# 基本溢出

## 什么是基本溢出

首先来看概念。字符串的长度是第一个NUL的位置（从0数起）。例如，31 00的长度是1，00的长度是0。光标位置＞长度时，就叫基本溢出，此时光标在NUL的后面。

一般来说，光标不能移动到NUL后面，因为当下一个字符是00时，再按$在数学模式中会移动到最左边，在线性模式中没有操作。

## 基本溢出的方法

1. 字符转换器。在31 FE 00中，只要从最左边开始连按两下$，就会到达FE 00右边，达成基本溢出。
2. (框)。框和它右边的字符是“绑定”的，在框左边按$会连续跳过两个字符，包括字符00。因此只要框在最后，就能用它达成基本溢出。提示：字符是q8R21，字符是Jn。刷框的办法除了字符转换器以外，还有一种，6÷2，不断输入根号直到无法再输入，在根号内填入1，移至最右端，输入:（Qy），sr=!，最后删去框右侧的括号即可。
3. 线性模式中的∑(溢出法。需要使用CALC。
4. 输入𝒙=AAin▸cm（q811），令初值A为199，对𝒙求解，C!。cw没有字符转换器也没有CALC，只有这种方法可以得到基本溢出。
5. 当算式中存在连续两个F开头的字节时，报错后按!可能导致溢出。此方法不稳定，需谨慎使用。

## 插入和删除

在上一章中，我们并没有仔细学习插入和删除的逻辑，只是感性理解了一下。这一章要细讲这个问题。

### 插入

先讲插入。假设现在字符串的总长度是L，从左侧第一个字符开始计算，到从左向右第一个00为止，不包括这个00；记最左侧坐标为0，每向右一个字节坐标加一，则光标的坐标为P，字节位置算法同理，最左侧的字节是第零个字节；插入的字符长度N。（如果在框上插入，因为插完后框就没了，所以N要减一）那么会进行三个操作：

1. 第L+N个字节设为00
2. 把[P, L)移动到[P+N, L+N)，空出[P, P+N)
3. [P, P+N)设为要插入的字符，光标移动到P+N

这个算法一般来说工作良好，可以完美实现需要的操作。但在基本溢出时却达不到应有的效果。例如，在31|33 34 00中插入32，此例中L=3，P=1，N=1：

31|33 34 00 ?? ?? ?? ... //?表示此字节值不确定

31|33 34 00 00 ?? ?? ...

31|\_\_ 33 34 00 ?? ?? ...

31 32|33 34 00 ?? ?? ...

但是在31 00 32|34 35 00中插入33，L=1，P=3，N=1：

31 00 32|34 35 00 ...

31 00 00|34 35 00 ... //由于P＞L，并不会移动字符

31 00 00 33|35 00 ...

可见有两个效果，第一，产生了一个NUL，第二，新字符直接替换了旧字符。第二点可以用来便捷快速地把双字节字符变成单字节字符，第一点可以用来去除双字节字符的后一个字节，得到字符转换器。例如，在框上按$，然后q.q.!!o，就可得到字符转换器：

|19 00 00 00 00 00 00 ...

19 00|00 00 00 00 00 ...

19 00 FD 18|00 00 00 ...

19 00 FD 00 FD 18|00 ... //注意前一个FD18的18变成00了

19 00|FD 00 FD 18 00 ...

19|FD 00 FD 18 00 00 ... //删除了单字节字符00

还记得吗，数学模式中在最左边处按!，会移动到第一个NUL处。按!直至移至最左端，再按!，然后输入(q8R26)：

19 FD|00 FD 18 00 00 ...

19 FD FE 20|00 00 00 ...

!!$移动到FE和20之间，输入1，o：

19 FD FE|20 00 00 00 ...

19 FD FE 31|20 00 00 ...

19 FD|20 00 20 00 00 ...

这就是通过基本溢出得到字符的办法。注意，数学模式中字符00后面的东西都不可见，线性模式中NUL后面的东西不可见。由于此处的操作都在字符00后面，因此输入的字符和光标都是看不到的，需要同学们做好规划。另外，数学模式下的“撤销”功能只会恢复到第一个NUL为止，后面的东西不能恢复，所以同学们一定要小心，按错了是没有补救机会的。

### 删除

接下来讲删除。删除比较简单，从当前字符到下一个字符00所有的字符都向左复制即可。有两点需要注意：

第一，如果删除的字符长度＞1，删除就会有残留：

31 FD 18|32 33 00 ...

31|32 33 00 33 00 ... //复制[32 33 00]并覆盖了32，但33没覆盖

一般来说这不要紧，但它却是后面数学模式字符复制的基础。

第二，和插入不同，删除是以光标右侧第一个字符为起点，一直向右到第一个字符00为止，将这一串字符向左复制。因此字符转换器的基本溢出和其他基本溢出在这里体现出区别：

31|FE 00 32 33 00 ...

|FE 00 32 33 00 00 ... //FE00不包含字符00，FE00，32，33，00四个字符被复制

而

31|19 00 32 33 00 ...

|19 00 00 32 33 00 ... //19后面是字符00，只有19和00被复制

## 第一章例题

1. 用框得到字符。

**参考思路：**我们知道通过基本溢出可以覆盖掉双字节字符的前一个字节。在框上按$进入基本溢出，输入字符。

19 00 FD 18|00 ...

!，输入字符“1”：

19 00 31|18 00 ...

这样FD就被覆盖了。然后两次o，删掉31和00，离开基本溢出，就得到了字符。

1. 用框得到到。

**参考思路：**思路和上一个一样，只要覆盖就行。在框上按$进入基本溢出，输入5个1：

19 00 00 31 31 31 31|00 00 00 ...

输入(q73u)，然后!!：

19 00 00 00 31 31 31 FD 3F|00 ...

19 00 00 00 31 31|31 FD 3F 00 ...

输入(q73x)，覆盖掉31FD，然后!!：

19 00 00 00 31 31 FD 3E|3F 00 ...

19 00 00 00 31|31 FD 3E 3F 00 ...

如此重复，直到输入(q737)，然后按一次!：

19 00 FD 3A|3B 3C 3D 3E 3F 00 ...

19 00|FD 3A 3B 3C 3D 3E 3F 00 ...

现在输入1覆盖掉FD，然后o两次：

19 00 31|3A 3B 3C 3D 3E 3F 00 ...

19|3A 3B 3C 3D 3E 3F 00 00 00 ...

就得到了到。回忆一下上一章讲的字符转换器，有一道例题也是这个，相比之下，基本溢出的按键数比字符转换器少一些。因此基本溢出适合打大量字符，而少量字符用字符转换器更方便。

在长200字节的输入区后面，紧接着还有一个同样长度的回放区，上一章提到过，按=,r,qr或J进行一次计算（即使报错了也没关系）会把输入区的内容复制到回放区（到NUL为止），C后按!或$会把回放区重新复制到输入区。一般来说回放区不能直接接触到，因为当输入区长度达到199字节时，就不能再输入字符。然而，基本溢出时输入的字符因为在NUL后面，不计入长度，所以可以通过基本溢出来使输入长度大于199字节，从而摸到回放区。这可以用来复制字符。例如，刷出框后，在框前输入任意式子，按=把式子复制到回放区（冒号表示输入区的末尾），然后在框前打很多字直到打不下，然后移动到框后面，进入基本溢出：

... xx|xx 19 00:xx xx ...

... xx xx 19 00|xx xx ...

按o删掉00：

... xx xx 19|xx:xx xx ...

把之前垫的字符都删掉，这样就把回放区的字符都“接”到了输入区，完成了一次复制。复制完以后，末尾依然有框，如有需要还能按=继续复制。这也是线性模式中复制字符的主要办法。

1. 尝试按上述方法复制字符串1+1。

**参考结果：**1+1□1+1□（复制结束后最初的框依然存在，如需消除可在该框内输入任何字符然后删除）

**参考思路：**见上文，不再赘述。

## 附：对回放区进行处理

基本溢出还能对回放区的字符进行后期处理，这是字符转换器做不到的。例如，你有一个字符串A6 FD 3A A6 FD 3B A6，假设这是个不好打的字符，你希望在不干扰的前提下，把FD3A和FD3B变成3A和3B。做法是，首先准备好字符转换器，放在历史记录里，然后输入那个字符串，按=把它存入回放区。接下来，找到字符转换器，用它刷出框，在它前面打满字（在数学模式，可以打一大堆分数线，会快一点），然后删掉一个字节：

19 00|00:A6 FD 3A A6 FD 3B A6 00 ...

删掉一个是因为，如果不删，字符串的长度就是199，那就不能再输入新东西了。现在输入1（不能只按$，会回到最左边）：

19 00 31|A6 FD 3A A6 FD 3B A6 00 ...

这样就摸到了回放区，按$跳过需要保留的A6，输入1把FD盖掉，再删除1：

19 00 31:A6|FD 3A A6 FD 3B A6 00 ...

19 00 00:A6 31|3A A6 FD 3B A6 00 ...

19 00 00:A6|3A A6 FD 3B A6 00 00 ...

以此类推，把下一个FD也删掉：

19 00 00:A6 3A A6|3B A6 00 00 00 ...

按C!，回放区的内容就会复制到输入区，这样就得到了想要的A6 3A A6 3B A6。各位思考一下，同样是基本溢出，这里为什么绕了一步，先把字符转换器变成框才能做呢？

原因是，刚才讲删除的时候说过，如果直接用字符转换器的话，打满字以后删掉一个，会使得后面的字符全都往前移：

xx|FE 00:A6 FD 3A A6 FD 3B A6 00 ...

|FE 00 A6:FD 3A A6 FD 3B A6 00 00 ...

其实，打满字再删一个只是为了让字符串的长度正好为198。仔细观察可以发现，长度达到190时，光标会变得很粗，提示你即将打满。如果用字符转换器，垫到光标变粗时开始数字符，正好数到198，那也可以。（注：如果显示出来的字符串超过200字节很多，在数学模式中有时会直接崩溃死机，所以保险起见还是建议用框）