

0day

**Joomla 1.0/1.5beta2 (latest)
upload file mishandling vulnerability**

0uTian < outian@chroot.org >

Agenda

- Apache + php
 - Set php file handling
 - AddHandler
 - Proper upload handler example
 - Joomla 1.0 、 Joomla 1.5 beta2 (latest)
 - Demo
 - Live demo
-
-

Apache + PHP

- Famous Web Application Platform
 - Works on Most of OS
 - Windows
 - Linux
 - FreeBSD
 - SunOS
 - ... others.
-
-

Set php file handling

- Set(In|Out)putfilter
 - SetOutputFilter PHP
 - SetInputFilter PHP
 - AddType
 - AddType application/x-httpd-php .php
 - AddHandler
 - AddHandler php5-script .php
 - Default used in
 - Fedora Core 4 ~ 7
 - CentOS 5.0 (RHEL ? Other Clone ?)
-
-

AddHandler

- Problem
 - *.php.* will be processed by php engine
 - When upload
 - *.php.gif
 - *.php.bmp
 - *.php.jpg
 - *.php.tgz
 - *.php.123456
 - ...
-
-

Example



Proper upload handler example

- When upload 『 ox.php.gif 』
 - Discuz Forum
 - rename to 『 20070722_{MD5}.gif 』
 - gallery 1 / gallery 2
 - rename to 『 ox_php.gif 』
 - lifetype blog
 - rename to 『 X-X.gif 』
 - wordpress blog
 - rename to 『 oxphp.gif 』
 - xoops
 - rename to 『 imgXXXXXXXXX.gif 』

Joomla

- CMS (Content Management System) , just like XOOPS
 - use php + mysql
 - combine with gallery/blog/forum/ ... etc
 - Official website : <http://www.joomla.org/>
 - Taiwan website : <http://www.joomla.org.tw/>
-
-

Exploitation

- login
- Upload a file containing ".php."
 - ex: ox.php.gif
- launch file from browser
 - <http://host/path/images/ox.php.gif>
- Do anything
 - ex: webshell

Demo



Live Demo



www.joomla.org.tw

TaiwanJoomla - 提供Mambo / Joomla架站軟體中文化支援 :: 開放原始碼, 自由軟體, 內容管理系統, 網站建置, 網頁設計 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 我的最愛

網址(D) http://www.joomla.org.tw/

2007/07/17, 週二

 **Taiwan Joomla**
誰是這個地球上最好的內容管理系統?

帳號: 密碼:
忘了您的密碼嗎?

首頁 Joomla!介紹 教學 下載 討論區 酷站秀 客服信箱 搜尋 J!種子計劃 活動報名

如梭資訊安全  **台灣第三屆駭客年會**
2007.7.21~22 **Call for Paper**
HTTP://WWW.ZUSO.ORG.TW
ZUSO SECURITY

J!種子活動：7月台北場次

本站新聞
作者 Administrator
2007/07/11, 週三

7月份的J!種子活動將於7月21日於台北的台灣科技大學舉行。以下是活動相關的資訊：

日期：2007年7月21日(星期六) 14:00 ~ 17:00
地點：台灣科技大學-國際大樓 1B-401 室,台北市基隆路4段43號。
費用：0 -

Joomla 1.5 beta2 下載


請勿使用1.5beta於正式網站中，目前仍為開發中的測試版本。

Joomla!主程式下載

- 1.0.12中文版
- 1.0.12官方版
- 1.5中文語言檔
- 1.5官方發展版

誰在線上
我們有 6 位訪客 和 7 位會員 在線上

活動報名

- VM購物車中文版開發現況
- Joomla + Discuz 發展現況
- 尋找下一個無名小站

Eddy's Joomla! Blog

http://eddychang.blogspot.com/ 網際網路

Live Demo

```
$ nc www.joomla.org.tw 80
```

```
HEAD / HTTP/1.0
```

```
Host: www.joomla.org.tw
```

```
HTTP/1.1 200 OK
```

```
Server: Apache/2.2.2 (Fedora)
```

```
X-Powered-By: PHP/5.1.6
```

```
Connection: close
```

```
Content-Type: text/html; charset=utf-8
```

