

代码审计之bluecms1.6后台SQL注入

原创

TuudOp 于 2018-11-07 19:19:11 发布 762 收藏

分类专栏: [Web安全](#) [代码审计](#) 文章标签: [代码审计](#) [web安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_39850969/article/details/83829919

版权



[Web安全](#) 同时被 2 个专栏收录

17 篇文章 0 订阅

订阅专栏



[代码审计](#)

4 篇文章 1 订阅

订阅专栏

bluecm1.6版本后台存在SQL注入

漏洞点链接:

```
http://127.0.0.1/bluecms_v1.6_sp1/uploads/admin/nav.php?act=edit&navid=1
```

代码:

```
elseif($act=='edit')
{
    $sql = "select * from ".table('navigate')." where navid = ".$_GET['navid'];
    $nav = $db->getone($sql);
    ...
    ...
}
```

就是当cat参数为edit是, 执行sql语句:

```
select * from ".table('navigate')." where navid = ".$_GET['navid']
```

参数navid是用户可控的, 没有做任何的过滤, 直接拼接在SQL语句后面, 所以就造成了SQL注入

本地测试:

Notice: Undefined variable: `_COOKIES` in `E:\PHPstudy\WWW\bluecms_v1.6_sp1\uploads\admin\include\common.inc.php` on line 29

Notice: Use of undefined constant `PHP_SELF` - assumed '`PHP_SELF`' in `E:\PHPstudy\WWW\bluecms_v1.6_sp1\uploads\admin\include\common.inc.php` on line 29

BlueCMS管理中心 -

编辑过后请更新缓存

导航名称: *

导航链接: *

是否打开新窗口:

类型:

顺序:

order by 6是正常的

Notice: Undefined variable: `_COOKIES` in `E:\PHPstudy\WWW\bluecms_v1.6_sp1\uploads\admin\include\...`

Notice: Use of undefined constant `PHP_SELF` - assumed '`PHP_SELF`' in `E:\PHPstudy\WWW\bluecms_v1.6_sp1\...`

Error: Query error:select * from blue_navigate where navid = 1 order by 7

order by 7报错

正常字段有六个

Notice: Undefined variable: _COOKIES in E:\PHPstudy\WWW\bluecms_v1.6_sp1\uploads\admin\include\common.inc.php on line 29

Notice: Use of undefined constant PHP_SELF - assumed 'PHP_SELF' in E:\PHPstudy\WWW\bluecms_v1.6_sp1\uploads\admin\include\common.inc.php on line 41

BlueCMS管理中心 -

编辑过后请更新缓存

导航名称: *

导航链接: *

是否打开新窗口: 否

类型:

顺序:

Powered By BlueCMS

https://blog.csdn.net/qq_39850969

Notice: Undefined variable: _COOKIES in E:\PHPstudy\WWW\bluecms_v1.6_sp1\uploads\admin\include\common.inc.php on line 29

Notice: Use of undefined constant PHP_SELF - assumed 'PHP_SELF' in E:\PHPstudy\WWW\bluecms_v1.6_sp1\uploads\admin\include\common.inc.php on line 41

BlueCMS管理中心 -

编辑过后请更新缓存

导航名称: *

导航链接: *

是否打开新窗口: 否

类型:

顺序:

Powered By BlueCMS

https://blog.csdn.net/qq_39850969