New issue

Jump to bottom

Z-BlogPHP 1.5.2 Open redirect vulnerability #216

Closed github123abc123 opened this issue on Apr 4, 2019 · 2 comments

Labels 重复(Duplicate)

github123abc123 commented on Apr 4, 2019 • edited

Z-BlogPHP 1.5.2 has an Open Redirect via the zb_system/cmd.php redirect parameter.
Open Redirection vulnerability Technical details:
URL : http://localhost/zblog/zb_system/cmd.php?atc=login&redirect=http://www.baidu.com
code:

```
case 'login':
if (!empty($zbp->user->ID) && GetVars('redirect', 'GET')) {
Redirect(GetVars('redirect', 'GET'));
}
if ($zbp->CheckRights('admin')) {
Redirect('cmd.php?act=admin');
}
if (empty($zbp->user->ID) && GetVars('redirect', 'GET')) {
setcookie("redirect", GetVars('redirect', 'GET'), 0, $zbp->cookiespath);
}
Redirect('login.php');
break;
```

First: You need login in,then the vulnerability can run.So we use vulnerability for phishing attacks.
Parameter Name : redirect
Parameter Type : GET
Attack Pattern : http://www.baidu.com

(auth:1521106949@qq.com)

Should there be anything else we can help you with, please do not hesitate to ask.

zsxsoft commented on Apr 4, 2019 Contributor

Duplicated with #209

```
0071602
```

zsxsoft closed this as completed on Apr 4, 2019

zsxsoft added the 重复(Duplicate) label on Apr 4, 2019

zsxsoft commented on Apr 4, 2019 • edited Contributor

还有我求求你们了用中文好不好，你们刷CVE的这些人要么百度翻译，要么写的英语谁都看不懂。

Akokonunes mentioned this issue on Jan 26

Create CVE-2020-18268.yaml projectdiscovery/nuclei-templates#3614

Merged

Assignees
No one assigned

Labels
重复(Duplicate)

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants