CTF——常见密码

原创

Captain Hammer 于 2019-08-18 20:43:53 发布 7912 收藏 82
分类专栏： web安全 CTF 类型题总结

本文链接：https://blog.csdn.net/vhkjhwbs/article/details/99692399


web安全 同时被 2 个专栏收录
19 篇文章 5 订阅
订阅专栏


CTF 类型题总结
11 篇文章 35 订阅
订阅专栏

		CTF题中遇到的密码总结：		
序号	名称	密文	原文	备注
1	栅栏密码：	fg2ivyo}l{2s3_o@aw__rcl@	flag{w22_is_v3ry_cool}	所谓栅栏密码，就是把要加密的明文分成N个一组，然后把每组的第1个字连起来，形成一段无规律的话。 不过栅栏密码本身有一个潜规则，就是组成栅栏的字母一般不会太多。（一般不超过30个，也就是一、两句话） （用一定的规则把原文打乱然后用@连接）
2	md5	18414996c5377f5f4419a40eba901789	flag{hello_world!}	一般为32位 由数字和小写字母组成
3	base64	ZmxhZ3toZWxsb193b3JsZCF9IAo==	flag{hello_world!}	base64 的空格被加密成=
4	base16	666C61677B6D795F6E616D655F482121487D	flag{my_name_H!!H}	由数字和大写字母组成
5	base58	xpoetRPM7vtSVDSRGRp4nXv	flag{hello-world}	**Base58**是用于Bitcoin中使用的一种独特的编码方式，主要用于产生Bitcoin的钱包地址。相比Base64，Base58不使用数字"0"，字母大写"O"，字母大写"I"，和字母小写"l"，以及"+"和"/"符号。

		CTF题中遇到的密码总结：		
序号	名称	密文	原文	备注
6	base 91	@iH<,{bdR2H;i6*Tm,Wx2izpx2!	flag{554a5058c9021c76}	国外解密网站：https://www.dcode.fr/base-91-encoding
7	unicode	\u0066\u006c\u0061\u0067\u007b\u0069\u005f\u0077\u0069\u006c\u006c\u005f\u006b\u0069\u006c\u006c\u005f\u0079\u006f\u0075\u0021\u007d	flag{i_will_kill_you!}	万国码：每一字符都用一个5位字符编码表示，并用\分割
8	摩斯电码	-... -.- -.-. - ..-. -- .. ... -.-.	BKCTFMISC	相当于二进制编码
9	摩斯电码变形	0010 0100 01 110 1111011 11 11111 010 000 0 001101 1010 111 100 0 001101 01111 000 001101 00 10 1 0 010 0 000 1 01111 10 11110 101011 1111101	flag{}m0rse_code_1s_interest1n9!}	特点：由0和1组成，并且每段的长度不一样
10	OOK语言	Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.……	flag{ok-ctf-1234-admin}	OOK！是一种为红毛猩猩设计的编程语言。OOK！与众所周知的深奥语言BrainF ***基本上是同构的，但语法元素更少
11	OOK语言变形	.... !?!!. ?.... ....?.?! .?... .!..... ..... !.?.. ..... !?!!. ?!!!! !!?.? !.?!! !!!.. ....!.?..... ...!? !!.?. ....?.? !.?.. ..... .!.?. .... !?!!. ?!!!!!!!!! !?.?! .?!.? ....! ?!!.? ....?. ?!.?.	flag{bugku_jiami}	OOK！是一种为红毛猩猩设计的编程语言。OOK！与众所周知的深奥语言BrainF ***基本上是同构的，但语法元素更少。
12	Brainfuck语言	++++++++++[>+++++++>++++++++++>+++>+<<<<-]>++.>+.+++++++..+++.>++.<<+++++++++++++++.>.+++.------.--------.>+.>.	Hello World!	+ > < .] [-，8种符号
13	凯撒密码	明文字母表：ABCDEFGHIJKLMNOPQRSTUVWXYZ 密文字母表：DEFGHIJKLMNOPQRSTUVWXYZABC		特点： 在原来字符上进行一定的偏移
14	escape	flag%7Bi-will-kill-you%21%7D	flag{i-will-kill-you!}	
15	核心价值观编码	公正公正公正诚信文明公正民主公正法治法治友善平等和谐敬业和谐富强和谐富强和谐文明和谐平等公正公正和谐法治公正公正公正文明和谐民主和谐敬业和谐平等和谐敬业和谐敬业和谐和谐和谐公正法治友善法治	flag{90025f7fb1959936}	由核心价值观的12个词语组成的编码方式
16	sha1	7c2380341e0f03f81f873ab8d2ea5b88bc690793	flag{hello_world!}	40 位 由数字和小写字母组成

		CTF题中遇到的密码总结：		
序号	名称	密文	原文	备注
17	urlencode	%68%61%63%6b%65%72%44%4a	hackerDJ	**将需要转码的字符转为16进制**，然后从右到左，取4位(不足4位直接处理)，每2位做一位，前面加上%，编码成%XY格式。 比如： 空格ASCII码是32，对应16进制是20，那么urlencode编码结果是:%20,但在新标准中空格对应的是+,见RFC-1738 **默认：字母是不进行编码的**
18	当铺密码	羊由大井夫大人王中工	9158753624	当铺密码 [1] 就是一种将中文和数字进行转化的密码，算法相当简单:当前汉字有多少笔画出头，就是转化成数字几
19	rot13	Ubj pna lbh gryy na rkgebireg sebz na vagebireg ng AFN? In the elevators, the extrovert looks at the OTHER guy's shoes.	How can you tell an extrovert from an introvert at NSA? Va gur ryringbef, gur rkgebireg ybbxf ng gur BGURE thl'f fubrf.	ROT13是它自己本身的逆反；也就是说，要还原ROT13，套用加密同样的算法即可得，故同样的操作可用再加密与解密。该算法并没有提供真正的密码学上的保全，故它不应该被套用在需要保全的用途上。它常常被当作弱加密示例的典型
20	词频分析	Eg qnlyjtcnzydl z umaujejmjetg qeydsn eu z bsjdtx tw sgqtxegc al kdeqd mgeju tw yrzegjsoj zns nsyrzqsx kejd qeydsnjsoj Ew ltm fgtk jds kzl tw sgqtxegc m kerr csj jds wrzc kdeqd eu qrzuueqzr-qeydsn_eu_gtj_usqmnejl_du	In cryptography a substitution cipher is a ?ethod of encoding by which units of plaintext are replaced with ciphertext If you know the way of encoding u will get the flag which is classical-cipher_is_not_security_hs	一种加密方式，做攻防世界的时候遇到的， 在线解密： https://quipqiup.com/
21	jsfuck	`(![]+[])[+[]]+(![]+[])[!+[]+!+[]]+(![]+[])[+!+[]]+(![]+[+[]]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+`	flag{hhaj}	F12打开控制台 将密文复制进去，回车就可以得到 密码

		CTF题中遇到的密码总结：		
序号	名称	密文	原文	备注
22	decode HTML	LzExOS8xMDEvMTA4Lzk5LzExM	LzExOS8xMDEvMTA4Lzk5LzExM	

二 对称加密：

名称	条件（秘钥）	密文	明文	备注
DES	秘钥：6XaMMbM7	U2FsdGVkX18IBEATgMBe8NqjIqp65CxRjjMxXlIUxljBnAODJQRkSLQ/+IHBsjpv1BwwEawMo1c=	ctf{67a166801342415a6da8f0dbac591974}	DES）是一种对称密钥加密块密码算法，1976年被美国联邦政府的国家标准局确定为联邦资料处理标准（FIPS），随后在国际上广泛流传开来。它基于使用56位密钥的对称算法

三，常见文件头：

常见文件头信息

文件类型：	文件头信息：	文件尾信息：
JPEG (jpg)	**FFD8FFE0或FFD8FFE1或FFD8FFE8**	FF
PNG (png)	89 50 4E 47	00 3B
pdf	25 50 44 46 2D 31 2E	
Windows Password (pwl)	E3 82 85 96	
RAR	**52 61 72 21**	
ZIP Archive (zip)	50 4B 03 04	50 4B

文件类型：	文件头信息：	文件尾信息：
JPEG (jpg)	**FFD8FFE0或FFD8FFE1或FFD8FFE8**	FF
PNG (png)	89 50 4E 47	00 3B
pdf	25 50 44 46 2D 31 2E	
Windows Password (pwl)	E3 82 85 96	
RAR	**52 61 72 21**	
压缩包	PK	
Word/Excel (xls.or.doc)	D0 CF 11 E0	
HTML (html)	68 74 6D 6C 3E	
MIDI (mid)	4D 54 68 64	
7z	37 7A BC AF 27 1C	
GIF	47 49 46 38 39 61	
bmp	42 4D 76 68	