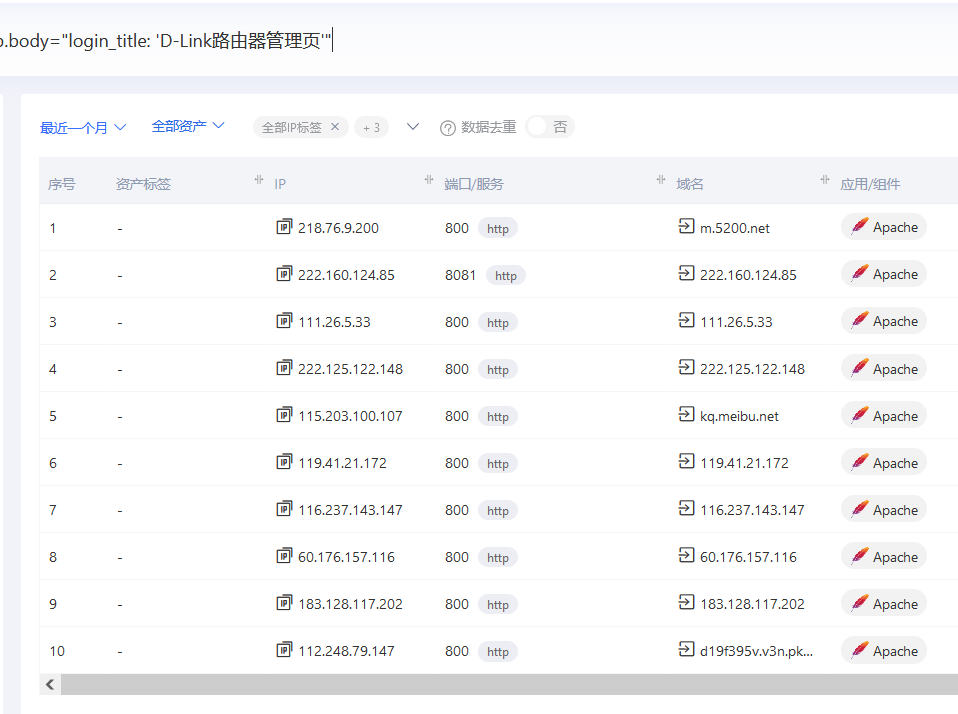
### 1. Search vulnerable products on internet

Go to [https://hunter.qianxin.com/](https://github.com/prismbreak/vulnerabilities/issues/url), and use this syntax to search potential vulnerable products existing on internet:**web.body="login\_title: 'D-Link路由器管理页'"**



Please note that not all assets displayed in the result table are target products. You need to right-click to view the website source code and view the "title" label in the form. If it is the "AC Central Management Platform", it is as follows:



A list of vulnerable targets are as follows:

<http://183.214.192.254:800>

<http://175.13.32.193:800>

<http://218.8.101.103:800>

<http://58.211.213.42:800>

<http://111.175.59.107:800>

<http://36.27.95.28:800>

<http://175.166.219.151:800>

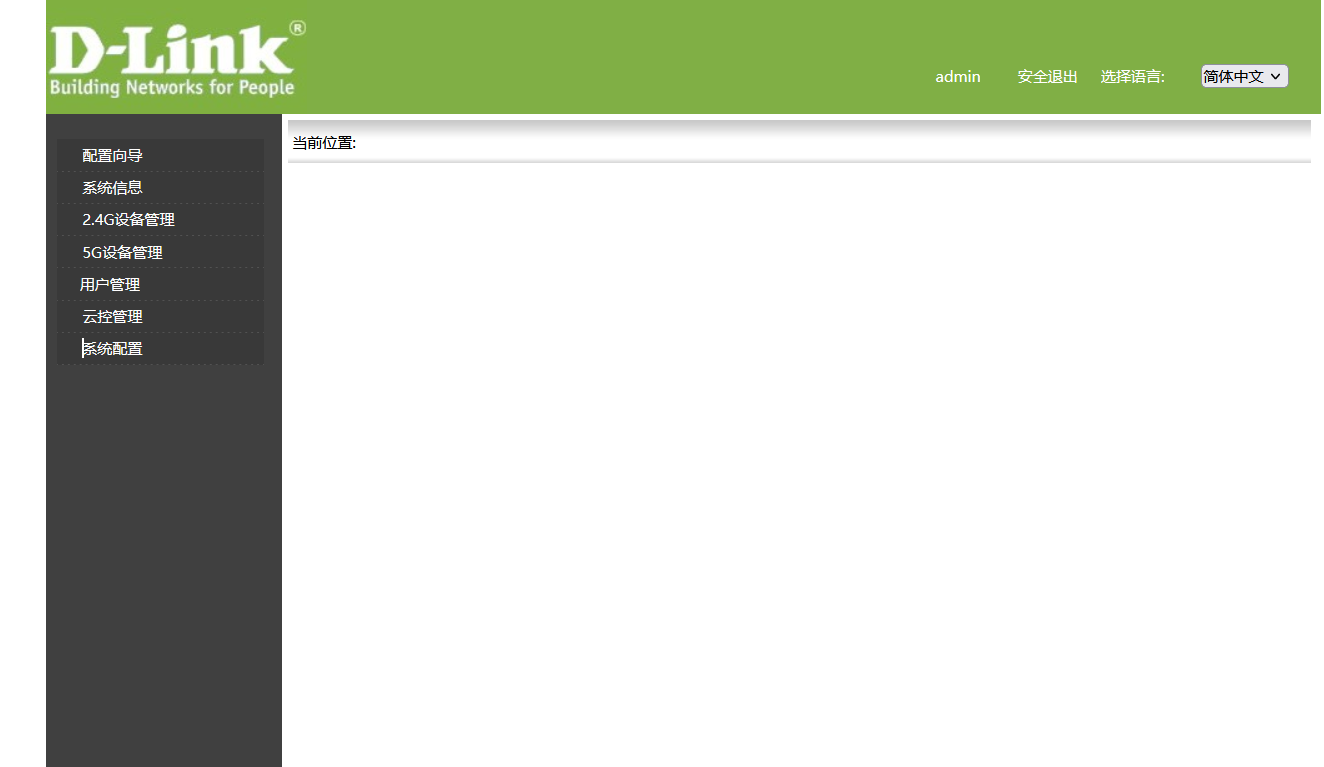
<http://222.175.246.46:800>

<http://112.248.79.147:800>

<http://125.120.107.39:800>

### 2. Login with default credential

The default credential is **admin : admin**



Login successful.

### 3. Upload your payloads

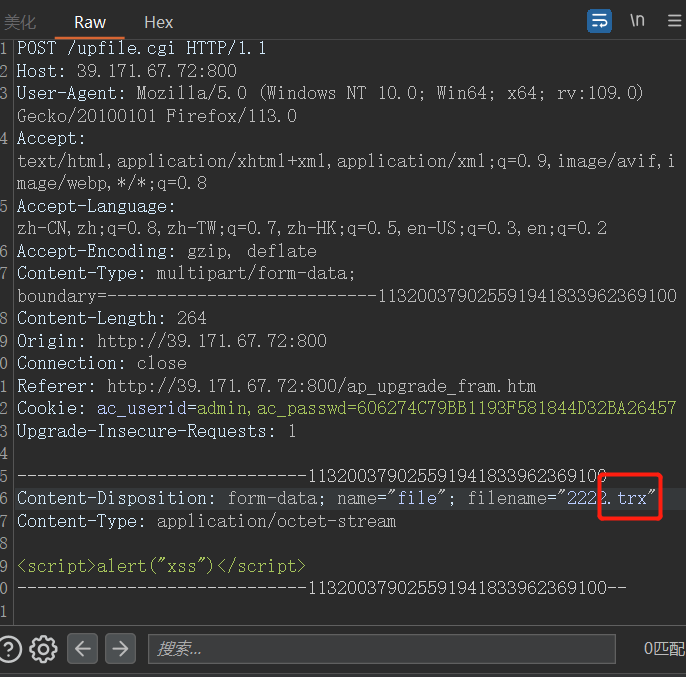
Firstly, click on "系统配置",

Secondly, click on "AP 系统管理",

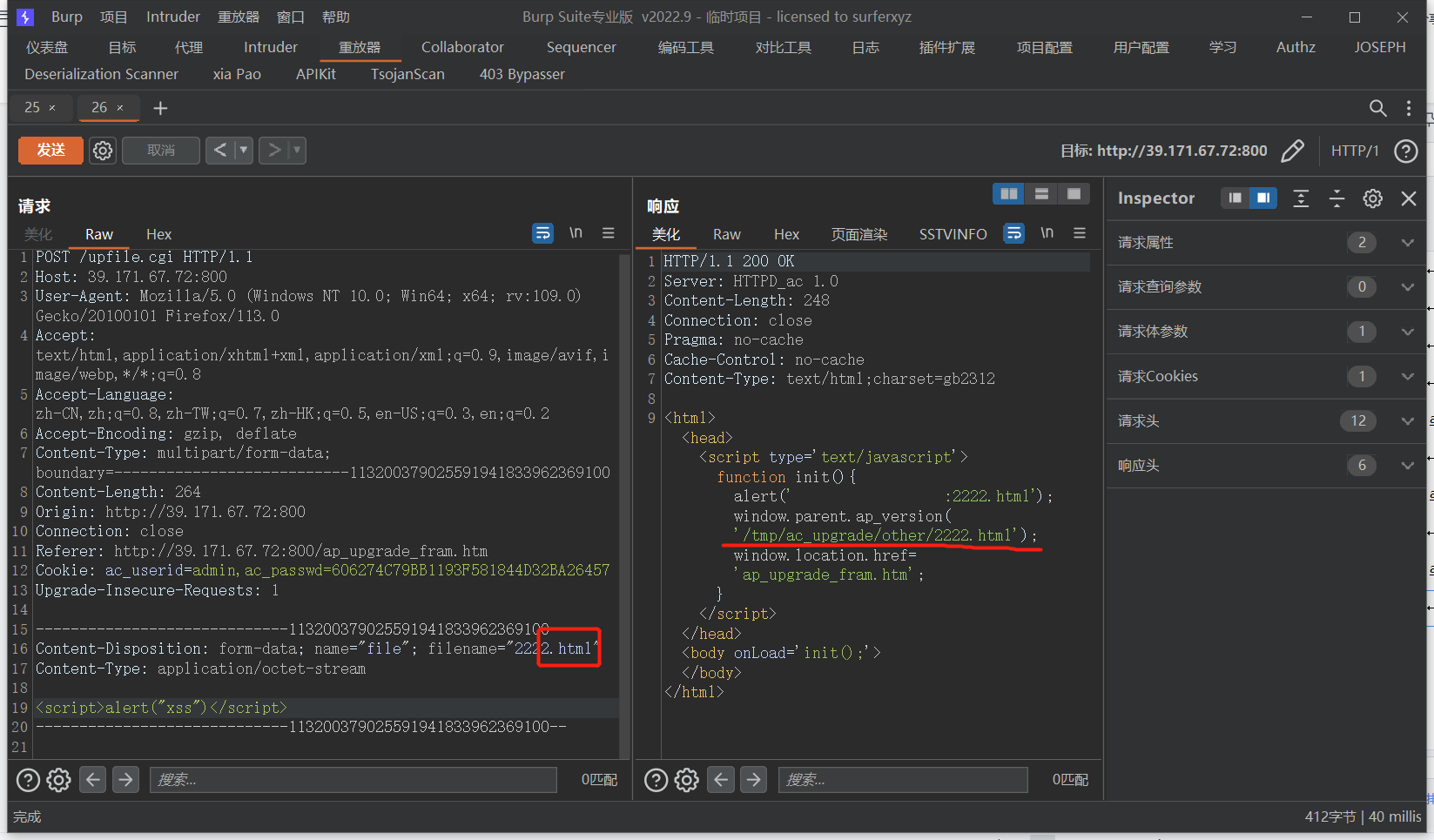
Then, we click to browse the file and need to upload a file with the suffix ".trx"

Finally, click on upload and we will use BurpSuite to intercept

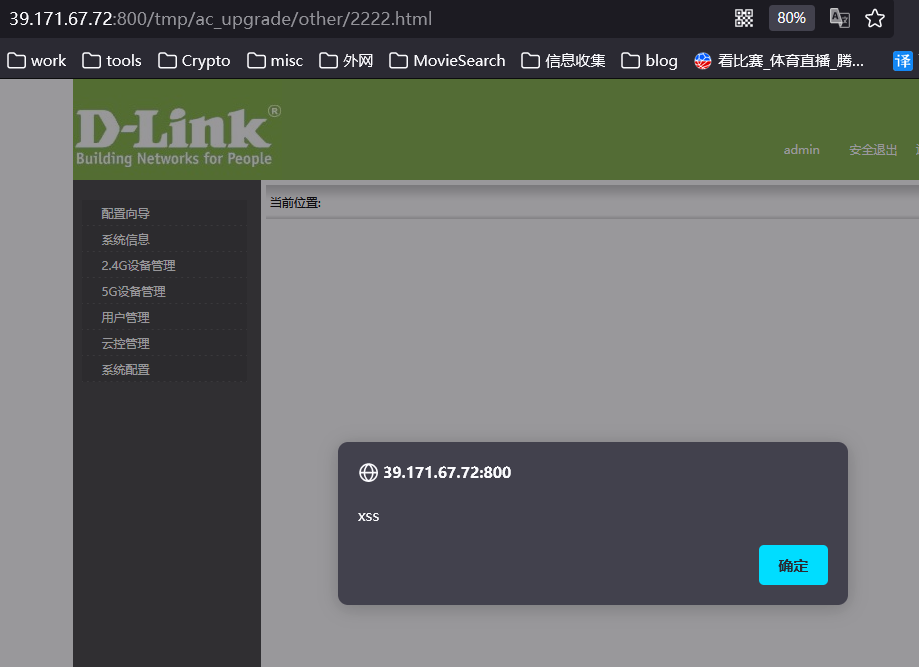




We need to change the suffix ". trx" marked in the diagram to ". html", and then proceed with the contract,

After the contract is awarded, there is a file path in the corresponding package for us to access

Finally, we can trigger by accessing this address



It is important that victims can access this url without login in.

