CTF 从入门到提升系列课程

为什么是从入门到放弃呢？（开个玩笑）

如果说大家对 CTF 有了解的话，其实应该知道 CTF 是一个什么类型的比赛，这个比赛涉及的范围和影响有多大，自然是不言而喻的。因此如果说你真的想打好比赛，那也是真的非常不容易的，所以说这是非常困难的一件事情，初期可能学着学着就想放弃了，所以我就以这个来作为一个标题，当然本意不是让大家去放弃，就是为了让大家入个门然后再提升！ 我会和我朋友一起来完成这门课程的讲解。

课程主要针对 web MISC 密码学，内容会尽可能多地去覆盖常见比赛中涉及到的一些考点解题技巧等，我们会先举例简单的考点考题作为案例来讲解一下。 这样的大家在学的同时可以上手做一个实验，便于理解和掌握。大家有什么问题可以留言做一个反馈，我会回复大家的。

我们进入正式课程，说到 CTF 它是什么有什么故事呢？以下是百度百科的定义：

CTF（Capture The Flag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF 起源于 1996 年 DEFCON 全球大会，以代替之前们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式。

DEFCON 作为 CTF 赛制的一个发源地，DEFCON CTF 成为了目前全球最高技术水平的和影响力的一个 CTF 竞赛，类似于 CTF 赛场中的“世界杯”。

关于比赛模式

常见的竞赛模式我这里只举了两种（百度百科上还提到了第三种就是混杂模式），我们就先看前两种：

第一种是解题模式，解题模式的话其实比较好理解，给我们一道题目去做一个解答。

参赛人员可以通过线上或线下去解出一个题目，解出题目后，你会拿到一个叫做 flag 的一个东西，那么你就要去提交这个 flag，如果你的 flag 是正确的你就会得分，类似于常规竞赛。很多比赛中如果你是前三名，比如说拿到一血二血三血这样子，你会有一个额外的一个加分；也会有其他的赛制，一道题目解出的人越多得分值就会越低（可以理解为解出的人多题就简单嘛）。

第二种攻防模式，攻防模式指参赛队伍在整个网络环境中做相互的攻防，每个队伍它都会拿到一台属于他们自己的服务器。首先你要对它做一个加固，因为其他队伍会来攻击你的服务器，如果攻击成功他们就会做一些操作，如果顺利可能获得一个 flag，那么他们就得分，所以你要给自己的服务器做好防守，同时你也可以根据上述流程去攻击别人的服务器，获得 flag。

关于比赛规则

比赛的时间周期可长可短，长的有 48 小时短的可能几个小时，比赛中时间会刷新，比如我有一个漏洞，按道理来说我们刷到一个漏洞，可以一直利用下去，那就可以一直得分了，其实并不是这样子的，它有个轮数限制，每一轮我设置成 5 分钟或者 15 分钟，你在一个目标服务器上，在规定时间内只能得一次分，过了这十分钟之后，那么你才能进行第二次得分，这种竞争就会非常的激烈，每一分每一秒你都你都有可能被人超过，或者你都有可能去超过别人。 如果你发现一个别人都没有补过的漏洞，那你就可以会全拿整个分数。

比赛的规则很多样，如果你把别人的服务器宕机掉了，在一些规则中是要扣分的。你即使不得分，你也会让别人失分，变相的会建立一些优势。

有些比赛中会检测 CPU 的使用率，如果服务器比较卡顿，会被认定该服务器不能正常服务，就会减分，所以说整个比赛中规则很多样，没有具体的非常标准化的规则，因比赛而异。

百度百科上提到的第三种是混杂模式，其实就是先解题得基础分，然后再进行攻防。但是实际比赛中，会有各种各样的需求，还有防守形式，那种的话就像是谁先攻占，谁先防守，然后看看时间长短。还有一种是每人一台服务器，我们做攻击，看对方的加固，目前国内还有一种工控形式的比赛。 给你一套正常的一套类似现实中的工控环境，对它进行渗透获取 flag，这种会更有趣一点。相信在之后 CTF 的赛制规则会越来越多，越来越有趣。

题型:

1、MISC

属于杂项，比如说你不知道该怎么分的时候，你就把它往杂项里丢。常规杂项包括哪些类型呢？首先第一个就是我们常说的隐写术，就是信息隐藏技术信息隐藏的话，你可以把信息隐藏在很多的东西中，比如说图片文件音频视频等等一系列都是可以的，然后你要通过非常多的技术手段分析，或者说配合工具的一些使用，去找到你要的一些消息，去获取到这样的一个 flag。

2、PPC

PPC 是一个编程类的，编程类的话就比如说就像之前前段时间有个五子棋比赛，你要把他下赢了才能够拿分，那你要么可以自己下，把它下赢也是没问题的；要么你就可以自己去写一个编程机器人去跟他做个对抗，去赢得比赛；通过编程来实现打分的形式，这种题目不会非常多的。

3、CRYPTO

CRYPTO 是密码学的题型，给你一串密文，去猜它使用了哪些加密方式，提取出你需要拿到的那个 flag 就可以。

4、REVERSE

REVERSE 是逆向的，对 windows 或者 Linux 的一个破解，这里的话因为现在移动安全也比较火，那么现在还会有衍生出来非常多的移动安全的题目，就类似安卓逆向等等。

5、PWN

基于程序的一个逻辑分析

6、WEB

我们就是常见的 web 狗，CTF 鄙视链的低端（哈哈哈哈哈）。web 的题型就非常多啦，

CTF 赛事

DEFCON CTF （CTF 赛事中的“世界杯”，往年都是美国夺冠，去年是韩国的战队）

日本的 SECCON 赛题也非常的难

XCTF 全国联赛

其他各种赛事

我们都会先去找一些网上可以你们可以访问到的题目。后期，比如说各种点都讲完了，会把这点混在一起，去找一些那种国际事国际赛事，或者是国内知名赛事，就相对来说难度大一些的，或者说是一些他们交流的，交就会内部交流的一些题目，或者说还有那种就是某些爱好者自己放出了一个挑战赛之类的这种题型，会拿出来给大家做一个分享。

然后除了国际赛的话，国内也有很多，比如说 XCTF 就是它的全国联赛，它有一站一站可以打过去。然后除了这些知名赛事之外，其实还有很多那种小赛事，你也别小看它，其实很多题目也都挺有意思的。这些题少，但是也可以去关注一下。

然后下面给大家推荐 2 个网站：

```
https://www.xctf.org.cn/ctfs/all/
https://ctftime.org/
```

会介绍国内国际上的要举行的一些 CTF 赛事的一些时间等等信息，一些战队的一些排名，像刚提到的 SECCCON 日本的黑客大会，都可以去了解一下。ctftime.org 是对一个在国际上比较重要的赛事的做一些记录，而且会还会给出赛事的一些权重，以及对这种 CTF 知名战队的一些排名，就可以去了解一下。

要提升自己的实力，开始入门尝试去找一些能够上手去练习的地方。因为其实如果一开始你直接去打各种比赛，都做不出来就很受打击，所以的话一开始的练习是非常重要的。那么这里就减给了一些那种你能够去练习的一些站点，

找地方练练手：

合天	http://www.hetianlab.com/
实验吧	http://www.shiyanbar.com/ctf/
i春秋	https://www.ichunqiu.com/
Bugku	http://ctf.bugku.com/
Xctf平台	http://oj.xctf.org.cn/
蓝鲸安全	http://whalectf.xin/
Jarvis OJ	https://www.jarvisoj.com/

如果说技术不太好的话，可以都看一看，都上手去试一试。

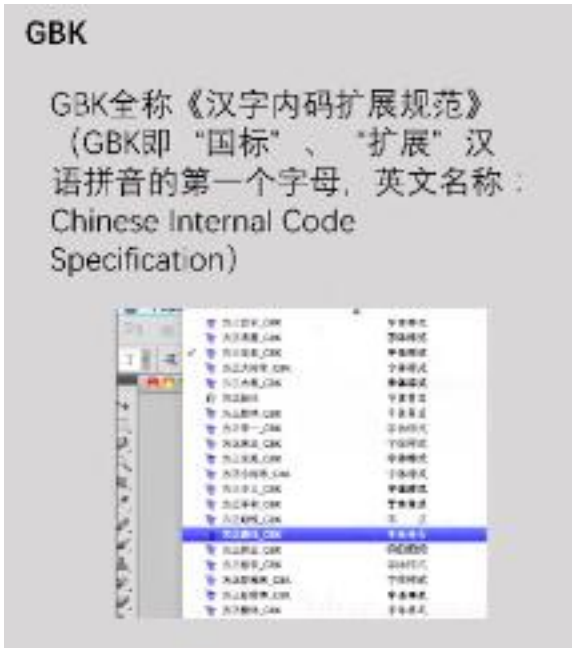
宽字节注入

首先对 sql 注入做一个系列的课程讲解。它是一个系列，因为它内容涉及非常多，就会一点一点地讲下去。一开始我先会讲关于一个宽字节的一个注入，因为宽字节相对来说比较简单，同时也就是即使你不会在这个地方你通过对宽字节注入的了解，你也大致能够了解基本注入的一个方式。

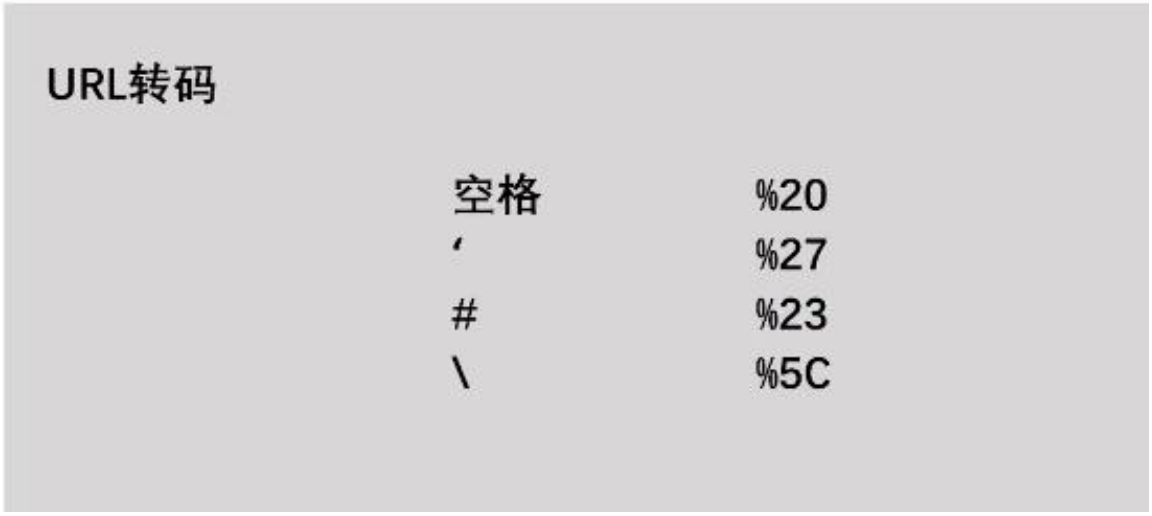
提到宽字节注入就要提到一些常见的编码方式，比如第一个 ASCII，我们看下这张表：

要点比如说它这个地方，它是从 0 到 127 的，那么其实就是阿斯克码表中，它会认为这种比如说字符调入 url 编码，一般来说它这种字母什么的，他可能就是你在传输过程中，你会发现它不是进行编码的。因为它这种小于 128 的，会认为这是一个单单个的一个字。但是我们知道如果我们在传输一个中文的时候，比如说你在网页网址中去输个中文，这个中文很多时候都会变成一个百分号开头的一串的一个字符串，其实就是相当于就要做一个转码的形式。

针对一个 GBK 的注入使用，GBK 是关于中文的一个编码，但这个 GBK 库其实是不全的。



我们先看一下对 url 转码的一个问题：



比如说我们去使用 hackbar，它是基于火狐浏览器的一个插件，你会发现里面除了空格之后，你再去发出请求，你再回过头去看 url，就是地址栏的时候，你会发现这个空格都会变成一个%20，它其实就是对这个东西做了一个 url 编码。（在

这里我做一个演示，如果大家想看可以到安全牛课堂的视频里看动手操作）

对某些符号的 url 编码其实要有要稍微要敏感一些，比如说空格在编程编之后就会变成一个%20，然后‘就更加要去重注意这个地方。为什么这样说？我们知道在注入的时候有一个很重要的一个问题，我们不去输入一个’，那么我们输入的内容是无法逃逸出对引号之间的，即使你这种时候去输再多的语句也是没有任何意义的。 所以说你对单引号要敏感一些。因为单引号中很重要，比如说像还有双引号这种，因为它有可能能够帮助你去逃逸，有的就是它把你限制死的框中，然后#2%#3%也很重要，因为什么？#就是我们常的一个注释符对吧？这里我们把%5C 拿出来，因为这里就要提到一个这个函数，这函数可以简单的看一下：

这个地方截图是来自于 php.net 官方手册上的一个截图。

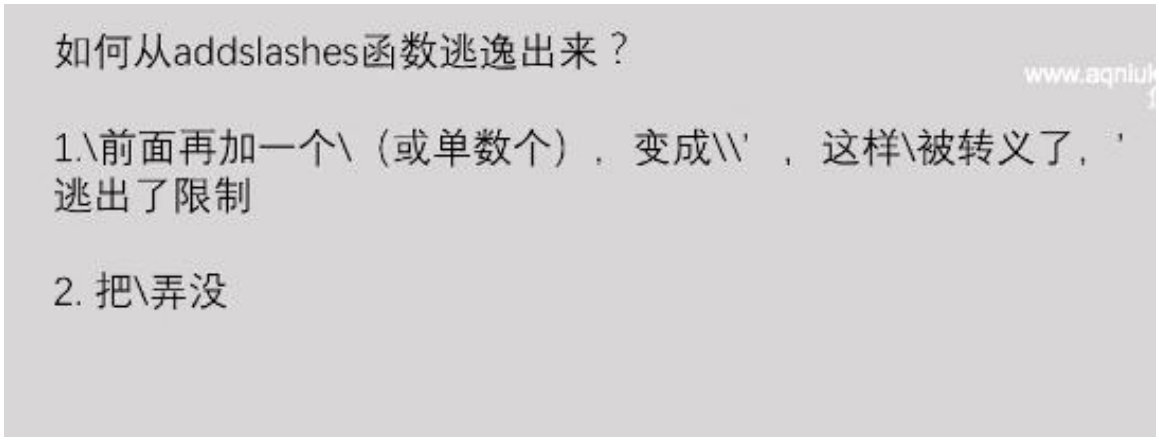
它这个地方其实像上面这个地方，它给的是一个当前函数知识的版本好。然后没有后面的话，如果讲到关于 php 的代码审计的一些问题的时候，就经常会去看这个手册，因为这些有些函数它其实它的问题是存在于某些版本之中的，或者说某某相

人术它在某些版本中是弃用的，所以像这种地方可以多去关注一下。

下面就给了一个简单说明，它的就是说它会返回一个字符串，你可以看到它该字符串就是为了数据库查询语句，等待需要某些字符串，字符前加上反斜线。

它提到的这些符号就是第一个是单引号双引号，然后反斜线，还有一个的单引号吗？你要知道加上反斜线的一个作用，加上反斜线之后，单引号就会变成加单引号全部加上一个反截线，那么反斜线其实起到的就是一个转移作用，单引号就是它就会变成它是个单引号，但是它只有长的是个单引号样，但是没有单引号在代码中的一个作用，那么这段以后就会失去它本身的一个作用，它只是看成你能看到它单引号，但是不能去实现一个注入的功能。

那么这个函数的话，其实你看它这么简单，但是其实很多这种 php 库中很多的使用的调用的第三方代码库，它其实都是基于这个函数做的二次开发封装之后的一个调用，就说它的本质还是使用了这个函数的。那么我们是接下来重点就是说如何从这个函数中去逃逸出来，我们因为他这个函数存在，我们就无法去插入一个单以后的双引号无法插入单引号，双引号的时候，我们就无法去实现语句的执行，因为我们数据都在引号之中.



它会把我们所有的东西都当成字符串去做一个查询的。

这里给两种思路:第一个的话，首先要么在前面\前面再去加一个\，那么\就把\给转移掉。那么单引号是不是就生效了。那么或者第二种思路就是单一，好想办法把它给弄没掉去，因为这样单引号不见了的话，那么不是单引号，就是反其先给弄没掉去，那么这样的话单引号就会生效了。所以就基于这两种树就要去做一个操作。这里提到了这宽字节，刚才是不是提到\其实是%5C。

之前一开始我就讲到说你比如说你输一个中文，你会在地址栏中发现它会变成一串%一个形式。那么但是我们其实知道%一串东西，它本意其实是一个汉字，那么 GBK 它用的就是这样一种形式，用\去和我们去数我们所有的东西，去重新构成一个汉字。（在这里我做一个演示，如果大家想看可以到安全牛课堂的视频里看动手操作）

它这地方是不是就给了一个单引号？然后’在前面去加个\，它其实就是%5C%27。因为这是 url 转码之后的。但是像下面这个地方，我就给出了一个%df%5C%27，那么它的转码之后是不是就经过那个函数过滤之后，是不是会在‘去加个反斜线，那么它其实就会变成三个字符。像 GB K 的问题，它就是把两个%开头的这种认为是一个汉字，而且我之前提到过，就对于阿斯科码 128 的一个，他就会认为他不是一个符号，他就会认为这两个拼接在一起才是一个，他就不会把它认为单一符号，而且级 PK 是两一个两个两两个自己认为一个是一个汉字，那么他就会把%5C 然后把%DF 和 800 分和 5C 去拼接在一起，作为一个汉字来识别。

那么这样的评级在一起之后，51%是不就不见了，51%它其实就是反切线，那这个时候分二期他就会逃逸出来，去达到一个逃逸的效果。我们可以看一下它的一个效果。

（在这里我做一个演示，如果大家想看可以到安全牛课堂的视频里看动手操作）

比如说像这个地方，它是一个网在线转码工具，我还是在这个地方去输一个，比如说中文你好，我对他做一个 url 解码，因为 GBK 的我要把它换成做个编码之后，你会看到%C4%E3 是两位的。那么按照我刚才的说法，是不是单引号会加\，他做个编码的形式的话，我要做的是在单引号去前面去加个%DF 我这时候再做个解码的时候，他会把这两个认为是一个汉字，做一个解码，你会看到这个时候，它把它认为一个汉字的时候，那么就是会变成这么一个字，这时候单引号就做出了一个逃逸。你要注意到这个时候，GBK 编码其实是由于数据库，它是使用 GBK 编码的，要不然的话，因为他查询的时候是把它其实会直接把%DF 和\’去直接插入到数据库里的，而不是说是因为前面的就在前端的一个执行，是因为它经过数据库的一个执行，然后或者说我们可以简单的去看一下。

（在这里我做一个演示，如果大家想看可以到安全牛课堂的视频里看动手操作）

比如说就说本地做的环境，这个环境其实是用之前很早的时候用的一个环境，它这个地方它的注入点是?如果说我在单引号它是没有效果，我去加个%df 的时候，它其实就会报错。

它实际去抄到数据库中去执行那个东西，这是非常老的一个工具，但是挺好用的。我在去执行一下，我对它做一个可能性。因为看到这个时候是不是\，\X 其实就是类似我们这个地方的一个%，就代表其实就是%df，因为其实这个 df 代表是 16 进制，X 代表其实就是 16 进制编码。然后 X 和 df 就会和反切像组成一个字去实现一个查询。这个其实就是对宽字节的一个基本原理。

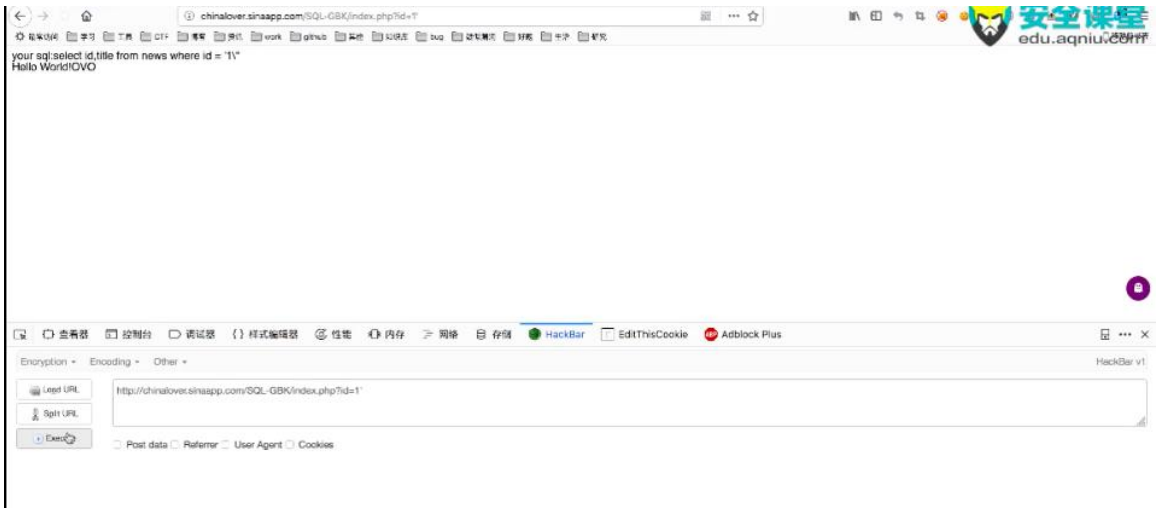
举例

（在这里我做一个演示，如果大家想看可以到安全牛课堂的视频里看动手操作，第一节 28 分 10 秒处）

那么这里的话我就拿了一个简单的一个例题来看一下。这个题目其实应该是南邮训练平台的一道题目。那么我们可以整个过程来看一下，到底是怎么来做这种题目，因为这种的话只是为了简单，先让我们回顾一下 SQL 注入这些问题，后面会越来越深入了解讲讲。首先的话，其实你知道我们目的是要去杀插入的单引号，因为它这个地方给出了我们这个语句，可以说这个语句。

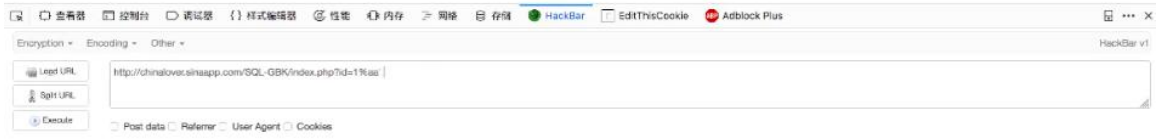
那么我先插入一个单引号，它是没有用的。反斜线就用刚才说的加了几个加上%df 去实现。然后其实刚才提到一个点，是不是不是针对%df 其实只要大于 128 其实就可以了，比如说 A 可以看一下到底行不行。你会发现 A 其实也是可以的，其实证明刚才说的是没有问题的。那么这样子可以之后，那么就要去做进一步的注入。

其实动画之后你会发现，其实也没有说如果说是这么顺利的可以坐下来，比如说你接下来就是要首先去跟一个单引号的话，配合上之后要去做一个#。他后面东西今后你发现它都是不报错了，之前去判断一下，看一下对不对。这就是没有生效，他这样才是有用，所以这道题到就黑开发的一个使用，很多时候就要去做一个转码，要不然它其实是会有问题的。而且其实要拖到转板这个问题，就不同的版本还可其实作用又不一样，像我这边的浏览器是新版火狐，像我在这个里面是旧版火狐，又会有一些简单的一些差异。你会发现其实就是输出点，那么首先去查 data base，这是它的当前的一个数据库。



your sql:select id,title from news where id = '1猪''

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in **SQL-GBK/index.php** on line **10**



要了解的话可以去网上去看一下，因为它只是基于数据库 my circle 数据库本身的一些自带的一些库，它会记录下来那些其他的一些库的信息，所以通过去查这个库中库中的某些表的数据，就可以去拿到一些数据，那么放他的条件是推波。贴宝贝 CHCHE 那么等于按道理来说，这个时候其实应该是不是要去说一个库名，如果像你这样的话，可以去说，可以试试看。因为发现这个时候，它会在单以后去前面再去加一个反斜线。

这样的话其实这个地方就会就出现问题了，那么其实这个地方的引号其实是不能去使用的。那么这个地方的话，第一种方法你可以用他的全具备用去代替。DATABSC 在特别是去做一个大 T 你会看到这时候存在一种数据表示 CTF 对吧？除了 CTF 之外，它会不会其他表呢？可以试看。Q 友看那就是 ct FCDFCP3CPACF 这么多的表，其实我也不知道他是哪张表，是答案所在，其实也无所谓，主要是为了掩饰整个的一个注入过程。

那么这样的话其实就说明我们能够拿到你们的数据表，那么接下来他就是我就假设，比如说要 CTF 这张表，我只是随便举例子，不一定把它做完，就是讲解这么一个方法。