0.1/~coj/phpsecinfo/
Google
Security Information About PHP
PhpSecInfo Version 0.2.0; build 20070226 · Project Homepage
Core
Test
Result
allow_url_fopen
Warning
allow_url_fopen is enabled. This could be a serious security risk. You should disable allow_url_fopen and consider using the PHP cURL functions instead.
Current Value: 1
Recommended Value: 0
More information »
allow_url_include
Pass
allow_url_include is disabled, which is the recommended setting
Current Value: 0
Recommended Value: 0
More information »
Notice
display_errors is enabled. This is not recommended on "production" servers, as it could reveal sensitive information. You should consider disabling this feature
Done

Test Suite

- 17 tests for commonly exploited security vulnerabilities in PHP environment
- Each test result shows:
  - Current Setting
  - Recommended Setting
  - Result (color-coded)
  - Explanation
  - Link to further info
- Simple metrics output

use_trans_sid	use_trans_sid is disabled, which is the recommended setting Current Value: 0 Recommended Value: 0 More information »

Tests Not Run

Test	Result
CGI::force_redirect	**Not Run** You don't seem to be using the CGI SAPI More information »

Test Results Summary

Test	Result
Notice	9 out of 17 (52.94%)
Pass	7 out of 17 (41.18%)
Warning	1 out of 17 (5.88%)

Consortium News

Fri, 20 Oct 2006
PHP Security Consortium Launches New Project - PHPSecInfo

Wed, 16 Nov 2005
Daniel Convissor Elected as Principal

Promotional Links

Please support us by providing a link to the PHP Security Consortium on your web site. You can also use our promotional image:

PhpSecInfo Test Information

allow_url_fopen

Test Description

This test checks to see if allow_url_fopen is enabled.

Security Implications

If enabled, allow_url_fopen allows PHP's file functions -- such as `file_get_contents()` and the `include` and `require` statements -- can retrieve data from remote locations, like an FTP or web site. Programmers frequently forget this and don't do proper input filtering when passing user-provided data to these functions, opening them up to code injection vulnerabilities. A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is *on* by default.

Recommendations

You should disable allow_url_fopen in the php.ini file:

```
; Disable allow_url_fopen for security reasons
allow_url_fopen = 'off'
```

The setting can also be disabled in apache's httpd.conf file:

```
# Disable allow_url_fopen for security reasons
php_flag  allow_url_fopen  off
```

Get PhpSecInfo

Download Now »

- **Version:** 0.2.0 20070226
- md5 hash

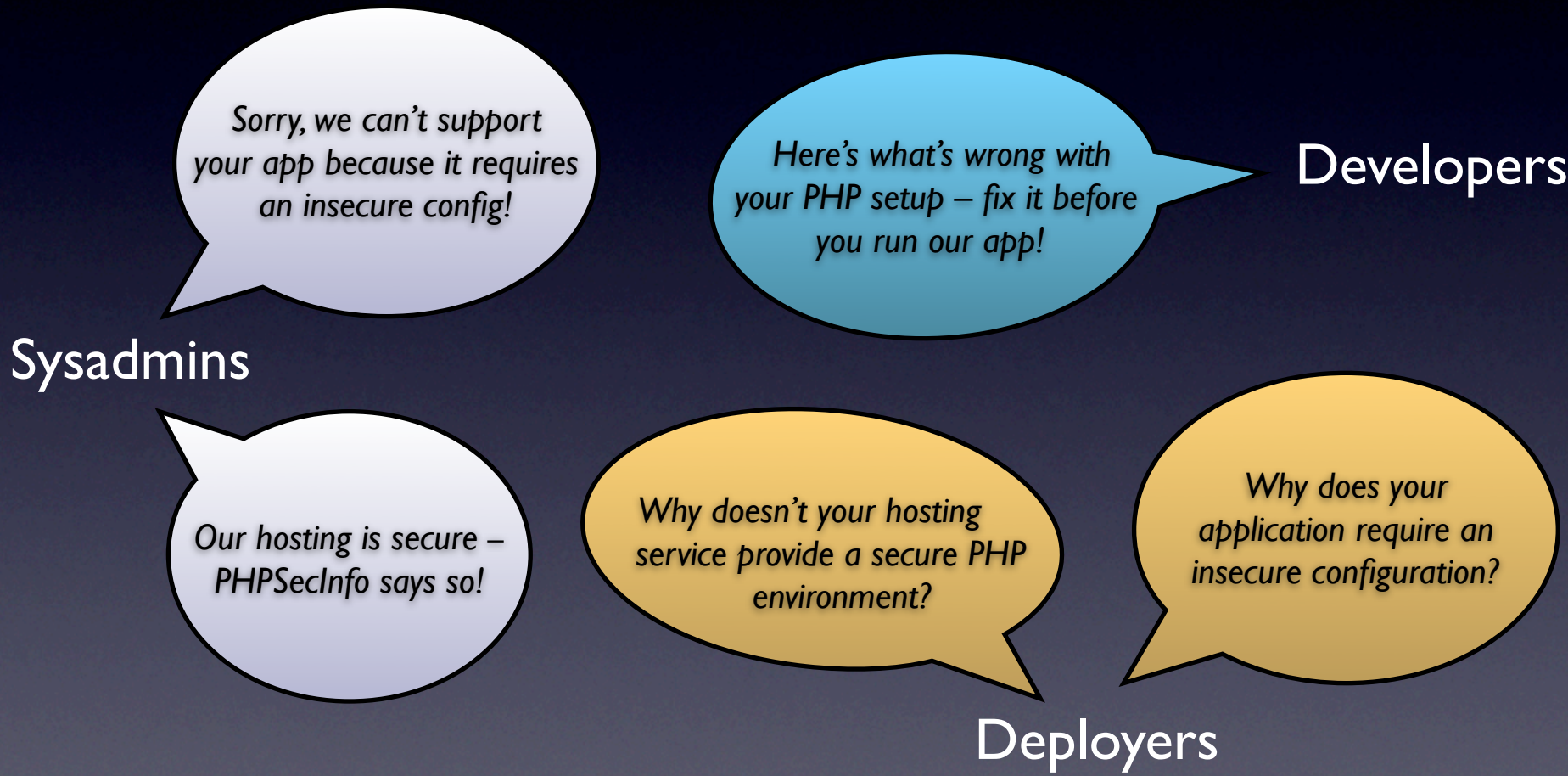
Documentation

- View README
- View CHANGELOG
- View generated documentation

Mailing List »

Screenshots:

PHPSecInfo encourages accountability



Ed Finkler <coj@cerias.purdue.edu>

For advanced users

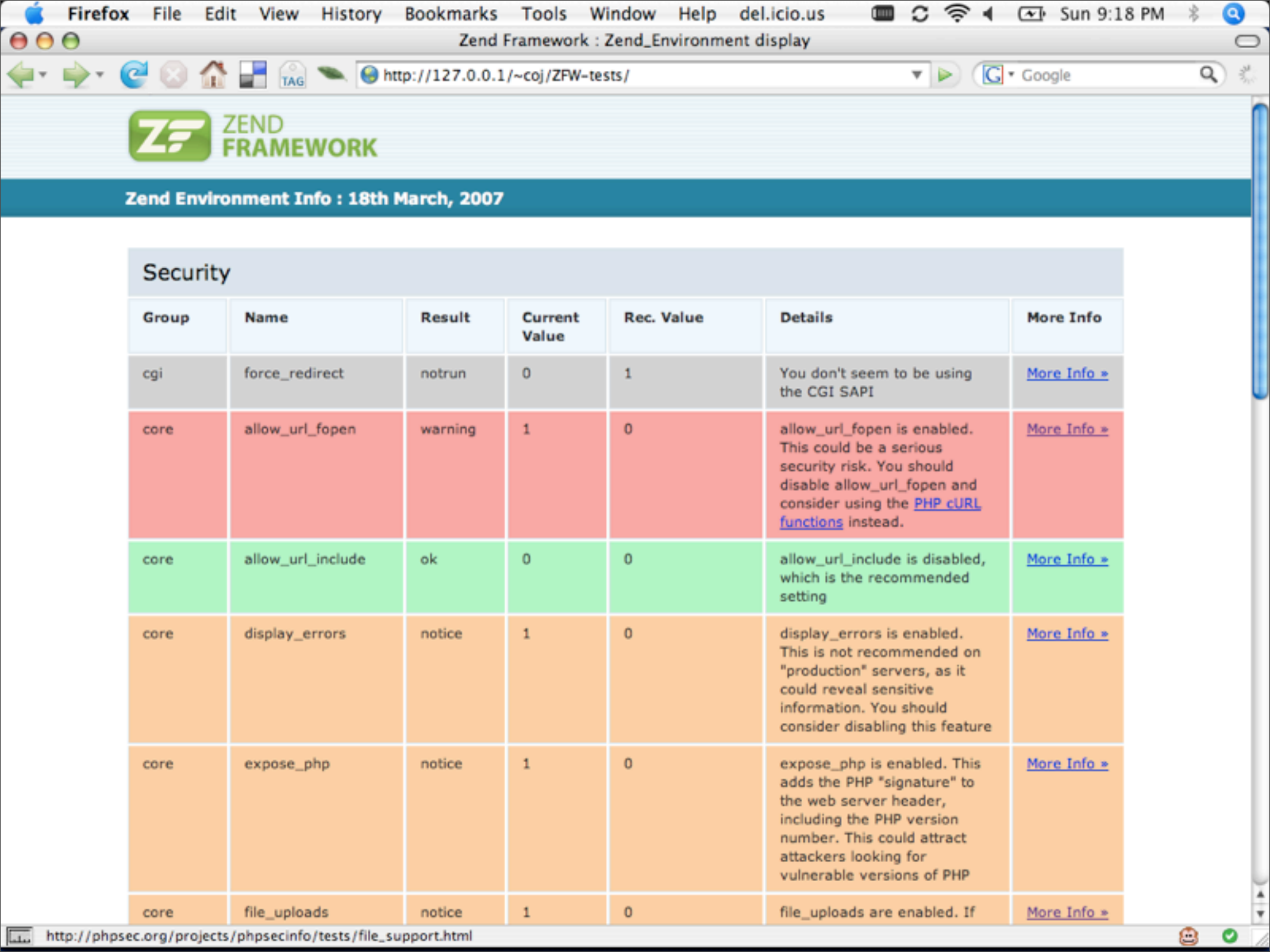
- Still a useful tool for evaluating PHP environments
  - Part of an auditing toolkit for web app security experts
- Extensible test framework
  - Create custom tests specific to an environment
  - Full generated documentation available

Ed Finkler <coj@cerias.purdue.edu>

Zend_Environment Security Module

- Part of Zend Framework
- PHP5-only
- Zend_Environment offers programatic access to PHP environment information
- Z_E security module based on PHPSecInfo
  - Offers better (for now) programatic access to test results
  - More flexible output (HTML, Text, etc)
  - Part of a full-featured development framework

Ed Finkler <coj@cerias.purdue.edu>


Firefox File Edit View History Bookmarks Tools Window Help del.icio.us
Sun 9:18 PM
Zend Framework : Zend_Environment display
http://127.0.0.1/~coj/ZFW-tests/
Google
ZEND FRAMEWORK
Zend Environment Info : 18th March, 2007
Security
Group
Name
Result
Current Value
Rec. Value
Details
More Info
cgi
force_redirect
notrun
0
1
You don't seem to be using the CGI SAPI
More Info »
core
allow_url_fopen
warning
1
0
allow_url_fopen is enabled. This could be a serious security risk. You should disable allow_url_fopen and consider using the PHP cURL functions instead.
More Info »
core
allow_url_include
ok
0
0
allow_url_include is disabled, which is the recommended setting
More Info »
core
display_errors
notice
1
0
display_errors is enabled. This is not recommended on "production" servers, as it could reveal sensitive information. You should consider disabling this feature
More Info »
core
expose_php
notice
1
0
expose_php is enabled. This adds the PHP "signature" to the web server header, including the PHP version number. This could attract attackers looking for vulnerable versions of PHP
More Info »
core
file_uploads
notice
1
0
file_uploads are enabled. If
More Info »
http://phpsec.org/projects/phpsecinfo/tests/file_support.html

More Information

phpsecinfo.com
phpsec.org
cerias.purdue.edu
framework.zend.com