

# 封闭的冲突与开放的和平

SOBUG 冷焰



2000

Blackhat

2008

腾讯

2014

2015

SOBUG

“安全行业的陋习都有哪些？”

—知乎问题

浮躁

娱乐圈

...

Helen

自买自夸

高调得没边

**hacked by xxxxx**

— 知乎匿名用户

“百度刘超事件”

# 宅客周刊 | 关于白帽子提交漏洞被抓，实名制风波，圈内人这么看

2016-07-01 小宅 宅客频道

想了解每周最有料的“黑客与极客”资讯，看|宅客精选|就够了。

1

## 白帽子提交漏洞被抓，圈内人这么看

近日，白帽子实习生袁炜因在乌云上提交世纪佳缘网的漏洞而被抓，引起了圈内的热议。行业两派的争议不断，互相鄙视，程度远远超过了当年Windows阵营对Mac阵营。

# 白帽子和漏洞的那些事？

2016-06-30 Fooying 优主张



今天受邀在雷锋网的《硬核公开课》就针对之前“白帽子在乌云网提交世纪佳缘网漏洞后被抓”的事情做了下对于白帽子和漏洞及事件的观点分享，把分享的东西整理下给大家分享。

# 安全观点|“白帽”黑客被抓事件，我想说....

原创 2016-06-25 301 301在路上



前言：强调本文是以个人白帽子身份表达自己的观点和态度，不代表任何公司立场态度，切勿对号入座。

今天，一则某“白帽子”因为提交某厂商漏洞信息，因为测试过程中涉及部分数据最后被抓的事件。在安全圈炸开了锅，朋友圈全部是有关这方面的讨论，对于“白帽子”而言大部分的声音都是偏负面，各种刺耳的言语，一系列轰炸，看完整个人都不好了。白天忙活一天，刚从外面回家，晚上跟朋友吃饭沟通的时候，心不在焉的状态，还是觉得无论从什么角度看，觉得自己得写一些东西，所以也在朋友圈发布了一则观点：

“用于商业目的的时候，满世界全部是白帽子黑客，遇到事件背锅的时候；清一色的落井下石。向坚守道德底线原则的白帽子们致敬。”

# 关于“世纪佳缘白帽子事件”，安在开了个研讨会

原创 2016-07-09 张耀疆 安在



知乎 搜索你感兴趣的内容... 首页 话题 发现 消息

信息安全 世纪佳缘 漏洞 乌云 (WooYun) 白帽黑客 (White Hat) 修改

# 如何看待白帽子在乌云网提交世纪佳缘网漏洞后被抓？ 修改



IT之家 IT圈 辣品

业界资讯 Win10之家 iPhone之家 安卓之家 评测中心  
软件之家 WP之家 iPad之家 数码之家 智能设备

1 微软Surface Book顶配版全面测评 2 苹果

首页 > IT资讯 > 网络

曝白帽子在乌云网提交世纪佳缘网漏洞后被抓

2016-6-26 15:01:54 来源：IT之家 作者：弥尘 责编：弥尘 评论：245

大洋网 news.dayoo.com 我爱广州 洋洋特供 天天315

您的位置： 新闻频道>财经 > 正文

# 白帽子发布漏洞后被抓 世纪佳缘否认“钓鱼”执法

2016-07-06 10:44 来源：京华时报

评论 0 分享



6月24日 12:52 来自 微博 weibo.com

有人向乌云提交某网站的 SQL 注入漏洞，测试中抓了 4000 条用户信息，然后厂商就找公安把人抓了。可能很多人不知道：按《刑法》285 条第 2 款及相关司法解释，入侵获取金融证券系统身份认证信息 10 条以上、一般系统 500 条以上，就可以判刑。以后开安全会议，可以考虑找个熟悉相关法律的律师普法。

搜狐科技 it.sohu.com

请输入搜索关键字

搜索

热门推荐： 阿里巴巴 小米 苹果

首页 互联网 通信 智能硬件 生活服务 创业 科学 IT/数码

搜狐科技 > 互联网

# 白帽子提交世纪佳缘漏洞后被抓3月 拷问安全边界

雷帝触网 2016-07-05 22:41:59 世纪佳缘 世纪 帽子 阅读(35485) 评论(1)

新浪 专栏 · 创事记

专栏首页 个人中心 创事记 作者 投稿

# 世纪佳缘钓鱼白帽子：不守规矩让自己更危险

2016年06月28日 08:23 创事记 微博 作者：maomaobear 我有话说(242人参与)

+ 订阅

# 众测模式争议中需要深度思考的三个事实

原创 2016-06-26 王小瑞 安全牛

白帽黑客因在漏洞众测平台提交漏洞，遭厂商举报并被警方抓捕一事，在发酵了一段时间之后，终于引起了大规模的争论。争论的焦点集中在“未经授权的渗透测试”这一模式是否应该继续进行下去。



非常感谢提交漏洞和对世纪佳缘的支持，我们已第一时间将漏洞修复完毕。

并抓捕了你

“SOBUG加入阿里云生态”

“真的感谢吗？”

## 漏洞回应

### 厂商回应：

危害等级：低

漏洞Rank：1

确认时间：2016-03-08 16:36

### 厂商回复：

非常感谢您的报告。该问题已经通过其它渠道发现并已着手处理。如您有进一步发现，请及时与我们联系。如果您有任何的疑问，欢迎反馈，我们会有专人跟进处理。

### 最新状态：

2016-03-08：已修复

### 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

2016-03-08 16:44 | 撸撸侠 (核心白帽子 | Rank:1475 漏洞数:84 | 我是撸撸侠)

 2

@ 1Rank 我不要了可以么？

1#

2016-03-08 16:45 | 独臂刀王 (普通白帽子 | 还没有发布任何漏洞 | 提交一个漏洞就可以买个袖子~~好爽~)

 2

@撸撸侠 你做梦呀！

2#

“开放的和平会怎么样？”

## SECURITY MANAGEMENT AND COMPLIANCE

### Managed Security Service Providers



### SIEM



### Security Training



### Governance, Risk and Compliance



## INFRASTRUCTURE SECURITY

### Data Masking



### Enterprise Network Firewalls



### Intrusion Prevention Systems



### Network Access Control



### Unified Threat Management



## CYBER SECURITY

### Secure Web Gateways



### Network Forensics



### Threat Intelligence Services



## ENDPOINT SECURITY

### Secure Email Gateways



### Data Loss Prevention



### Endpoint Protection & Anti-virus



### Endpoint Threat Detection & Response



## APPLICATION SECURITY

### Application Security Testing



### Web Application Firewalls



### Application Control

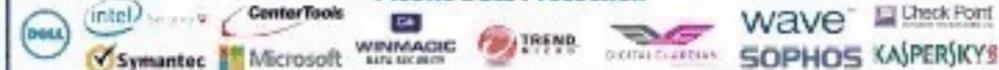


## CLOUD SECURITY

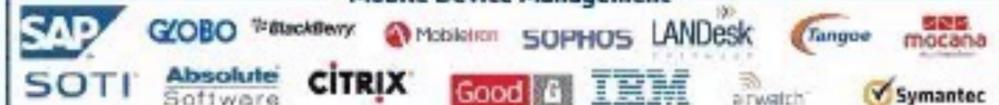


## MOBILE SECURITY

### Mobile Data Protection



### Mobile Device Management



## IDENTITY AND ACCESS MANAGEMENT

### User Authentication



### Identity Governance and Administration



## SECURITY PARTNERS

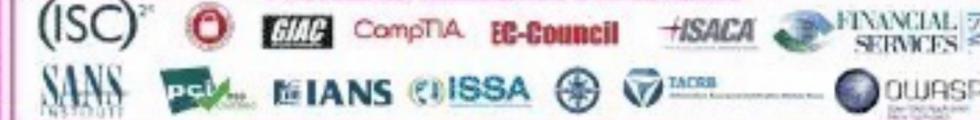


## SECURITY ORGANIZATIONS

### Education & Academic



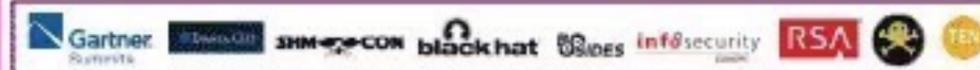
### Professional Associations & Certification



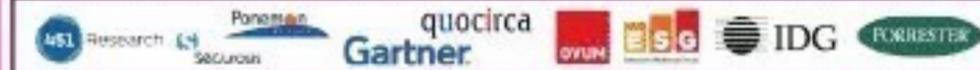
### Government



## SECURITY CONFERENCES



## ANALYST HOUSES



 Jouko Pynnönen (jouko)

816

Reputation

-

Rank

6.42

Signal

97th

Percentile

31.05

Impact

98th

Percentile

25

#136169

## OneLogin authentication bypass on WordPress sites

Share:



State ● Resolved (Closed)

Participants



Disclosed publicly June 6, 2016 5:54pm +0800

Reported To [Uber](#)

Type Authentication

Bounty \$10,000

Collapse

### TIMELINE



[jouko](#) submitted a report to [Uber](#).

May 4th

First, I'm sorry about reporting another WordPress bug (my intention was just to check if WP-OneLogin stores any sensitive info that could be used to attack OneLogin on your other websites).

### Overview

The \*.uber.com WordPress sites use OneLogin SAML-SSO instead of the normal WordPress login. The WordPress plugin shipped by OneLogin has a bug which allows anyone to login without a password or other authentication.

The attacker can supply a username, email address, name, and a role. If the username doesn't already exist in the WordPress database, then the plugin will create a new user (if the provisioning setting is on, which it was on the two sites I tested).

It looks like in order to gain administrator privileges the attacker has to guess some information - a role name such as "administrator", or the email address or username of an existing administrator.

### PoC

I tried this on two sites. On eng.uber.com I couldn't guess a correct role name, user name, or email address to get administrator privileges and therefore was able to create only a "subscriber" level account. On newsroom.uber.com the role name apparently was simply "administrator" so I got that privilege on the system. Some other plugin settings may affect this behavior too.

待审核  
这个  
刚  
赞  
同时我们还在

我插一句嘴：@jouko，快别这么说，我们非常欢迎任何报告，特别是来自于像你这样善于表达的报告者。我们只是需要查清楚WordPress的问题对Uber到底会产生何种影响，请你理解，见谅。



jouko posted a comment  
Admin Dashboard

1 attachment:  
newsroom2.png



mandatoryuber posted a comment.  
Yikes, that's not good - investigating this now.

May 5th (2 months ago)



mandatoryuber changed the status to Triaged.  
Triaging, we should have a response on this later today.

May 5th (2 months ago)



jouko posted a comment.

May 5th (2 months ago)

The screenshot (Screenshot list) grabbed

While I was looking at the PHP function that connects to the database etc.

Hi @jouko，我们决定对这个漏洞奖励最高金额，1万美金，因为它跟[team.uberinternal.com](http://team.uberinternal.com)共享同一套JS，而这可以放大漏洞的影响。

发现

“白帽子是流动的”



解决

“处理更快”

“解决更彻底”



复盘

“为什么会发生？”

“还有哪些有问题？”

收敛

“数据驱动的SRC指标”



沉淀

“案例”

“员工教育”

发现

解决

复盘

收敛

沉淀

“红蓝对抗”

“数据驱动”

Wooyun is good But good is not enough

谢谢