三问乌云“白帽子”：有些人这辈子洗不白了

北京时间 2014 年 1 月 23 日晚上 8 点 24 分，有一位乌云的白帽子在乌云社区发了一篇名为《习科论坛疑似被人搞了，提交了还没被审核！发社区好了！》的文章。这篇文章我们是根据 url 的 referers 检测到的，来源是在乌云社区 id 为 10139 的文章。

文章大概意思是，有某位白帽子对习科进行所谓的“友情检测”，扫到了一枚 webshell，并将其提交到了乌云漏洞平台，不过乌云的管理员并没有审核通过。

提交者口中的后门地址在：data.blackbap.org/help.php，对于这件事，小编只想说呵呵呵呵呵，故事由此展开。

一说习科分站后门

习科有 5 个顶级域名，连同下面的 13 个二级域名暂时都还没有哪个地方发现过被入侵的迹象，所谓的“被人搞了”或者“脱库”还未成为现实，如果真有大神，欢迎来习科领取你的土豪金。

二说习科分站后门

“白帽子”口中所谓的“后门”既不是“被人搞了”，也不是习科技术人员自己留下方便管理的，而是地地道道的钓鱼页面。谁是鱼呢？愿者上钩，有些上钩的还不知道自己上钩了，岂不是太悲惨了？

小编就是为了不让这么悲惨的事情发生，所以公布一下钓鱼脚本的核心代码，如下：

```php
  return $t;
}
setcookie("referers",$_SERVER['HTTP_REFERER'],time()+3600*24);
if(!empty($_POST['silicpass'])){
$pass = addslashes(substr($_POST['silicpass'],0,25));
$ip = $_SERVER['REMOTE_ADDR'];
$ua = indent($_SERVER['HTTP_USER_AGENT'],100);
$time = time();
$referer = empty($_COOKIE['referers']) ? $_SERVER['HTTP_REFERER'] : $_COOKIE['referers'];
$from = indent($referer,80);
$conn = @mysql_connect("[redacted]");
@mysql_select_db([redacted], $conn);
@mysql_query("SET NAMES utf8");
$sql = "INSERT INTO `logs`(`id`,`password`,`ip`,`ua`,`time`,`from`)VALUES(NULL,'".$pass."
@mysql_query($sql,$conn);
@mysql_close();
}
/*************************************
CREATE TABLE IF NOT EXISTS `logs` (
```

至于作用嘛，非常简单的一个脚本，不懂的可以自行查阅 php 基本函数手册。

一问乌云：漏洞的审核标准

最近很多会员在习科论坛发一些漏洞，原因是乌云经常性的拒绝审核通过。

经过小编的观察，对于有商业价值的漏洞，乌云一定会通过审核，对于没有商业价值的漏洞，呵呵呵呵呵。即便是二手漏洞贩子，存在漏洞就是存在漏洞，“自由平等开放的漏洞报告平台”并没有完全体现。

当然了，按照习科小编的惯例，这不是高潮，如果乌云的管理员或者脑残粉觉得上面小编说的不对，小编可以道歉。

高潮是这位名为点点的“白帽子”在乌云社区发表文章的时候是晚上 8 点，原作者在文章中说他提交漏洞并没有通过审核。

而习科这里记录到的是从中午 11 点开始，有一个 ip 为 123.114.61.183 北京联通 ad 的人开始对习科的钓鱼页面暴力破解，共进行 406 次密码破解。

	cisco	123.114.61.183	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (K...	1390455426	http://
	disco	123.114.61.183	Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (K...	1390455445	http://
	123	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455504	http://
	xxoo	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455540	http://
	xiaotao	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455540	http://
	xiaopi	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455541	http://
	xiaoli	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455541	http://
	123	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455541	http://
	yueshaowen	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455541	http://
	xiaodi	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455541	http://
	www.jujingw.com	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455541	http://
	U	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455542	http://
	wangerhan	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455542	http://
	wang880	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455542	http://
	ste	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455542	http://
	xiaoguang	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455542	http://
	niao	123.114.61.183	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:26...	1390455542	http://

第一个时间戳是 1390455426，换成北京时间是 2014 年 1 月 23 日 13:37:06，这个 ip 进行暴力破解的时候应该是开了虚拟机。

开了虚拟机没关系，习科这里没有北京的 ip 分配方案也没关系，刚巧有些人正在部里开会，什么人在用这个 ip 呢，其实我们不去查也知道是谁，你猜我们查没查这个 ip？

不过显然这个页面是登陆不上的。小编的这个问题就是：乌云管理员审核漏洞到底是根据其商业价值还是根据其管理员是否能“二进宫”来评定的？

二问乌云：谁授权乌云管理员的权力，谁来监管平台？

如果习科只是个特例，习科小编想问一下，所有在乌云提交的漏洞，管理员是不是都“二进宫”过恐怕答案显而易见吧。这个问题或许会很容易回答，因为平台要确认是不是误报，顺便把数据库下一遍？

其实我比较好奇 2000w 开房记录是怎么传出来的，即便和乌云没有关系，管理员自己电脑里有多少未授权下载的数据库，自己清楚吧。

小编承认习科的人也未经授权下别人数据库，习科从来是当了婊子就绝不立牌坊，但是声明一点，习科任何一台公司或者个人电脑中不存国内站点的数据库，呵呵呵呵呵。

打开天窗说亮话，平台靠什么来监管？因为是平台，所以可以随意登陆漏洞站点后门，所以可以为所欲为的暴力破解，为所欲为的下别人数据库吗？

三问乌云：你们这辈子还能洗白吗？

小编在库里执行：

```
1. SELECT DISTINCT `ip` FROM `logs` WHERE 1
2. SELECT COUNT(*) FROM `logs` WHERE 1
```

仅仅三天就得到了 9k+条密码字典，ip 超过 300+了哦，密码真是千奇百怪。小编精选几条给大家过过眼瘾好了。

乌云管理员退了虚拟机的最后一条密码是：xikesb。啥？因为自己的字典跑不出密码 xike 就是 sb？

骂人的不止乌云管理员一个，四川眉山的 182.132.204.131 朋友，尝试了俩密码就开始“wocaonimabideyiqundasb”，为何是“一群”不是“一坨”？为何是一群“大 sb”不是一群“羊驼”？

小编我相信上面四川的朋友你在上海嘉定一定有个失散多年的兄弟 180.174.13.148，密码有“helen”,“xikenishishabima?”,“shabixige?”,“wooyunbaimaozicaoxikenima”，你确定你是白帽子？小编我忘了，乌云你们全家都是白帽子。下次麻烦拼正确了，xike 和 xige 差了很远，用 wooyun 就拿 silic 对应啊，不会拼下次让小编教你拼音好了。

一位 123.14.63.189 的郑州朋友怕字典太慢，一边用 ua 为 httpclient 的工具以每秒 3 条的速度暴力破解，一边手工尝试密码，真是迫不及待啊，这么赶，破解出来您想干嘛？小编摸摸良心说一句，这些暴力破解的 200+个朋友，属你的字典最全了，谢谢啦！

这位用 42.120.74.204 的朋友，所有的 300+个 ip 里面，属你和 126.254.129.23 的 Mac 笔记本最叼了，黑产捞了不少吧，有空来习科讲讲心得啊，顺便说一句，我们是习科不是 F4ckteam，你拿这个密码试习科的管理员，你咋不用 xijinping 去当密码登陆白宫呢？

也不缺乏一些大神即便是手机，也不放弃尝试密码的，例如使用苹果 ios 7.0.4 的 27.206.182.39 山东朋友，还有摩托罗拉 XT889 的安卓 180.98.3.72 朋友，其他的手机大神小编不一一罗列的。

文章下面有很多白帽子留言说是习科自己留的，或者说是习科自己拿来收集密码的，有“智者”会选择挂上海外 vpn 只尝试一个单引号密码就放弃，例如 60.50.188.241 的兄弟。

这么多密码，小编不一一罗列了，有机会小编会把字典整理发出来的。

最后说一句，习科的 data 域名下文件不少，不过没啥值得你去扫的，网站日志的分析可比暴力破解的日志多的多了，就不分析了，小编比较好奇为什么都喜欢扫/.svn 呢？习科除了 cracker 分站有 svn 而且不在网站目录，其他分站都没有那东西。顺便说一句，119.57.107.16 你的字典很奇葩，我们收藏啦！

小编知道诚然有真正的白帽子，虽然那些人在那么多“白帽子”里的比例很呵呵，不过小编还是不一竿子打死所有人，只问那些搞黑产的白帽子们：“**你们在外面这么叼，你们这辈子还洗的白吗？**”

评论：