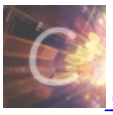
WeChall CTF Writeup（二）

原创

lmn_ 于 2022-02-25 21:54:03 发布 782 收藏

分类专栏： CTF 文章标签： CTF WeChall

本文链接：https://blog.csdn.net/weixin_43211186/article/details/123141845



以下题目标题组成：

[Score] [Title] [Author]

文章目录

0x06 1 Encodings: URL by Gizmore

题目意思：

你的任务就是去解码，一看就是url加密

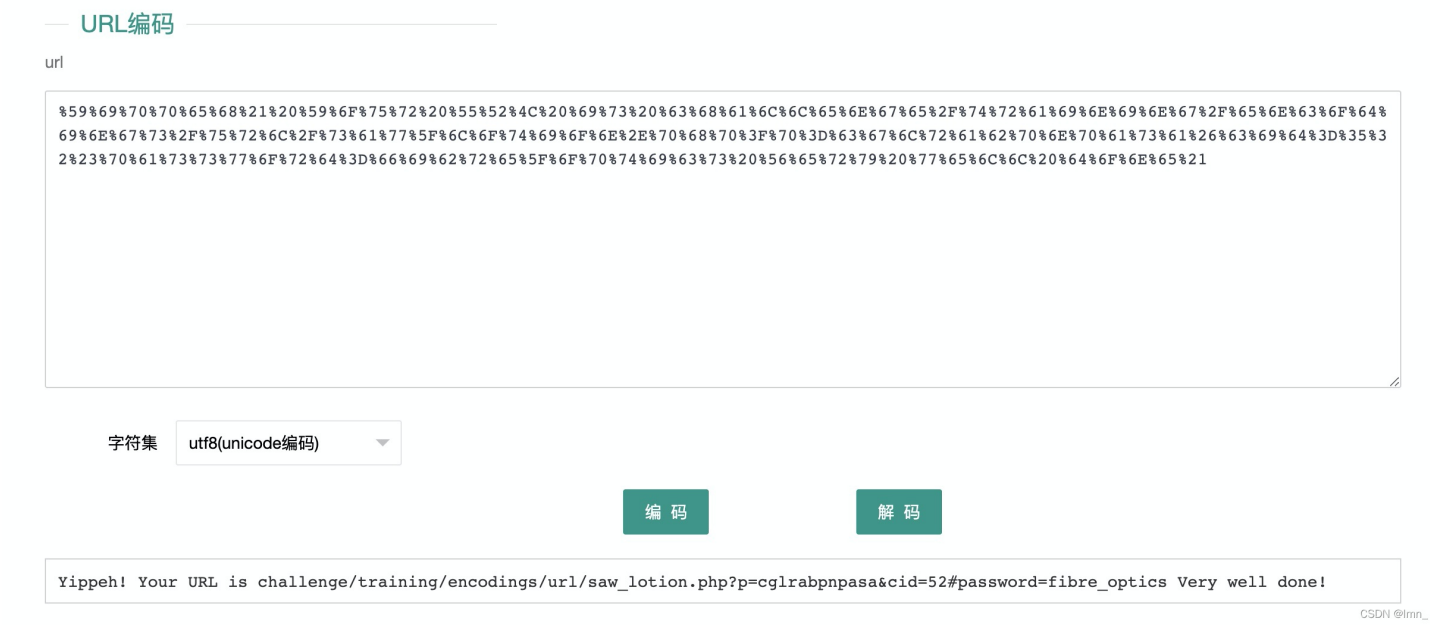
明文：

%59%69%70%70%65%68%21%20%59%6F%75%72%20%55%52%4C%20%69%73%20%63%68%61%6C%6C%65%6E%67%65%2F%74%72%61%69%6E%69%6E%67%2F%65%6E%63%6F%64%69%6E%67%73%2F%75%72%6C%2F%73%61%77%5F%6C%6F%74%69%6F%6E%2E%70%68%70%3F%70%3D%63%67%6C%72%61%62%70%6E%70%61%73%61%26%63%69%64%3D%35%32%23%70%61%73%73%77%6F%72%64%3D%66%69%62%72%65%5F%6F%70%74%69%63%73%20%56%65%72%79%20%77%65%6C%6C%20%64%6F%6E%65%21

解密网站：

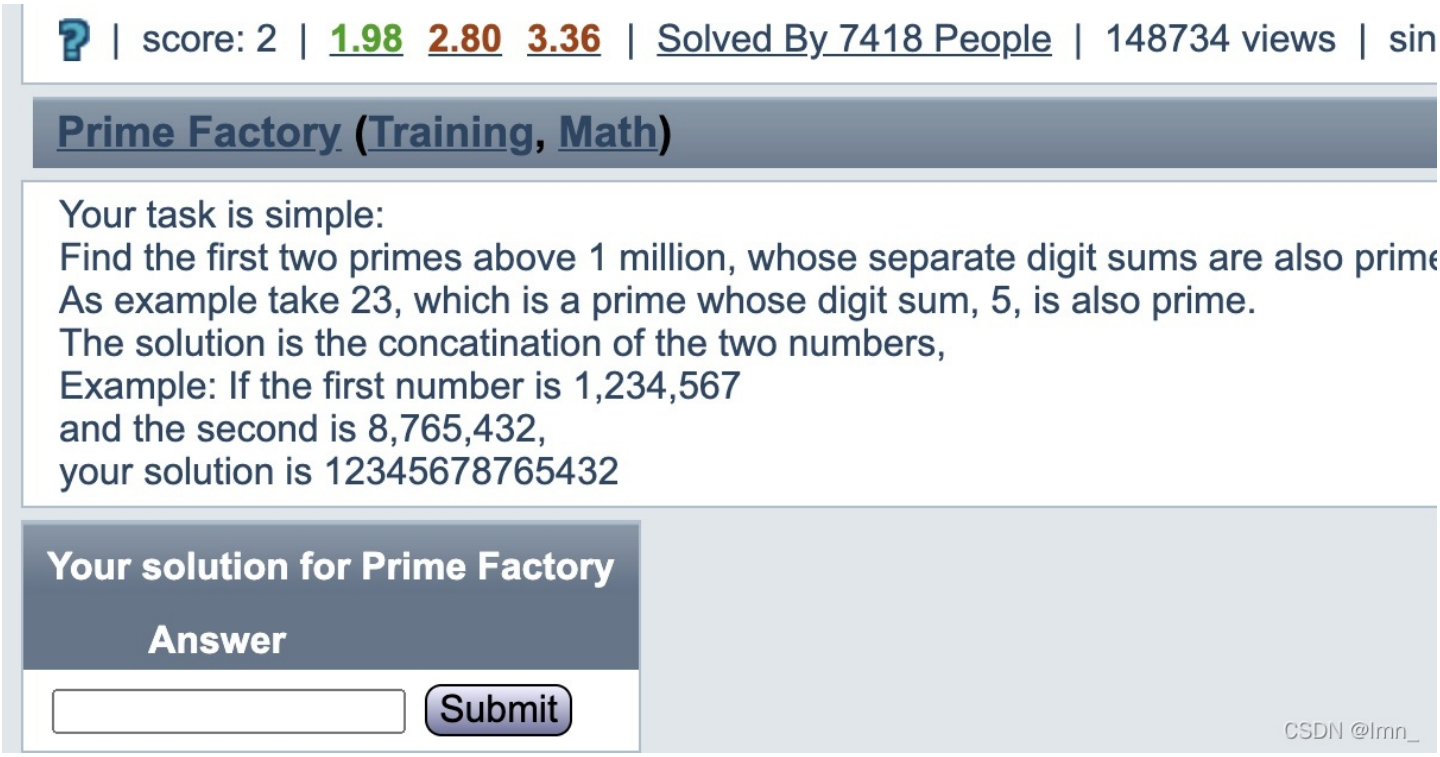
http://www.hiencode.com/url.html

密文：



Yippeh! Your URL is challenge/training/encodings/url/saw_lotion.php?p=cglrabpnpasa&cid=52#password=fibre_optics Very well done!

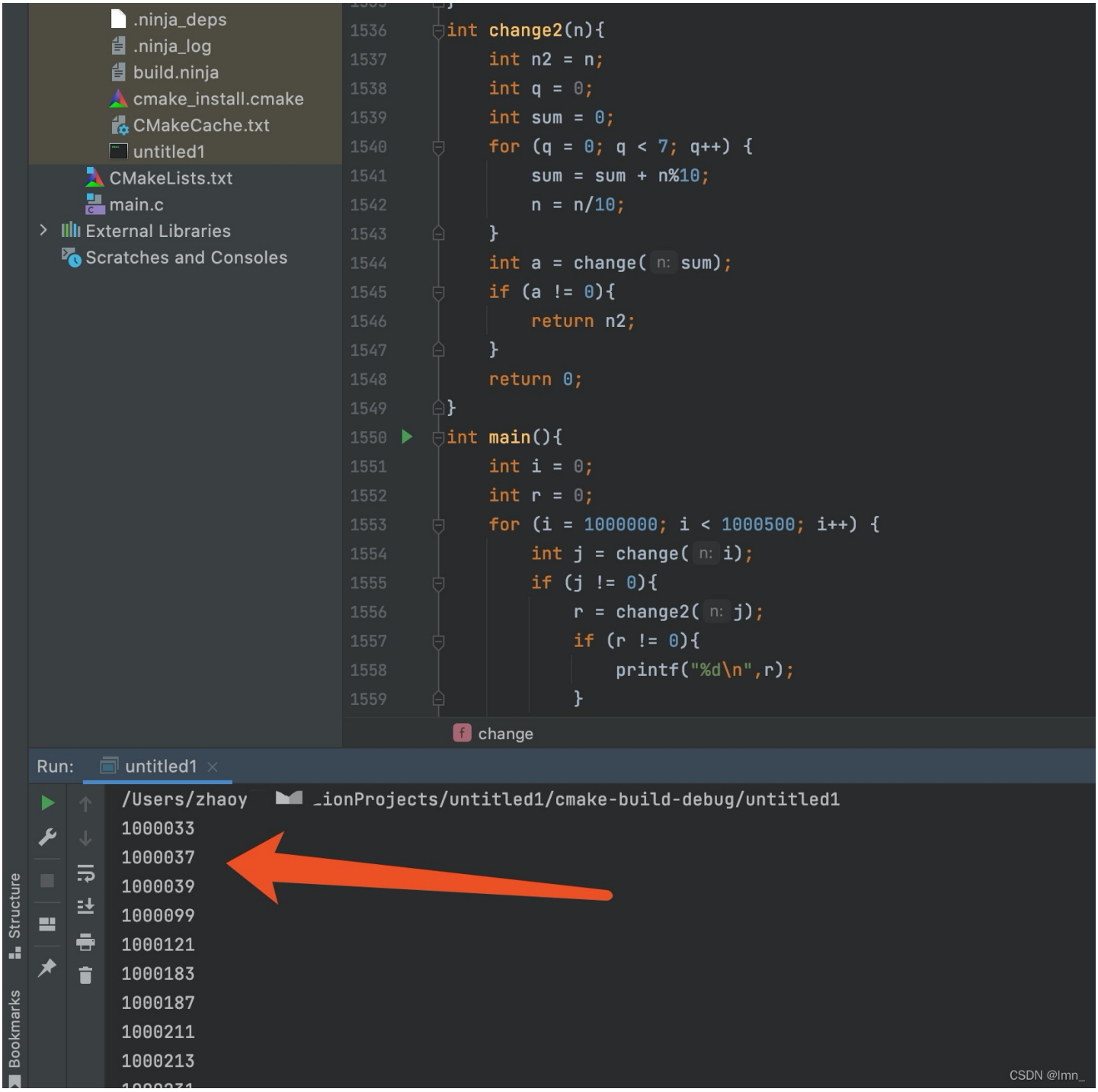
0x07 2 Prime Factory by ch0wch0w



题目意思：
你的任务很简单：
找出 100 万以上的前两个素数，它们的单独数字和也是素数。
以 23 为例，它是一个素数，其数字和 5 也是素数。
解决方案是两个数字的连接，
例如：如果第一个数字是 1,234,567
，第二个是 8,765,432，则
您的解决方案是 12345678765432

思路：只要找出1000000+的随便两个素数并且每个位加起来也是素数的两个素数拼在一起就是result
随便写了个比较啰嗦的C代码

```
int change(int n){
    int m = 0;
    for (m = 2; m < n; m++) {
        if (n % m == 0){
            return 0;
        }
    }
    return n;
}
int change2(n){
    int n2 = n;
    int q = 0;
    int sum = 0;
    for (q = 0; q < 7; q++) {
        sum = sum + n%10;
        n = n/10;
    }
    int a = change(sum);
    if (a != 0){
        return n2;
    }
    return 0;
}
int main(){
    int i = 0;
    int r = 0;
    for (i = 1000000; i < 1000500; i++) {
        int j = change(i);
        if (j != 0){
            r = change2(j);
            if (r != 0){
                printf("%d\n",r);
            }
        }
    }
}
```



0x08 2 Training: Encodings I by Gizmore

| score: 2 | 3.35 4.33 3.93 | Solved By 4925 People | 111209 views | since Jun 18, 2008 - 21:41:30

Training: Encodings I (Training, Encoding)

We intercepted this message from one challenger to another, maybe you can find out what they were talking about.
To help you on your progress I coded a small java application, called JPK.
Note: The message is most likely in english.

```
10101001101000110100111100110100
00011101001100101111100011101000
10000011010011110011010000001101
11010110111000101101001111010001
00000110010111011101100011110111
11100100110010111001000100000110
00011110011110001111010011101001
01011100100000101100111011111110
10111100100100000111000011000011
11001111100111110111110111111100
10110010001000001101001111001101
00000110010111000011110011111100
11110011111010011000011110010111
01001100101111100100101110
```

Your solution for Training: Encodings I

Answer

Submit

题目意思：
我们从一个挑战者那里截获了这条消息，也许你可以找出他们在说什么。
为了帮助您取得进展，我编写了一个名为JPK的小型 Java 应用程序。
注意：该消息很可能是英文的。

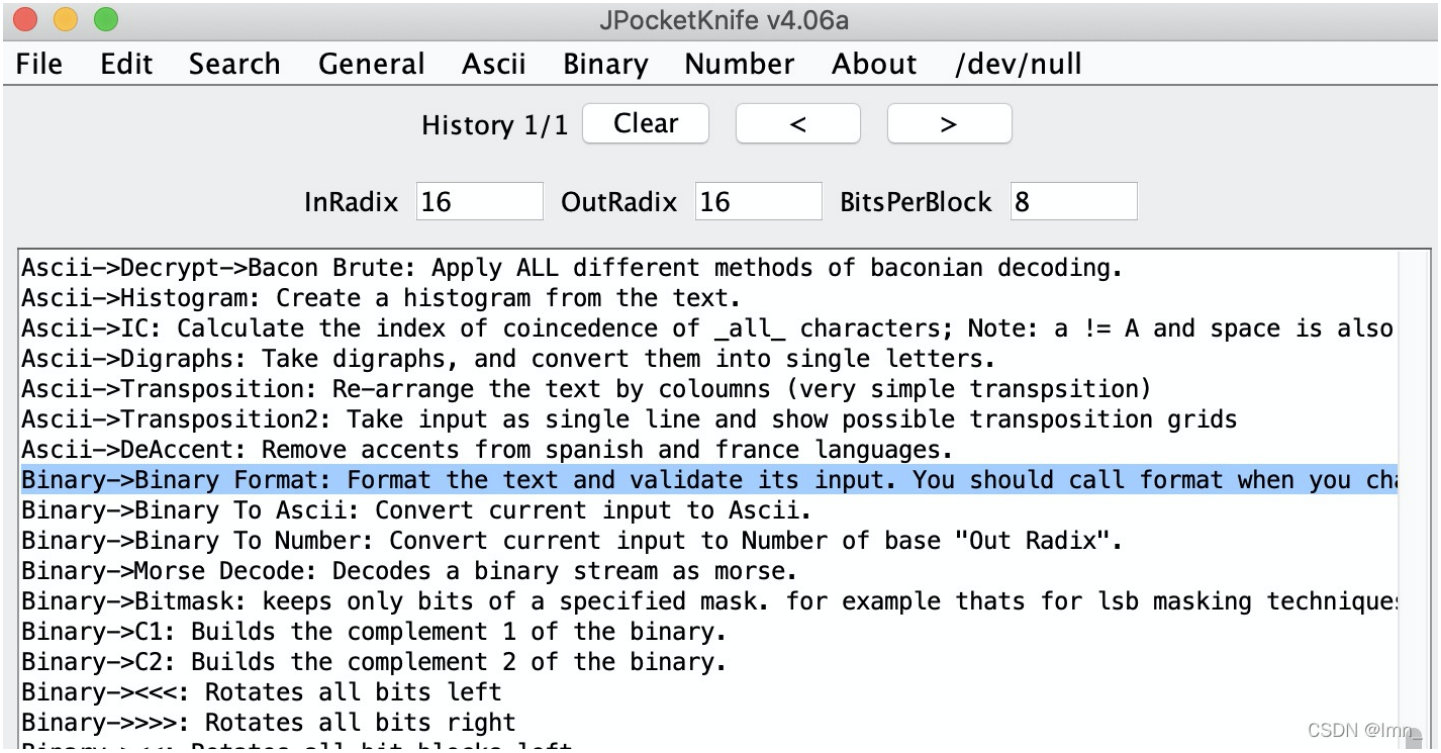
密文：
10101001101000110100111100110100
00011101001100101111100011101000
10000011010011110011010000001101
11010110111000101101001111010001
00000110010111011101100011110111
11100100110010111001000100000110
00011110011110001111010011101001
01011100100000101100111011111110
10111100100100000111000011000011
11001111100111110111110111111100
10110010001000001101001111001101
00000110010111000011110011111100
11110011111010011000011110010111
01001100101111100100101110

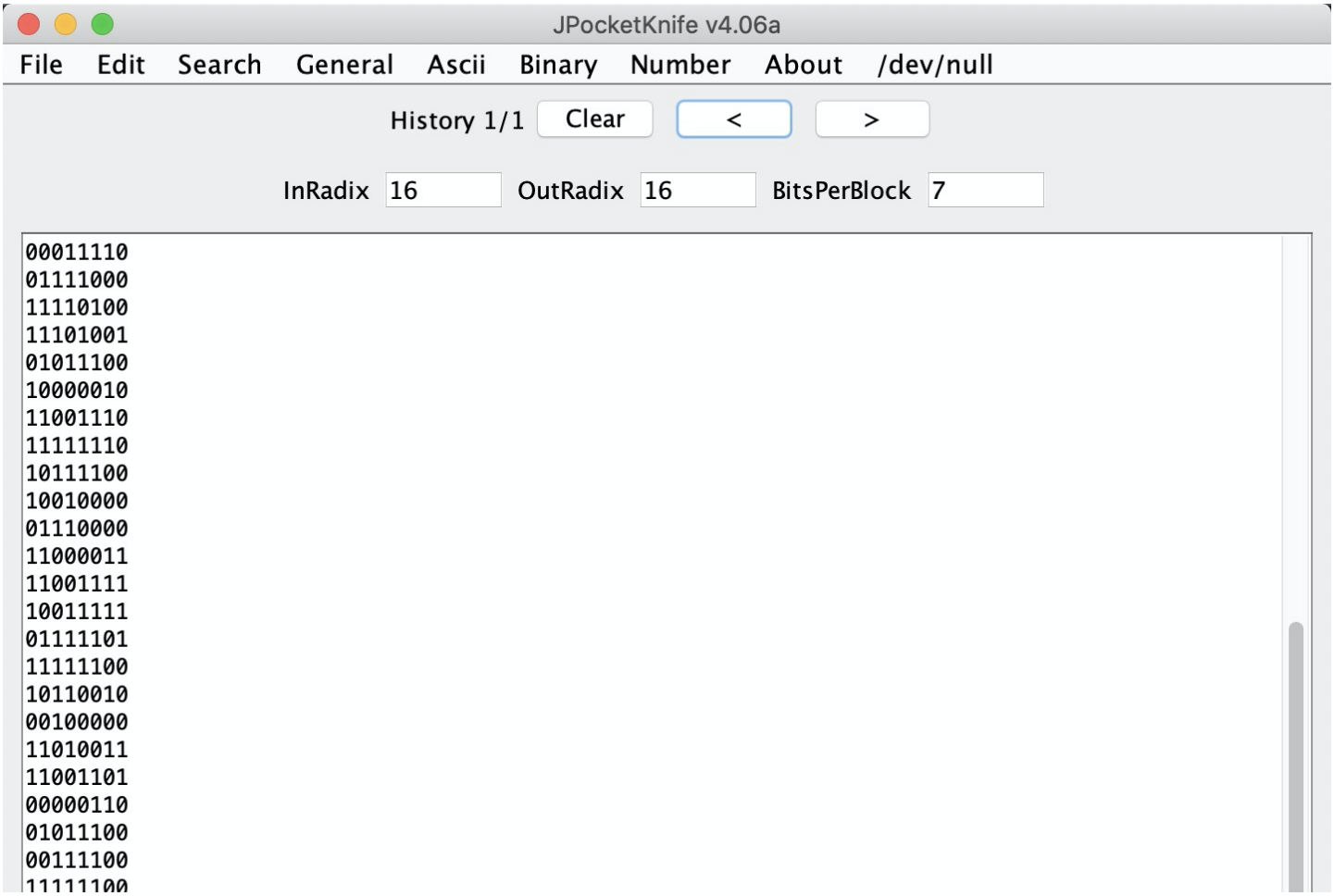
我们下载他提供的jar工具

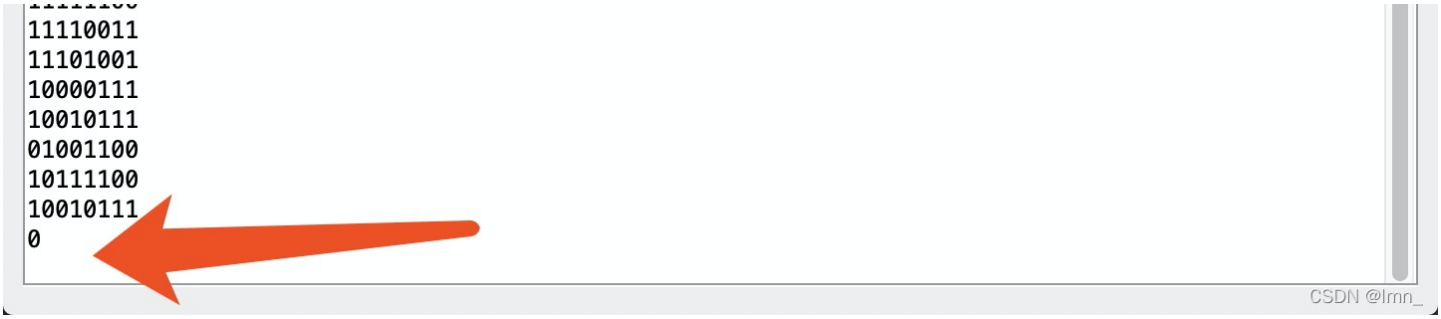
Now this is JPK,
feel free to peek the source at JPK.jar
The jar will also run as standalone application.


This page has been viewed 64289 times.
CSDN @lmn_

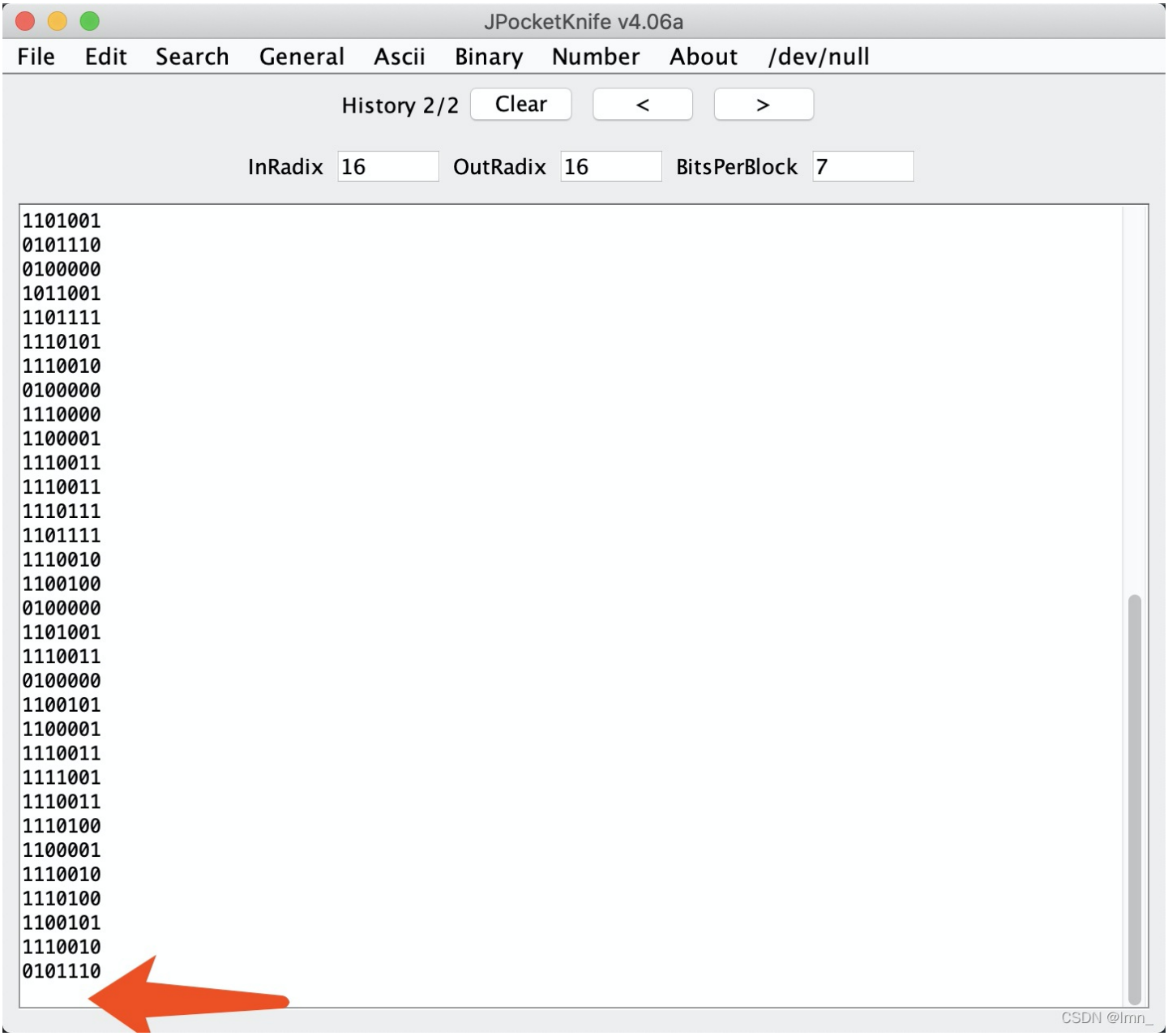
从帮助里找到这么一条

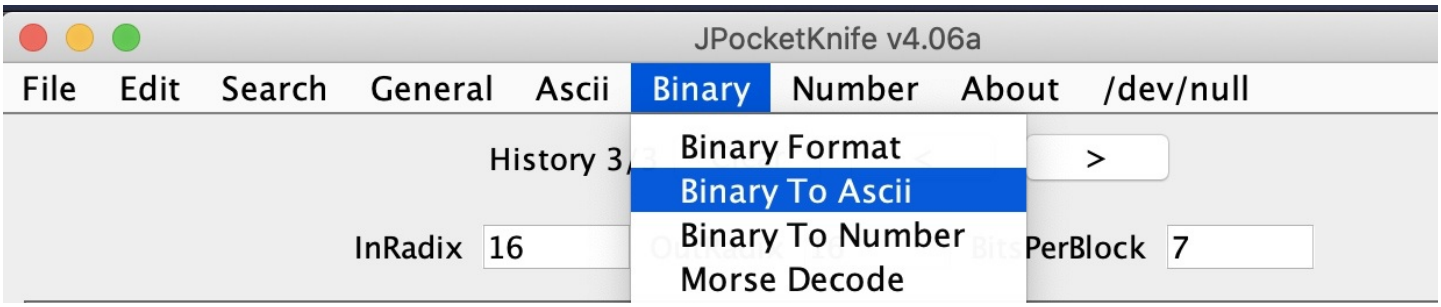

JPocketKnife v4.06a
File Edit Search General Ascii Binary Number About /dev/null
History 1/1 Clear < >
InRadix 16 OutRadix 16 BitsPerBlock 8
Ascii->Decrypt->Bacon Brute: Apply ALL different methods of baconian decoding.
Ascii->Histogram: Create a histogram from the text.
Ascii->IC: Calculate the index of coincedence of _all_ characters; Note: a != A and space is also
Ascii->Digraphs: Take digraphs, and convert them into single letters.
Ascii->Transposition: Re-arrange the text by coloumns (very simple transpsition)
Ascii->Transposition2: Take input as single line and show possible transposition grids
Ascii->DeAccent: Remove accents from spanish and france languages.
Binary->Binary Format: Format the text and validate its input. You should call format when you ch
Binary->Binary To Ascii: Convert current input to Ascii.
Binary->Binary To Number: Convert current input to Number of base "Out Radix".
Binary->Morse Decode: Decodes a binary stream as morse.
Binary->Bitmask: keeps only bits of a specified mask. for example thats for lsb masking technique
Binary->C1: Builds the complement 1 of the binary.
Binary->C2: Builds the complement 2 of the binary.
Binary-><<<: Rotates all bits left
Binary->>>>: Rotates all bits right
CSDN @lmn_

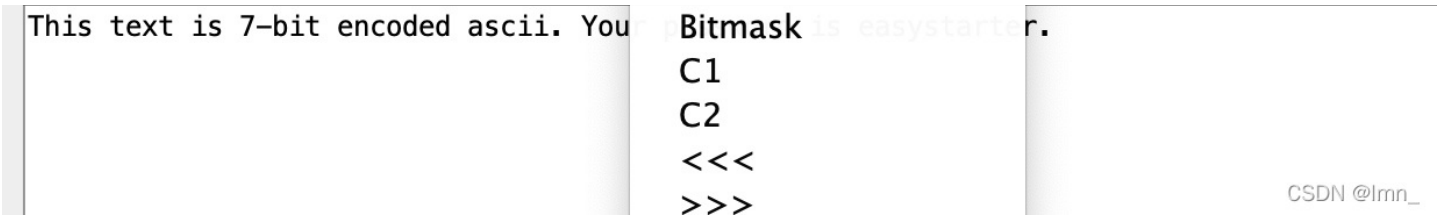

JPocketKnife v4.06a
File Edit Search General Ascii Binary Number About /dev/null
History 1/1 Clear < >
InRadix 16 OutRadix 16 BitsPerBlock 7
00011110
01111000
11110100
11101001
01011100
10000010
11001110
11111110
10111100
10010000
01110000
11000011
11001111
10011111
01111101
11111100
10110010
00100000
11010011
11001101
00000110
01011100
00111100

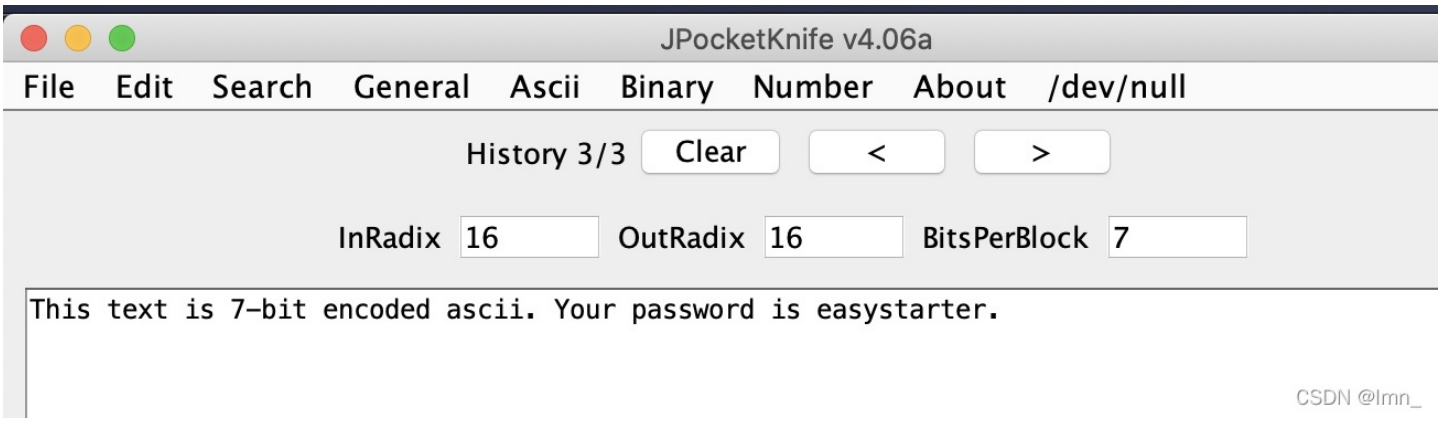


每行8个还多出来一个，那就每行7个，因为可以7位或8位二进制转ASCII







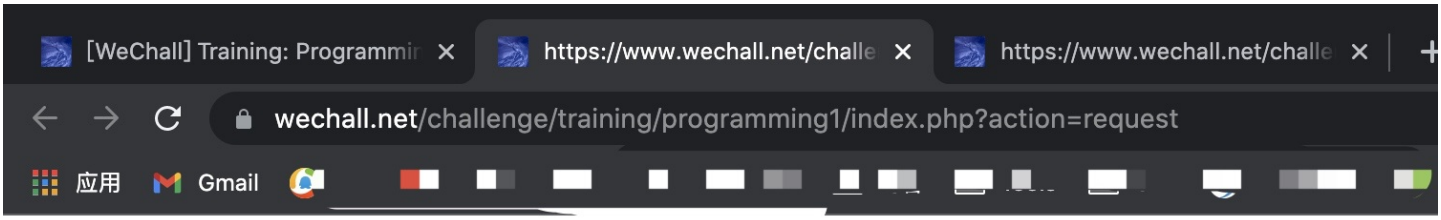


This text is 7-bit encoded ascii. Your password is easystarter.

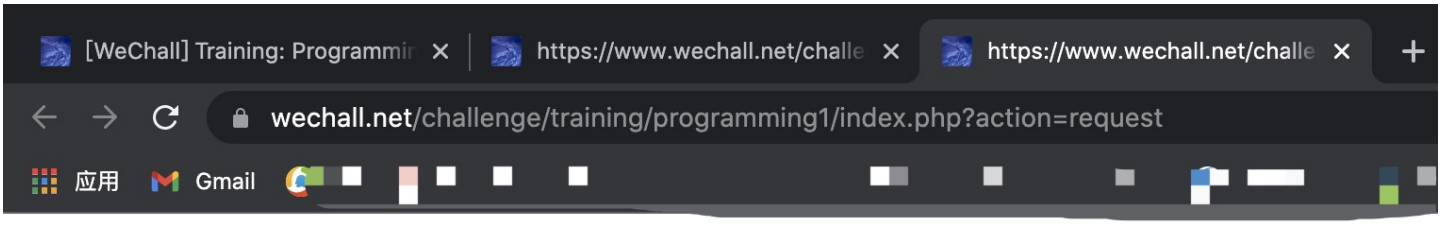
0x09 2 Training: Programming 1 by Gizmore

题目意思：
当您访问此链接时，您会收到一条消息。
将相同的消息提交回 https://www.wechall.net/challenge/training/programming1/index.php?answer=the_message
您的时间限制是 1.337 秒

点开this page为



ysJtHYH7vXvf



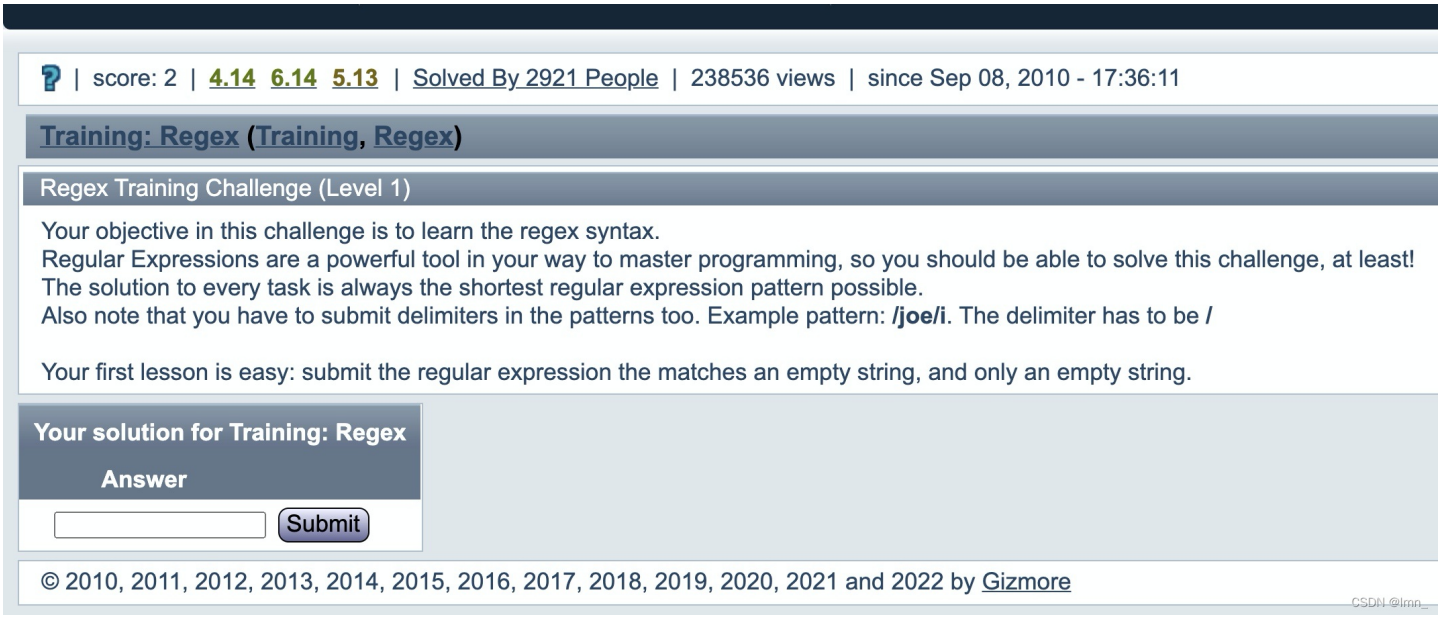
dd5x5Shlai

可以看到为动态码

python实现

```
import urllib.request
import http.cookiejar
import webbrowser
url1 = "http://www.wechall.net/challenge/training/programming1/index.php?action=request"
url2 = 'http://www.wechall.net/challenge/training/programming1/index.php?answer='
header = {}
req = urllib.request.Request(url1,headers = header)
req.add_header('Cookie','WC=16296850-61988-XXXXXXXXXXXXXXXX')
message = urllib.request.urlopen(req).read().decode('utf-8')
url2 = url2+message
webbrowser.open(url2)
```

0x10 2 Training: Regex by Gizmore



题目意思：

您在本次挑战中的目标是学习正则表达式语法。

正则表达式是您掌握编程的强大工具，因此您至少应该能够解决这个挑战！

每个任务的解决方案总是尽可能最短的正则表达式模式。

另请注意，您也必须在模式中提交分隔符。示例模式：/joe/i,分隔符必须是/

Level 1

你的第一课很简单：提交匹配一个空字符串的正则表达式，并且只有一个空字符串。

条件：1、一个空字符串 2、只有一个

特别字符	描述
$	匹配输入字符串的结尾位置。如果设置了 RegExp 对象的 Multiline 属性，则 $ 也匹配 '\n' 或 '\r'。要匹配 $ 字符本身，请使用 \$。
()	标记一个子表达式的开始和结束位置。子表达式可以获取供以后使用。要匹配这些字符，请使用 \(和 \)。
*	匹配前面的子表达式零次或多次。要匹配 * 字符，请使用 *。
+	匹配前面的子表达式一次或多次。要匹配 + 字符，请使用 \+。
.	匹配除换行符 \n 之外的任何单字符。要匹配 . ，请使用 \. 。
[	标记一个中括号表达式的开始。要匹配 [，请使用 \[。
?	匹配前面的子表达式零次或一次，或指明一个非贪婪限定符。要匹配 ? 字符，请使用 \?。
\	将下一个字符标记为或特殊字符、或原义字符、或向后引用、或八进制转义符。例如， 'n' 匹配字符 'n'。'\n' 匹配换行符。序列 '\\' 匹配 "\"，而 '\(' 则匹配 "("。
^	匹配输入字符串的开始位置，除非在方括号表达式中使用，当该符号在方括号表达式中使用时，表示不接受该方括号表达式中的字符集合。要匹配 ^ 字符本身，请使用 \^。
{	标记限定符表达式的开始。要匹配 {，请使用 \{。
|	指明两项之间的一个选择。要匹配 |，请使用 \\|。

字符	描述
\cx	匹配由x指明的控制字符。例如， \cM 匹配一个 Control-M 或回车符。x 的值必须为 A-Z 或 a-z 之一。否则，将 c 视为一个原义的 'c' 字符。
\f	匹配一个换页符。等价于 \x0c 和 \cL。
\n	匹配一个换行符。等价于 \x0a 和 \cJ。
\r	匹配一个回车符。等价于 \x0d 和 \cM。
\s	匹配任何空白字符，包括空格、制表符、换页符等等。等价于 [\f\n\r\t\v]。注意 Unicode 正则表达式会匹配全角空格符。
\S	匹配任何非空白字符。等价于 [^ \f\n\r\t\v]。
\t	匹配一个制表符。等价于 \x09 和 \cI。
\v	匹配一个垂直制表符。等价于 \x0b 和 \cK。

空字符 != 空白字符

答案为：/^$/

Level 2

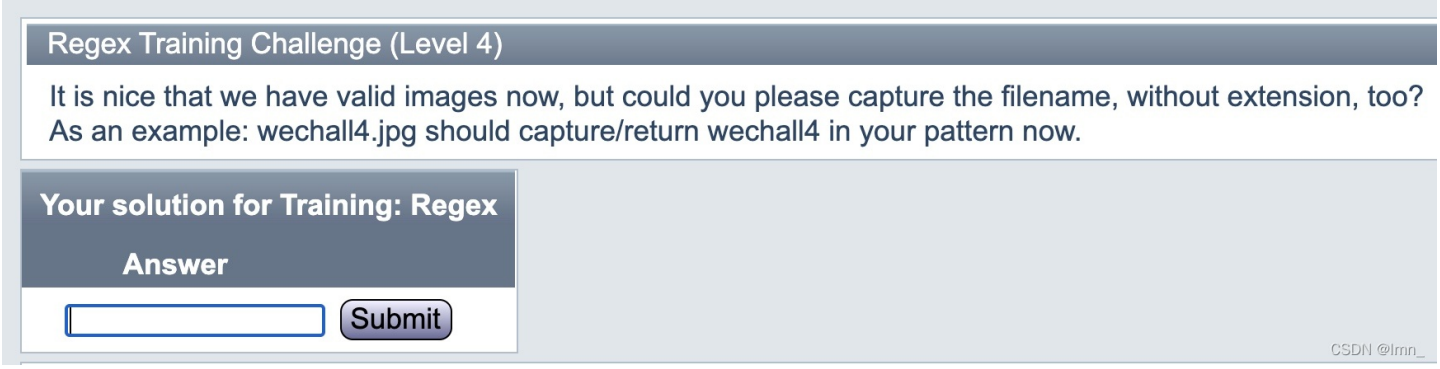
匹配”wechall”，/^wechall$/

Level 3

题目意思：
匹配静态字符串不是正则表达式的主要目标。
您的下一个任务是提交与某些图像的有效文件名匹配的表达式。
您的模式应匹配名称为 wechall.ext 或 wechall4.ext 和有效图像扩展名的所有图像。
有效的图像扩展名是 .jpg、.gif、.tiff、.bmp 和 .png。
以下是一些有效文件名的示例：wechall4.tiff、wechall.png、wechall4.jpg、wechall.bmp

/^wechall4?.(?:jpg|gif|tiff|bmp|png)$/

Level 4



题目意思：
很高兴我们现在有有效的图像，但是您能否也捕获文件名，不带扩展名？
例如： wechall4.jpg 现在应该在您的模式中捕获/返回 wechall4。

需要对文件名添加捕获分组
/^(wechall4?).(?:jpg|gif|tiff|bmp|png)$/