

New issue

Jump to bottom

重定向漏洞 #209

Closed

QiAnXinCodeSafe opened this issue on Feb 19, 2019 · 1 comment

Assignees



Labels

BUG

Milestone

1.6

QiAnXinCodeSafe commented on Feb 19, 2019

您好:

我是360代码卫士的工作人员, 在我们的开源代码检测项目中发现zblogphp项目中存在一个重定向漏洞. 详细信息如下:
在cmd.php页面中, 当action为login, 且用户已登陆时, line 19中会获取get参数redirect并用作重定向的路径

```
ajax.php x c_system_common.php x cmd.php x main.php x
16 switch ($action) {
17     case 'login':
18         if (!empty($bp->user->ID) && GetVars( name: 'redirect', type: 'GET')) {
19             Redirect(GetVars( name: 'redirect', type: 'GET'));
20         }
21         if ($bp->CheckRights('admin')) {
22             Redirect( url: 'cmd.php?act=admin');
23         }
24         if (!empty($bp->user->ID) && GetVars( name: 'redirect', type: 'GET')) {
25             setcookie( name: 'redirect', GetVars( name: 'redirect', type: 'GET'), expire: 0, $bp->cookiespath);
26         }
27         Redirect( url: 'login.php');
28         break;
29     case 'logout':
30         CheckIsRefererValid();
31         Logout();
32         Redirect( url: '../');
33         break;
34     case 'admin':
35         Redirect( url: 'admin/index.php?act=admin');
36         break;
37     case 'verify':
38         /*
39          * 考虑兼容原因, 此处不加CSRF验证. logout加的原因是主题的退出无大碍。
40          */
41 }
```

pc:localhost/zblogphp/zblog_system/cmd.php?act=login&redirect=http://www.baidu.com

zsxsoft commented on Feb 19, 2019

Contributor

非常感谢360代码卫士的支持, 我们会尽快修复!

zsxsoft added the BUG label on Feb 19, 2019

zsxsoft assigned rainbowsoft on Feb 19, 2019

rainbowsoft added a commit that referenced this issue on Feb 20, 2019

#209 修正了一个链接跳转的问题;

0071602

zsxsoft closed this as completed on Feb 20, 2019

zsxsoft mentioned this issue on Apr 4, 2019

Z-BlogPHP 1.5.2 Open redirect vulnerability #216

Closed

zsxsoft added this to the 1.6 milestone on Dec 26, 2019

Assignees

rainbowsoft

Labels

BUG

Projects

None yet

Milestone

1.6

Development

No branches or pull requests

3 participants

