ctf常用密码总结

原创

favorhau 已于 2022-02-02 21:46:17 修改 1380 收藏 2
分类专栏： ctf求生之路 文章标签： 安全 web安全 哈希算法
于 2020-12-18 22:38:24 首次发布

作为入门的ctf玩家，需要懂得常用的密码。

说到密码，很多人会把MD5、base64等混淆在一起（~~包括我之前也会把md5称为“密码”~~）。其实严格区分起来，应该是：

- 加密(encipher/decipher)：加密传输信息，保证信息安全性，通过密钥和密文可以还原原始信息
- 编码(encode/decode)：将数据转化成某种固定格式的编码信息，方便不同系统间的传输，通过解码编码信息可以得到原始信息。
- 散列(hash)：也叫摘要或哈希，验证信息的完整性，不能通过哈希值还原原始信息。

比起系统学习各种密码（编码），更多的应该是在做题、项目中习得，比方说url编码、base64编码等就经常会被使用。

编码

常见的编码：ASCII（美国信息交换标准代码）、Base64、URL编码、HTML编码、Unicode编码、UTF-8、莫斯电码、二维码

- ASCII

  （American Standard Code for Information Interchange，美国标准信息交换代码）是基于拉丁字母的一套电脑编码系统，主要用于显示现代英语和其他西欧语言。它是现今最通用的单字节编码系统，并等同于国际标准ISO/IEC 646。

ASCII表

（ American Standard Code for Information Interchange 美国标准信息交换代码 ）

高四位 / 低四位		ASCII控制字符 0000 0						ASCII控制字符 0001 1						ASCII打印字符 0010 2		ASCII打印字符 0011 3		ASCII打印字符 0100 4		ASCII打印字符 0101 5		ASCII打印字符 0110 6		ASCII打印字符 0111 7		
		十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	Ctrl
0000	0	0		^@	NUL	\0	空字符	16	▶	^P	DLE		数据链路转义	32		48	0	64	@	80	P	96	`	112	p	
0001	1	1	☺	^A	SOH		标题开始	17	◀	^Q	DC1		设备控制 1	33	!	49	1	65	A	81	Q	97	a	113	q	
0010	2	2	☻	^B	STX		正文开始	18	↕	^R	DC2		设备控制 2	34	"	50	2	66	B	82	R	98	b	114	r	
0011	3	3	♥	^C	ETX		正文结束	19	‼	^S	DC3		设备控制 3	35	#	51	3	67	C	83	S	99	c	115	s	
0100	4	4	♦	^D	EOT		传输结束	20	¶	^T	DC4		设备控制 4	36	$	52	4	68	D	84	T	100	d	116	t	
0101	5	5	♣	^E	ENQ		查询	21	§	^U	NAK		否定应答	37	%	53	5	69	E	85	U	101	e	117	u	
0110	6	6	♠	^F	ACK		肯定应答	22	▬	^V	SYN		同步空闲	38	&	54	6	70	F	86	V	102	f	118	v	
0111	7	7	•	^G	BEL	\a	响铃	23	↨	^W	ETB		传输块结束	39	'	55	7	71	G	87	W	103	g	119	w	
1000	8	8	◘	^H	BS	\b	退格	24	↑	^X	CAN		取消	40	(	56	8	72	H	88	X	104	h	120	x	
1001	9	9	○	^I	HT	\t	横向制表	25	↓	^Y	EM		介质结束	41	)	57	9	73	I	89	Y	105	i	121	y	
1010	A	10	◙	^J	LF	\n	换行	26	→	^Z	SUB		替代	42	*	58	:	74	J	90	Z	106	j	122	z	
1011	B	11	♂	^K	VT	\v	纵向制表	27	←	^[	ESC	\e	溢出	43	+	59	;	75	K	91	[	107	k	123	{	
1100	C	12	♀	^L	FF	\f	换页	28	∟	^\	FS		文件分隔符	44	,	60	<	76	L	92	\	108	l	124	|	
1101	D	13	♪	^M	CR	\r	回车	29	↔	^]	GS		组分隔符	45	-	61	=	77	M	93	]	109	m	125	}	
1110	E	14	♫	^N	SO		移出	30	▲	^^	RS		记录分隔符	46	.	62	>	78	N	94	^	110	n	126	~	
1111	F	15	☼	^O	SI		移入	31	▼	^-	US		单元分隔符	47	/	63	?	79	O	95	_	111	o	127	⌂	^Backspace 代码：DEL

注：表中的ASCII字符可以用“Alt + 小键盘上的数字键”方法输入。

- Base64

  一般可以用来处理在HTTP环境下传递较长的标识信息

- URL编码

  这个是非常常见的 不能漏掉（相当于一种规范）

- Unicode

  Unicode是为了解决传统的字符编码方案的局限而产生的，它为每种语言中的每个字符设定了统一并且唯一的二进制编码，以满足跨语言、跨平台进行文本转换、处理的要求。

  ~~（其实一直对Unicode 、 gbk 、 utf-8 不理解，直到我看到了这个）传送门~~

  Unicode：OSI指定的编码标准；

  GBK：Chinese Internal Code Specification 汉字内码扩展规范

  UTF-8：一种针对Unicode的一种可变长度字符编码

- 其他编码

  ~~其实编码给我的感觉就是：无密码的密码~~

  剩下的还有诸如莫斯电码（不同网站出来的结果会不一样）、二维码这些。

加密

加密常规一般可以分为，对称性加密目前研究已经相对充分，而非对称性加密还有很长的路需要走。

- 对称性加密（symmetrical encryption）
- 非对称性加密（Asymmetric encryption）

对称性加密

“对称密钥”的加密算法主要有DES、TripleDES、RC2、RC4、RC5和Blowfish等。
以上的加密算法基本准寻以下算法特征：

1. 加密方和解密方使用同一个密钥；
2. 加密解密的速度比较快，适合数据比较长时的使用；
3. 密钥传输的过程不安全，且容易被破解，密钥管理也比较麻烦；

非对称加密

对称加密算法在加密和解密时使用的是同一个秘钥；而非对称加密算法需要两个密钥来进行加密和解密，这两个密钥是公开密钥（public key，简称公钥）和私有密钥（private key，简称私钥）
非对称性加密一般有：RSA、DSA、ECDSA。

说到非对称性加密 那就不得不说RSA了。

RSA

RSA公开密钥密码体制是一种使用不同的加密密钥与解密密钥，“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。
找了挺多的体制解释，比较好的是这个传送门
梳理了一下思路 大概上就分为四个步骤。

1. 选取素数n
2. 选取大整数e
3. 确定密钥d
4. 公开n和e保存d
   当然具体过程并没有那么简单。
   而如果要破解此加密的关键就是选取的*大素数n*无法被分解（目前仅能分解到2048位)
   但是
   {% cq %}2020年12月4日，中国科学技术大学宣布该校潘建伟等人成功构建76个光子的量子计算机九章{% endcq %}
   当然，要对付量子计算机，会有专门的量子密码~~（仅了解，虽然我也不懂具体是啥）~~
   诚然，从来就没有绝对的安全。安全都是相对的。

其他非对称性加密

对称性加密最经典的、以及最常见常用的应该是RSA。公钥密码体制采用的加密密钥(公开钥)和解密密钥(秘密钥)是不同的。由于加密密钥是公开的，密钥的分配和管理就很简单，而且能够很容易地实现数字签名，因此最适合于电子商务应用的需要。
其主要的优点是：
(1)密钥分配简单。
(2)密钥的保存量少。
(3)可以满足互不相识的人之间进行私人谈话时的保密性要求。
(4)可以完成数字签名和数字鉴别。
但在实际应用中，公钥密码体制并没有完全取代私钥密码体制，这是因为公钥密码体制在应用中存在以下几个缺点：
(1)公钥密码是对大数进行操作，计算量特别浩大，速度远比不上私钥密码体制。
(2)公钥密码中要将相当一部分密码信息予以公布，势必对系统产生影响。
(3)在公钥密码中，若公钥文件被更改，则公钥被攻破。
（摘自百度百科）

哈希

常见摘要：MD5、SHA1（主要适用于数字签名标准DSS里面定义的数字签名算法）
无论多长的一段数据经过MD5之后都会变成指定的长度。
把MD5称为“加密”应当是不准确的，MD（Message-Digest Algorithm）信息摘要算法
最直观的应该是MD5*不可逆*，~~（虽然有很多声称MD5破解的网站）~~
有MD5,也有MD4,MD2等。
目前没有软件能有效地破解 MD5。大多数时候只是把常见字符串的 MD5 存了起来为彩虹表，然后直接反查。
所谓”破解“的网站无非就是存了大量的可能密码。
比如 https://cmd5.com/

写在后面

CTF基本上看不懂的文字上面大都已经涵盖（可能只是小部分），在实战中（听说）还会出现诸如彩虹密码等*新型密码*，这就得看造化（yun qi）了。