2099年的flag——writeup



CTF 专栏收录该内容

2篇文章0订阅 订阅专栏

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

	答題	朝田		;			
本队token : ea9b2e09d753049649538bd11ffb5135iMsGbEbe							
^{66pt} 2099年的flag _任	10pt MIShttp://bi		已解决!				
only ios99 can get flag(Maybe	you can easily get the flag in	2099					
http://2099.hctf.io/ 35pt							
Web	MISC	Web	MISC				

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

(1) 2099.hctf.io				V 🕅 🗸	Q. 百度 <ctrl+k></ctrl+k>		☆ 自	ŧ	俞为	- 14 -	Aa	≡
🤌 最常访问 🛄 哔哩哔哩弹幕视频网 🋞	【推荐】逆向分析基… 📍	信息安全第一课 君君… 🏺	IDF实验室 CTF训练营	F FreeBuf.COM	M 关注 🔐 RCTF_XCTF_CTF	训练 🛞 X	CTF-Time(🕃 Web	Goat — OV	VASP		~
only ios99 can get flag(Maybe you can easily get the flag in 2099												

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,我们 ۰ III

Request Response

Raw Params Headers Hex

GET / HTTP/1.1 Host: 2099.hctf.io User-Agent: Mozilla/5.0 (Windows NT 10.0; W0W64; rv:49.0) Gecko/20100101 Firefox/49.0 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-Inngtage: 2n-Ch,2n,q-0.5,en-03, Accept-Encoding: gzip, deflate Referer: http://2099.hctf.io/ Cookie: td_cookie=18446744070176589107 Connection: close Upgrade-Insecure-Requests: 1

Þ

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。



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

⑦ iphone 各版本的useragent, 谁有发一下



•iOS

Mozilla/5.0 (iPhone; U; CPU like Mac OS X; en) AppleWebKit/420+ (KHTML, like Gecko) Ver sion/3.0 Mobile/1C28 Safari/419.3 http://blog.csdn.net/

•iOS2

Mozilla/5.0 (iPhone; U; CPU iPhone OS 2_0 like Mac OS X; ja-jp) AppleWebKit/525.18.1 (KH TML, 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 (KH TML, 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 (K HTML, 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。

		Target: http://2099.hctf.io			
Response					
Raw Headers	Hex HTML Render				
Name	Value				
HTTP/1.1	200 OK				
Date	Sun, 27 Nov 2016 06:44:20 GMT				
Server	Apache/2.4.10 (Debian)				
flag	hctf{h77p_He4dEr_50_E4sy}				
Vary	Accept-Encoding				
Content-Length	294				
Connection	htt <mark>close</mark> //blog.csdn.net/				
Content-Type	text/html; charset=UTF-8				
html					
<html></html>					
<head></head>					
	<pre><meta charset="utf-8"/> </pre>				
	<pre>>crere>weicome co Heikinte</pre>				
chadres					