Проблеми със сигурността в PHP приложения

Представени от Георги Чорбаджийски
georgi@unixsol.org
http://georgi.unixsol.org/

Базирано на : http://www.securereality.com.au/studyinscarlet.txt

Глобални променливи

- register_globals

```
<?php
  # $authenticated = false;
  if ($password == "secret")
    $authenticated = true;
  if ($authenticated) {
    print 'Secret info';
  }
?>
```

- http://server/script.php?authenticated=1
- Решения
  - register_globals = off
  - Инициализация на променливите

File Upload (old style)

```
<FORM METHOD="POST" ENCTYPE="multipart/form-data">
<INPUT TYPE="FILE" NAME="up">
<INPUT TYPE="SUBMIT" NAME="submit">
</FORM>
```

- $up Filename on local machine ("/tmp/phpxXuoXG")
- $up_size Size in bytes of file (e.g 1024)
- $up_name The original name of the file on the remote system (e.g"/home/gf/blah.txt")
- $up_type Mime type of uploaded file (e.g "text/plain")

- http://server/upload.php?up=/etc/passwd&.....&submit=submit
- Решения
  - Използване на new style uploads
    - $HTTP_POST_FILES && related functions
  - register_globals = off

Remote Files

- Функциите `require()` и `include()`
- Използване и странични ефекти
  - `include('file.php');`
  - `include('http://server/file.php');`
- Забрани
  - allow_url_fopen = off

„Библиотеки“ 1/2

- Проблеми:
  - Използване на „странни“ разширения
  - Код, който прави това:

```
<?
  $lang = "bg";
  include("$lang/loadlan.php");
?>

А файлът loadlang.php е:
<?
 // Do some initialization
 include("$lang/defs.php");
?>
```

- Какво става ако извикаме директно loadlang.php с параметър $lang='http://.....'?

„Библиотеки“ 2/2

- Решения
  - Използвайте стандартни разширения на файловете
  - register_globals = off
  - allow_url_fopen = off
  - Библиотеките се слагат извън web дървото или в недостъпна директория
  - Дефинират се константи и се проверяват

Session Files

- По подразбиране се съхраняват в /tmp
- Сървъра имат достъп до тях

Loose Typing and Associative Arrays

- PHP не е език, който изисква твърди типове на променливите
- Не изисква дори дефиниране на променливите
- Обърнете внимание на разликите между
  - `$data[0]` и
  - `$data["000"]`
- Решения
  - Дефинирайте си променливите
  - Пишете код, който работи без грешки, когато е дефинирано `error_reporting(E_ALL);`

Опасни функции

- include, require
- eval
- exec, passthru, ``, system, popen
- fopen, readfile, file

Защити в PHP

- safe_mode
- open_basedir
- register_globals
- allow_url_fopen
- disable_functions
- file_uploads
- magic_quotes_gpc
- display_errors
- log_errors

Въпроси?