



Enabling Grids for E-science

# Systems and Software Security Session – Your Web server (a bit more) safe & sound

*Gerard Frankowski*

*Poznań Supercomputing and Networking Center*

[www.eu-egee.org](http://www.eu-egee.org)



- **The purpose of the talk**
  - Experience from testing EGEE web sites
  - Who we are going to help this time?
- **The basics of securing a Web server**
- **Information disclosure attacks**
  - Short introduction
  - How an administrator may help?
  - How a developer may help?
- **Apache and PHP secure configuration**
  - A simple tool for scanning your PHP settings
- **More info, contact data**
- **Questions**



- **Web servers testing in EGEE**
  - Grid monitoring service ([monitoring.egee.man.poznan.pl](http://monitoring.egee.man.poznan.pl))  
penetration testing
  - Some other sites seen at a glance
- **We see that many EGEE services are Web-based**
- **Sometimes the IT people in education/science tend to forget about security – we want to help**
- **Apache and PHP will be assumed – the most of reviewed services based on them**
  - General hints are common though



- **Try to have as current version of the software as possible**
  - Costs some effort for patches and updates
- **Remember not only about a Web server**
  - The interpreter (e.g. PHP), database engines or crypto library also matters
  - And the operating system?
  - Costs even more effort for patches and updates...
  - Sometimes certain elements of this puzzle do not cooperate...
- **Configuration issues**
  - Respect the least privileges principle
  - Thoroughly analyze what is necessary for whom
  - The default configuration offer offers too much!

- **Information disclosure (information leak) – a situation where someone may access the data that are not necessary for him or her**
  - Installed software with version numbers
  - Error messages
  - The database structure
  - Directory contents or other filesystem details
  - Internal network addresses
  - Statistics pages made public
  - User names
- **Especially easy to conduct for Web applications**
  - Web servers, scripting engines etc. often suffer from leaving them configured by default

- **Some examples**
  - Apache and other installed software version numbers



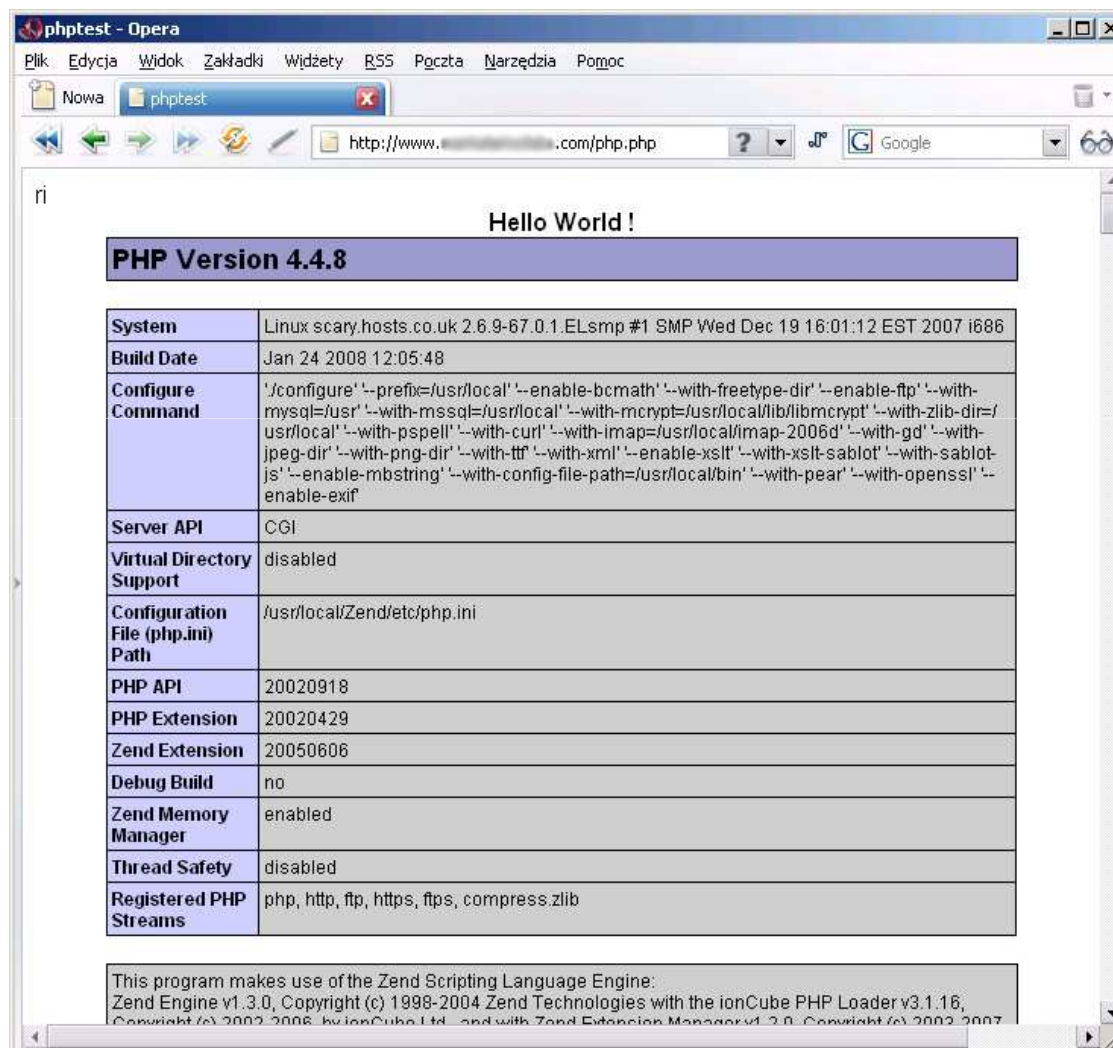
- Directory contents





- **Some examples - PHP**

- Our favorite phpinfo()
- We look at:
  - phpinfo.php
  - info.php
  - test.php
  - php.php
  - p.php
  - a.php





- Some examples: PHP (cont.)
  - Displaying error messages



- A PHP 4.x Easter egg:



- **Advices for the administrators**
  - Learn about the configuration of your software
  - Switch off disclosing internal information
    - Remember: long fingerprinting will disclose much anyway, however an attacker may look for other (insecure) sites
  - However, log the necessary information instead
- **Information disclosure for the developers**
  - Implement error handling appropriately
    - Not too much information displayed
    - The user is not interested in technical details, he should only know what he or she should do (whom to ask for help)
    - The application should have appropriate logging facilities instead



- **The most popular server in the world**
  - Netcraft (August 2009): 46,30% of sites
- **Configuration file: httpd.ini**
- **The main hints (incomplete list):**
  - Remove unnecessary default directories (e.g. manual, icons)
  - If possible, switch off SSI (disabled by default) and CGI
  - Use directives Deny, Allow with respect to least privileges principle
  - Configure logging facilities
  - Run mod\_security
  - Stop unnecessary modules



- **Avoiding Information Disclosure**

- Switching off displaying server signatures

```
ServerSignature Off
```

- Hiding the directory contents

```
<Directory "./Apache/Apache2/htdocs">
```

```
Options -Indexes
```

```
</Directory>
```

- Custom error message pages

```
ErrorDocument 400 /errordocs/400.html
```

```
ErrorDocument 401 /errordocs/401.html
```

```
ErrorDocument 403 /errordocs/403.html
```

```
ErrorDocument 404 /errordocs/404.html
```

- **The best known server-side free scripting engine**
- **Is it secure?**
  - *To say PHP has a security problem suggests that it's impossible to develop a secure PHP application, but to say PHP doesn't have a security problem suggests that everything is perfect – neither is true (Chris Shifflet)*
  - *PHP is neither inherently secure nor insecure. It is the responsibility of the programmer of a web application, the database administrator and the system administrator to ensure that security is not compromised at several levels (James D. Keeline)*

- **Avoiding information disclosure**
  - `error_reporting = E_ALL & ~E_NOTICE`
  - `expose_php = off`
  - `display_errors = off`
  - `log_errors = on`
  - `error_log = /var/log/phplog`



- **Set limits on users**
  - memory\_limit = 8M
  - max\_input\_time = 60
  - max\_execution\_time = 120
- **Respect the least privileges principle**
  - file\_uploads = off
  - register\_globals = off
  - allow\_url\_fopen = off
  - disable\_functions = „passthru, exec, ...”
- **Do not let your brain to be switched off**
  - magic\_quotes\_gpc = off (?!)
  - safe\_mode = off (?!)

- **An exhaustive list of functions that switching off should be considered**
  - apache\_child\_terminate, apache\_get\_modules, apache\_get\_version, apache\_getenv, apache\_lookup\_uri, apache\_note, apache\_setenv, chmod, exec, get\_cfg\_var, getenv, getmypid, getmyuid, ini\_alter, ini\_get, ini\_get\_all, ini\_set, link, mail, passthru, pcntl\_exec, phpuname, popen, posix\_..., posix\_kill, proc\_open, send\_mail, shell\_exec, shmop\_open, symlink, syslog, system, virtual



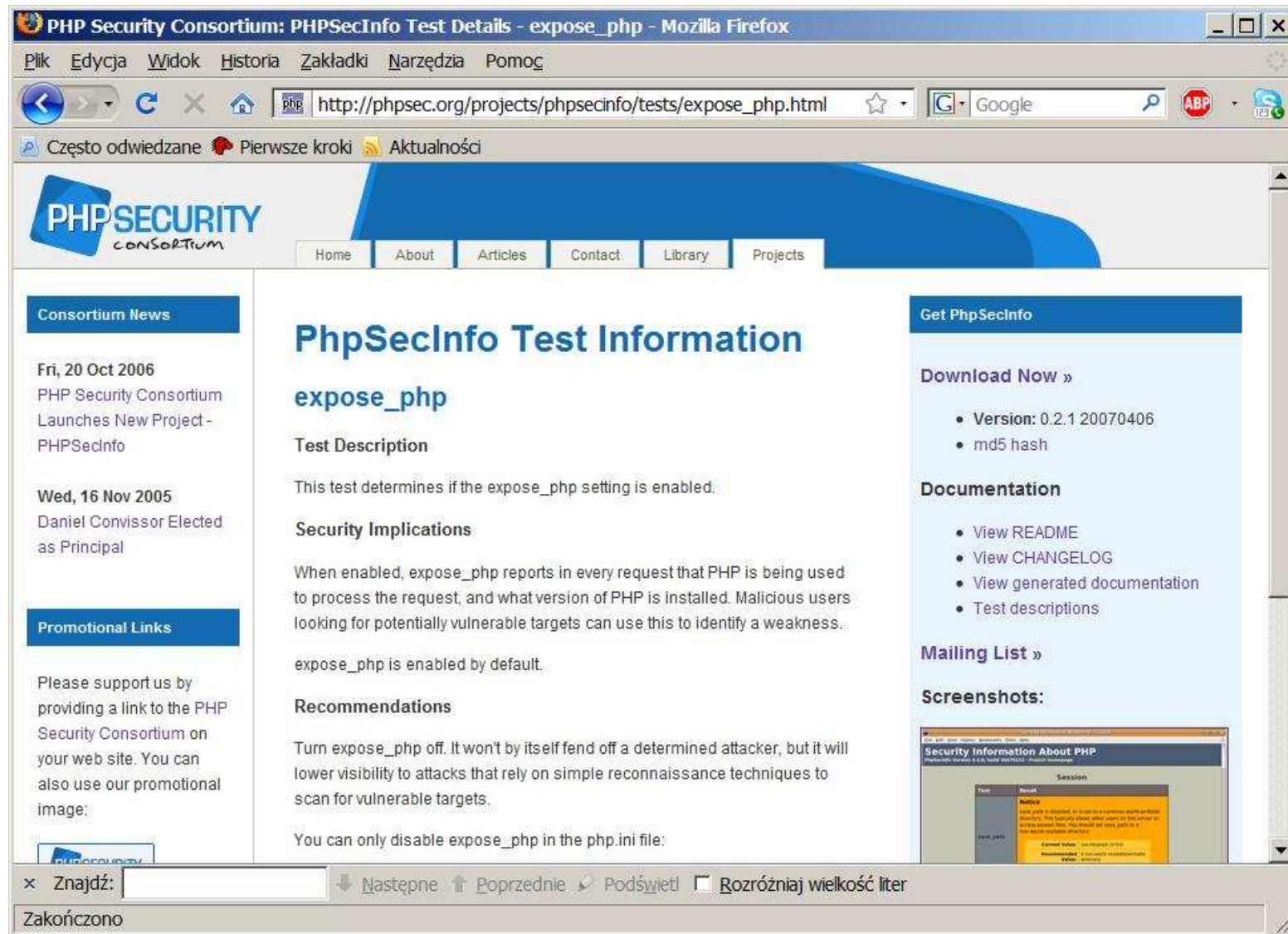
- **A simple PHP configuration scanner**
  - Developed by PHP Security Consortium
  - The latest version: 0.2.1 (April 2007)
    - Seems a bit immature and outdated, but do helps!
  - Systems: all where PHP can be run
    - Written in PHP itself
    - Several tests are system-specific though
- **Usage**
  - Just put into your website and run as e.g.  
<http://127.0.0.1/phpsecinfo>
- **Result analysis**
  - A nice-looking graphical summary with criticality levels, fix suggestions, additional information and hints



Security Information About PHP  
 PhpSecInfo Version 0.2.1; build 20070406 · Project Homepage

## Core

Test	Result				
allow_url_fopen	<p><b>Warning</b></p> <p>allow_url_fopen is enabled. This could be a serious security risk. You should disable allow_url_fopen and consider using the <b>PHP cURL functions</b> instead.</p> <table border="1"> <tr> <td>Current Value:</td> <td>1</td> </tr> <tr> <td>Recommended Value:</td> <td>0</td> </tr> </table>	Current Value:	1	Recommended Value:	0
Current Value:	1				
Recommended Value:	0				



The screenshot shows a Mozilla Firefox browser window with the address bar containing the URL `http://phpsec.org/projects/phpsecinfo/tests/expose_php.html`. The page title is "PHP Security Consortium: PHPSecInfo Test Details - expose\_php". The browser's menu bar includes "Plik", "Edycja", "Widok", "Historia", "Zakładki", "Narzędzia", and "Pomoc". The address bar also shows a search engine (Google) and a search box.

The page content includes the PHP Security Consortium logo and a navigation menu with links for "Home", "About", "Articles", "Contact", "Library", and "Projects". The main content area is titled "PhpSecInfo Test Information" and "expose\_php". It contains sections for "Test Description", "Security Implications", and "Recommendations".

**Test Description**  
This test determines if the expose\_php setting is enabled.

**Security Implications**  
When enabled, expose\_php reports in every request that PHP is being used to process the request, and what version of PHP is installed. Malicious users looking for potentially vulnerable targets can use this to identify a weakness.

expose\_php is enabled by default.

**Recommendations**  
Turn expose\_php off. It won't by itself fend off a determined attacker, but it will lower visibility to attacks that rely on simple reconnaissance techniques to scan for vulnerable targets.

You can only disable expose\_php in the php.ini file:

**Get PhpSecInfo**  
Download Now »

- Version: 0.2.1 20070406
- md5 hash

**Documentation**

- View README
- View CHANGELOG
- View generated documentation
- Test descriptions

**Mailing List »**

**Screenshots:**

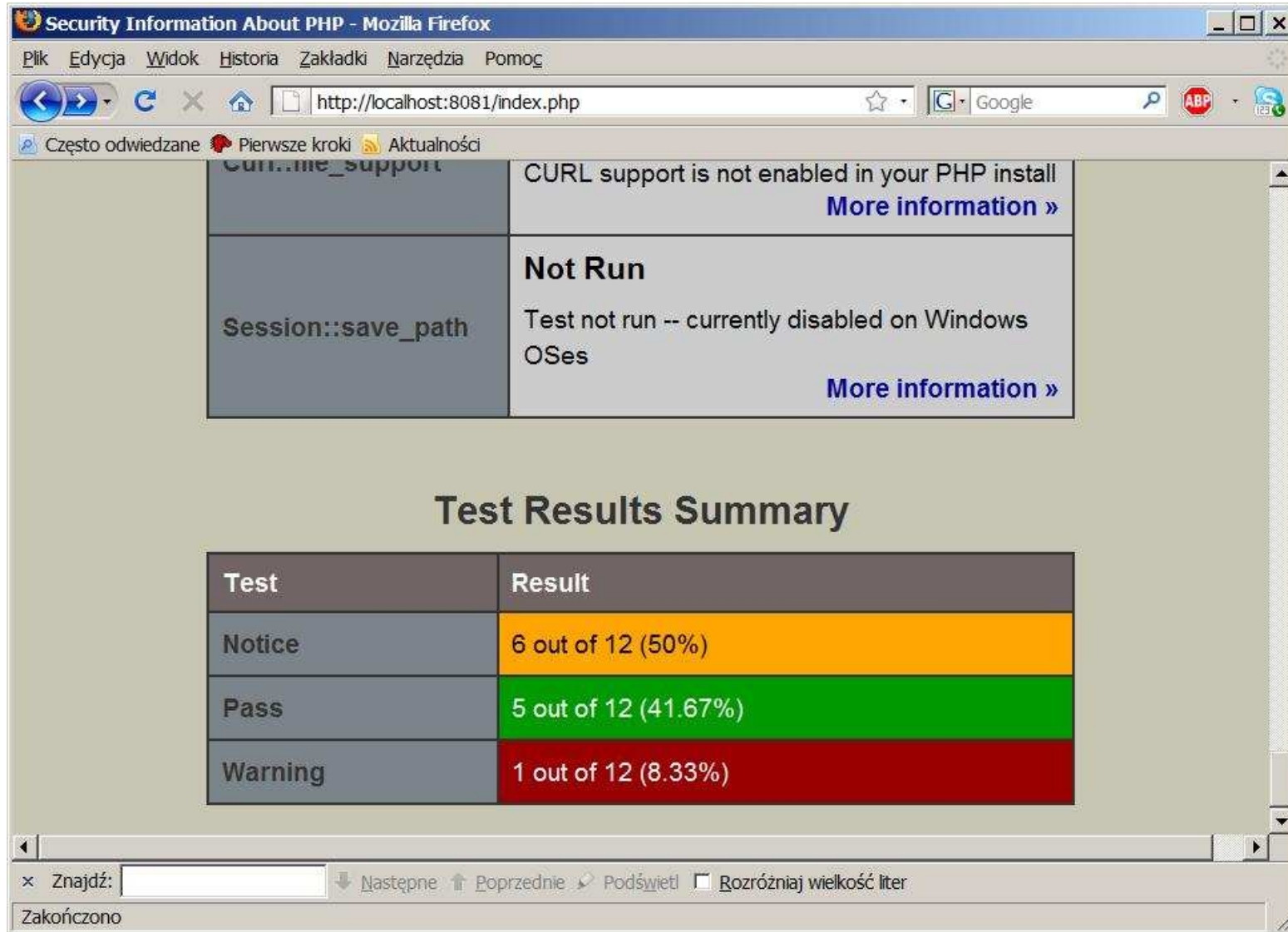
A screenshot of the "Security Information About PHP" page is shown, displaying a "Notice" box with the following text:

```

Notice
-----
Your php.ini is disabled. It is not a secure default
configuration. This feature shows other users on the server
to what version they are running. You should set
expose_php=0 in your php.ini file.
  
```

The browser's status bar at the bottom shows "Zakończono" and navigation controls like "Znajdź:", "Następne", "Poprzednie", "Podświetl", and "Rozróżnij wielkość liter".





Security Information About PHP - Mozilla Firefox

http://localhost:8081/index.php

CURL support	CURL support is not enabled in your PHP install <a href="#">More information »</a>
Session::save_path	<b>Not Run</b> Test not run -- currently disabled on Windows OSes <a href="#">More information »</a>

### Test Results Summary

Test	Result
Notice	6 out of 12 (50%)
Pass	5 out of 12 (41.67%)
Warning	1 out of 12 (8.33%)

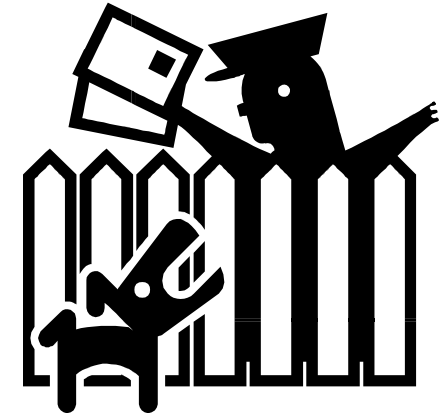
Zakończono

- **Apache security tips**
  - [http://httpd.apache.org/docs/2.2/misc/security\\_tips.html](http://httpd.apache.org/docs/2.2/misc/security_tips.html)
- **20 ways to Secure your Apache Configuration**
  - <http://www.petefreitag.com/item/505.cfm>
- **PHP security manual**
  - <http://php.net/security>
- **PHP security guide**
  - <http://phpsec.org/php-security-guide.pdf>
- **EGEE Security Best Practices**
  - [https://edms.cern.ch/file/926685/1/EGEE\\_best\\_practices.pdf](https://edms.cern.ch/file/926685/1/EGEE_best_practices.pdf)
  - Chapter 2.4 “Services and software”





- **The author of the presentations**
  - e-mail: [gerard@man.poznan.pl](mailto:gerard@man.poznan.pl)
- **PSNC**
  - WWW: [http://www.man.poznan.pl/\(en\)](http://www.man.poznan.pl/(en))
  - e-mail: [office@man.poznan.pl](mailto:office@man.poznan.pl)
- **PSNC Security Team**
  - WWW: <http://security.psnc.pl/en>
  - e-mail: [security@man.poznan.pl](mailto:security@man.poznan.pl)





**Thank you for your attention and attendance!**