2099年的flag——writeup

原创

iRudy 于 2016-11-27 14:21:22 发布 1104 收藏
分类专栏： CTF 文章标签： CTF

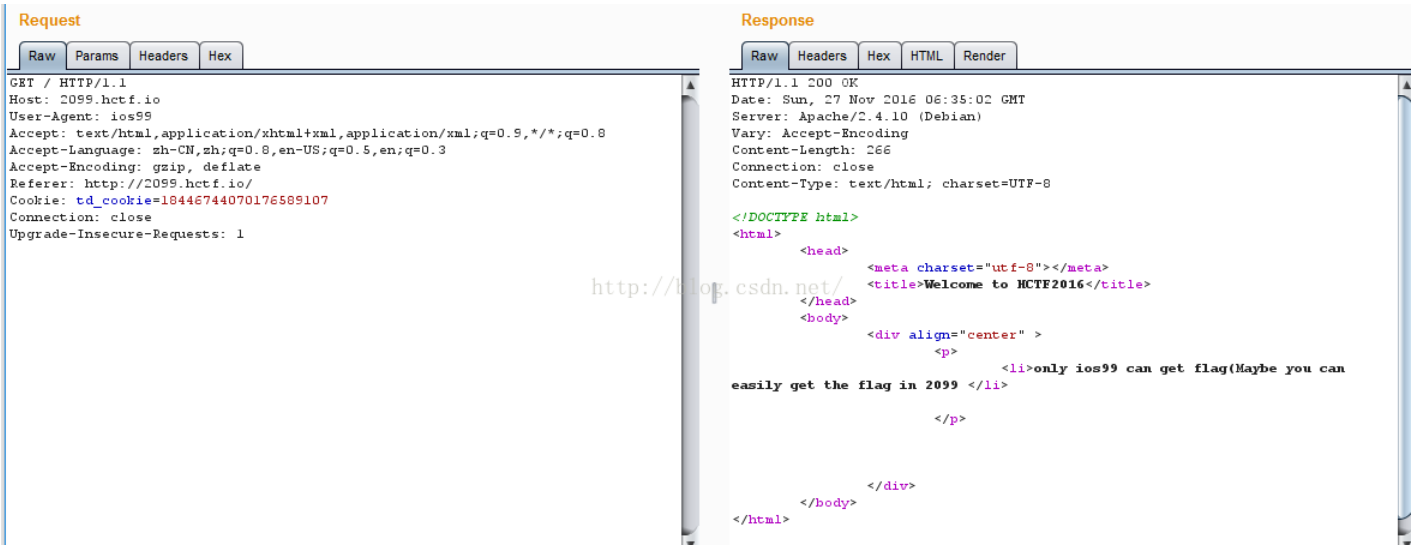
首先，根据提示，可以得到信息ios99,2099年，可以知道这两个应该是切入点

接着我们点开链接，还是这句话，查看源码，并没有得到什么其他信息，这个时候我们就需要用Burp Suite来查看下

请求

从请求和响应来看都没有什么重要的信息，也没有跳转，这个时候根据提示，我

用burp拦截修改user-agent,可是我这里修改为ios99,以及其他很多种情况，都没有出来flag，我甚至把电脑的时间改为2099年。。这里很久没有头绪。



Request

Raw | Params | Headers | Hex

```
GET / HTTP/1.1
Host: 2099.hctf.io
User-Agent: ios99
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://2099.hctf.io/
Cookie: td_cookie=18446744070176589107
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Sun, 27 Nov 2016 06:35:02 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 266
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
        <head>
                <meta charset="utf-8"></meta>
                <title>Welcome to HCTF2016</title>
        </head>
        <body>
                <div align="center" >
                        <p>
                                <li>only ios99 can get flag(Maybe you can
easily get the flag in 2099 </li>
                        </p>


                </div>
        </body>
</html>
```


卡了一段时间后，才想到自己简直智障，应该把user-agent更改为ios设备自动构造的请求信息，而不是单纯的自己编写！ok，直接上百度，复制

iphone 各版本的useragent，谁有发一下

barbell | 浏览 4963 次

最佳答案

发布于2015-05-07 15:58

●iOS

Mozilla/5.0 (iPhone; U; CPU like Mac OS X; en) AppleWebKit/420+ (KHTML, like Gecko) Version/3.0 Mobile/1C28 Safari/419.3

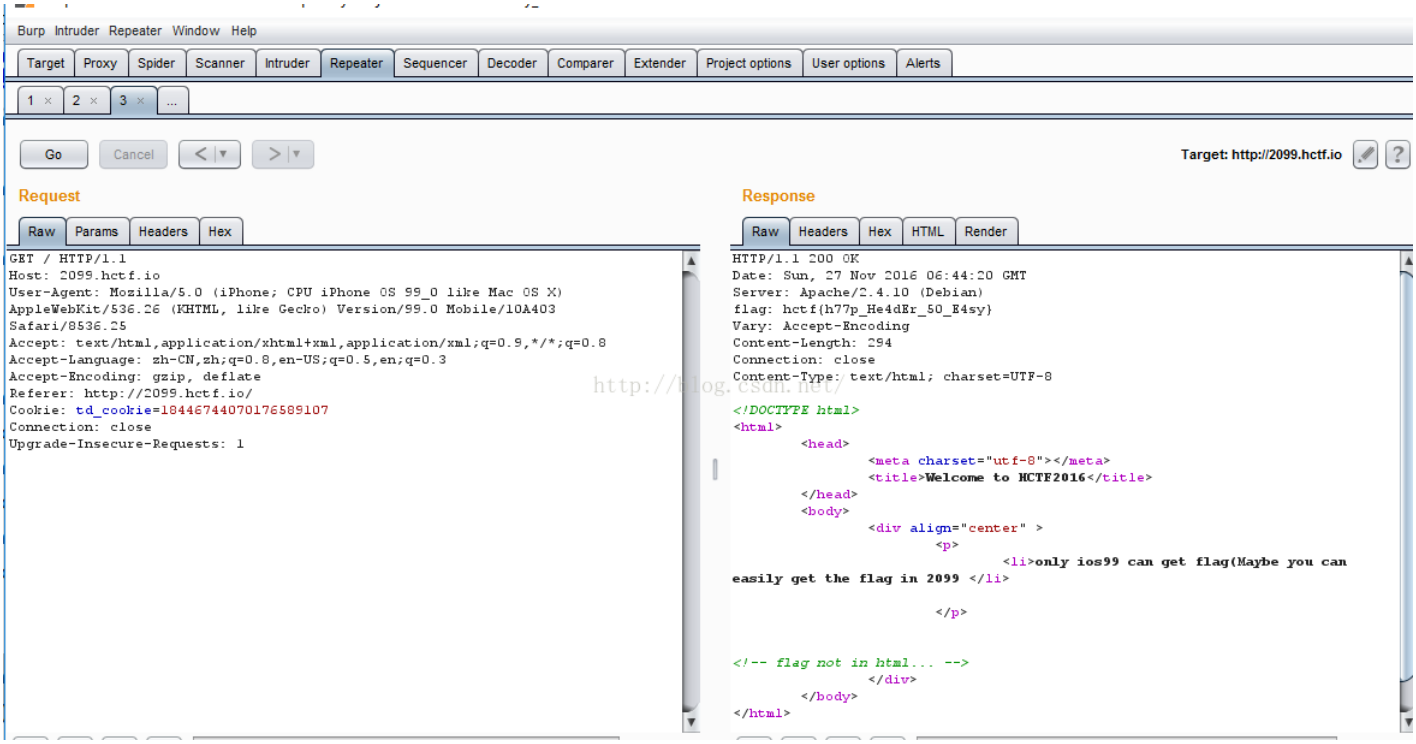
●iOS2

Mozilla/5.0 (iPhone; U; CPU iPhone OS 2_0 like Mac OS X; ja-jp) AppleWebKit/525.18.1 (KHTML, like Gecko) Version/3.1.1 Mobile/5A347 Safari/52

Mozilla/5.0 (iPhone; U; CPU iPhone OS 2_0 like Mac OS X; ja-jp) AppleWebKit/525.18.1 (KHTML, like Gecko) Version/3.1.1 Mobile/5A345 Safari/525.20

Mozilla/5.0 (iPhone; U; CPU iPhone OS 2_0_1 like Mac OS X; ja-jp) AppleWebKit/525.18.1 (KHTML, like Gecko) Version/3.1.1 Mobile/5B108 Safari/525.20

我们再重新用burpsuite提交，这里我我把OS 6_0,以及Version/6.0改为OS 99_0,以及Version/99.0，提交，OK，响应里终于出现了不一样的绿字flag not in html。这里有个问题我用ios2版本的信息修改不行，而用ios6的就行，其他的我没试过，所以有时候要多尝试几遍。



既然不在html里，那肯定在响应头里咯，找找看。果然，可以看到flag了，这道题就解决了。其实这道题很容易，主要是我做的题太少，有时候完全没思路。