**[[【原创】]](https://forum.90sec.org/forumdisplay.php?fid=10&filter=type&typeid=2) Bluecms 0day 大集合**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 本帖最后由 西毒 于 2012-8-27 00:01 编辑   既然论坛都整改了，把我所有所有的JB都清空了。大家有0day都舍不得放出来，好吧，从我开始吧，把我挖的0day都放出来了。希望大家有0day的都放出来。别藏着了，藏着Mjj了。 Bluecms也就是从一个公司教程看到的cms，然后想了想，既然那里面拿来做教程，我就挖挖这套cms漏洞，我也没深挖到底，也没能坚持把代码看完。但是已经发现了很多很多的问题。其实能拿到shell就可以了。  author： 西毒    来自 :<http://hi.baidu.com/sethc5/blog>  https://forum.90sec.org/images/default/attachimg.gif1.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTM3NHwxM2Y2NzY3NnwxMzUyOTk5NjU2fDk2MzlHQW52OVBjUVJTODNUcXkzZS9VVGlndlNWZjV4bTBkazZaRTh4NlZsbXRJ&nothumb=yes) (63.57 KB)  2012-8-26 23:36  采集俺的MJJ   **0x01. 注入**  client\_ip伪造注入  看代码吧，  这里的getip函数是获取Ip的，由于，client\_ip和x\_forwarded\_for都可以伪造。  在 include/common.fun.php 的106行  [预览源代码](https://forum.90sec.org/thread-3616-1-4.html#viewSource)    [打印](https://forum.90sec.org/thread-3616-1-4.html#printSource)[关于](https://forum.90sec.org/thread-3616-1-4.html#about)   |  |  | | --- | --- | | 01 | function getip() | | 02 | { |  |  |  | | --- | --- | | 03 | if (getenv('HTTP\_CLIENT\_IP')) | | 04 | { |  |  |  | | --- | --- | | 05 | $ip = getenv('HTTP\_CLIENT\_IP'); | | 06 | } |  |  |  | | --- | --- | | 07 |  | | 08 | elseif (getenv('HTTP\_X\_FORWARDED\_FOR')) |  |  |  | | --- | --- | | 09 | { //获取客户端用代理服务器访问时的真实ip 地址 | | 10 | $ip = getenv('HTTP\_X\_FORWARDED\_FOR'); |  |  |  | | --- | --- | | 11 | } | | 12 | elseif (getenv('HTTP\_X\_FORWARDED')) |  |  |  | | --- | --- | | 13 | { | | 14 | $ip = getenv('HTTP\_X\_FORWARDED'); |  |  |  | | --- | --- | | 15 | } | | 16 | elseif (getenv('HTTP\_FORWARDED\_FOR')) |  |  |  | | --- | --- | | 17 | { | | 18 | $ip = getenv('HTTP\_FORWARDED\_FOR'); |  |  |  | | --- | --- | | 19 | } | | 20 | elseif (getenv('HTTP\_FORWARDED')) |  |  |  | | --- | --- | | 21 | { | | 22 | $ip = getenv('HTTP\_FORWARDED'); |  |  |  | | --- | --- | | 23 | } | | 24 | else |  |  |  | | --- | --- | | 25 | { | | 26 | $ip = $\_SERVER['REMOTE\_ADDR']; |  |  |  | | --- | --- | | 27 | } | | 28 | return $ip; |  |  |  | | --- | --- | | 29 | } |   我们继续跟踪一下getip()这个函数的应用。  comment.php中的113行  [预览源代码](https://forum.90sec.org/thread-3616-1-4.html#viewSource)    [打印](https://forum.90sec.org/thread-3616-1-4.html#printSource)[关于](https://forum.90sec.org/thread-3616-1-4.html#about)   |  |  | | --- | --- | | 1 | $sql = "INSERT INTO ".table('comment')." (com\_id, post\_id, user\_id, type, mood, content, pub\_date, ip, is\_check) | | 2 | VALUES ('', '$id', '$user\_id', '$type', '$mood', '$content', '$timestamp', '".getip()."', '$is\_check')"; |  |  |  | | --- | --- | | 3 |  | | 4 | $db->query($sql); |   这里我们伪造下ip测试下。 https://forum.90sec.org/images/default/attachimg.gif2.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTM3NXw0M2NjNWNlM3wxMzUyOTk5NjU2fDk2MzlHQW52OVBjUVJTODNUcXkzZS9VVGlndlNWZjV4bTBkazZaRTh4NlZsbXRJ&nothumb=yes) (36.17 KB)  2012-8-26 23:38  https://forum.90sec.org/images/default/attachimg.gif3.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTM3NnwxYTUxNDlmM3wxMzUyOTk5NjU2fDk2MzlHQW52OVBjUVJTODNUcXkzZS9VVGlndlNWZjV4bTBkazZaRTh4NlZsbXRJ&nothumb=yes) (13.04 KB)  2012-8-26 23:39  看看结果  https://forum.90sec.org/images/default/attachimg.gif4.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTM3N3wxNGU5Yjg2ZHwxMzUyOTk5NjU2fDk2MzlHQW52OVBjUVJTODNUcXkzZS9VVGlndlNWZjV4bTBkazZaRTh4NlZsbXRJ&nothumb=yes) (27.98 KB)  2012-8-26 23:40  可以看到了么？  已经是注入了  问题这里的是报错是。。它已经单独写出报错的语句，以致我们不能利用报错语句，直接爆出用户名和密码。但是我们可以用盲注的方式进行来搞用户名和密码了。但是这样子太麻烦了。之前，我一直在想啊，想啊，用啥方法来注呢， 注，注。。。。。。。  毕竟人的思维太宽了。因为这是个insert的语句，我们可以插入我们想要的信息，然后通过前台页面显示出来，  我们可以这样子构造语句  a','xxx'),('','1','1','1','2',(select concat(admin\_name,0x3a,pwd) from blue\_admin limit 0,1),'1645457407','sss','1')#  前面的闭合前面一个insert语句，因为insert语句的话，我们可以insert into table (a,b,c) values ('fuck1','fuck2','fuck3'),('fuck4','fuck5','fuck6')......这样可以多插几个的。这样子，我们就可以意淫了，  我们测试下  看到了么？用户名和密码已经被我们搞到手了 https://forum.90sec.org/images/default/attachimg.gif5.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTM3OHxkZjE5Mzc3ZHwxMzUyOTk5NjU2fDk2MzlHQW52OVBjUVJTODNUcXkzZS9VVGlndlNWZjV4bTBkazZaRTh4NlZsbXRJ&nothumb=yes) (9.35 KB)  2012-8-26 23:42  这是其一。   **0x02 继续上个注入**  在 ad.js.php中 19行  [预览源代码](https://forum.90sec.org/thread-3616-1-4.html#viewSource)    [打印](https://forum.90sec.org/thread-3616-1-4.html#printSource)[关于](https://forum.90sec.org/thread-3616-1-4.html#about)   |  |  | | --- | --- | | 1 | $ad\_id = !empty($\_GET['ad\_id']) ? trim($\_GET['ad\_id']) : ''; | | 2 | if(empty($ad\_id)) |  |  |  | | --- | --- | | 3 | { | | 4 | echo 'Error!'; |  |  |  | | --- | --- | | 5 | exit(); | | 6 | } |  |  |  | | --- | --- | | 7 |  | | 8 | $ad = $db->getone("SELECT \* FROM ".table('ad')." WHERE ad\_id =".$ad\_id); |   这里的$ad\_id未经过任何过滤就传过来了，并且这里就直接注入了   所以这里就是赤裸裸的注入   所以这里随便选取个站，已经取到  https://forum.90sec.org/images/default/attachimg.gif6.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTM3OXw2MzA4OGU2NnwxMzUyOTk5NjU2fDk2MzlHQW52OVBjUVJTODNUcXkzZS9VVGlndlNWZjV4bTBkazZaRTh4NlZsbXRJ&nothumb=yes) (16.43 KB)  2012-8-26 23:43  **0x03 getshell**  再说一下，直接getshell把  由于存在fck  版本，2.6.3  直接getshell https://forum.90sec.org/images/default/attachimg.gif7.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTM4MHw5ODFmYjQ0NnwxMzUyOTk5NjU2fDk2MzlHQW52OVBjUVJTODNUcXkzZS9VVGlndlNWZjV4bTBkazZaRTh4NlZsbXRJ&nothumb=yes) (67.52 KB)  2012-8-26 23:44  **0x04 后台拿shell**  来到系统设置 再到 模板管理 然后点击编辑   这里编辑的是模板 https://forum.90sec.org/images/default/attachimg.gif8.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTM4MXw1YjhmYjNjM3wxMzUyOTk5NjU2fDk2MzlHQW52OVBjUVJTODNUcXkzZS9VVGlndlNWZjV4bTBkazZaRTh4NlZsbXRJ&nothumb=yes) (25.89 KB)  2012-8-26 23:46  然后点编辑  https://forum.90sec.org/images/default/attachimg.gif9.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTM4MnwyNjU3MmI0OXwxMzUyOTk5NjU2fDk2MzlHQW52OVBjUVJTODNUcXkzZS9VVGlndlNWZjV4bTBkazZaRTh4NlZsbXRJ&nothumb=yes) (91.07 KB)  2012-8-26 23:48  我们跳到上层目录去 https://forum.90sec.org/images/default/attachimg.gif10.jpg  [**下载**](https://forum.90sec.org/attachment.php?aid=NTM4M3wzYTViYjNmNHwxMzUyOTk5NjU2fDk2MzlHQW52OVBjUVJTODNUcXkzZS9VVGlndlNWZjV4bTBkazZaRTh4NlZsbXRJ&nothumb=yes) (32.96 KB)  2012-8-26 23:49  可能问题还很多。  总之一句，无论一套程序出现的安全问题多大，我还是不会去鄙视这些程序员，因为真正的一套cms要我来开发，我只能说我。。。。。。，以前我也是怀着BS的心态去看待一些爆有很多安全问题的程序。终于当有一天去做开发，我就明白了。其实俺当初怀着SB的心态去看我今天写的SB程序。所以最后一句还是那句，尊重别人的劳动果实。转摘请注明转自 <http://hi.baidu.com/sethc5/blog> 西毒 |