

BEZPIECZEŃSTWO W PHP

W jaki sposób ??

1. Od strony serwera

- uszczelnianie samego serwera (apache)
- ostrożność w operowaniu modułami
- php.ini !!

2. Od strony skryptu

- inteligencja i wyobraźnia programisty

Od strony serwera(1)

◎ httpd.conf :

```
ServerTokens Prod  
ServerSignature Off
```

```
deny from all
```

```
RewriteEngine on  
RewriteCond %{REQUEST_METHOD} !^(GET|POST|HEAD)$  
RewriteRule .* - [F]
```

◎ ssl.conf

```
SSLProtocol -ALL +SSLv3 +TLSv1  
SSLCipherSuite  
ALL:!ADH:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

Od strony serwera(2)

◎ php.ini

- `expose_php = off`
- `display_errors = off`
- `file_uploads = off` (jeśli nie będziemy używać uploadu)
- `allow_url_fopen = off`
- `session.use_only_cookies = 1`
`session.cookie_domain = www.my_server.pl`
`session.entropy_length = 16`
`session.entropy_file = /dev/urandom`
`session.hash_bits_per_character = 6`
- `disable_functions = dl, exec, pcntl_exec, passthru, system, shell_exec, popen, phpinfo, fsockopen, pfsockopen, proc_open, popen, curl_exec, curl_multi_exec, parse_ini_file, show_source`

Od strony serwera(3)

- ◎ safe_mode (do php 6.0.0)
- ◎ register_globals (do php 6.0.0)
- ◎ open_basedir
- ◎ magic_quotes_gpc (do php 6.0.0)

- ◎ robots.txt :
 User-agent: *
 Disallow: /

A co ze skryptami ?

Local file inclusion

`include()`

`require()`

`require_once()`

`include_once()`

`readfile()`

`fopen()`

`pfopen()`

Co nie uchroni ?

- ◎ strip_tags, htmlspecialchars, htmlentities
- ◎ urldecode
- ◎ niestaranne filtrowanie ciągów
- ◎ MAGIC_QUOTES_GPC

Co pomoże ?

- ◎ addslashes, stripslashes (?)
- ◎ file_exists
- ◎ SAFE_MODE (OPEN_BASEDIR)
- ◎ ALLOW_URL_FOPEN
- ◎ DISPLAY_ERRORS

- Zwykły switch bez żadnych zabezpieczeń

Arbitrary file download

- Nieprawidłowo skonstruowany skrypt downloadu, może pozwolić na ściągnięcie dowolnego pliku z serwera w formie tekstowej (kodowej)

PYTANIA ?!

  **DIĘKUJĘ ZA UWAGĘ**  