matlab 中ctf,CTF中常见的web

转载

weixin_39806288 于 2021-03-21 12:28:34 发布 143 收藏
文章标签： matlab 中ctf

一、SQL注入

0x01宽字节注入

copy一份解释过来：mysql在使用GBK编码的时候，会认为两个字符为一个汉字，例如%aa%5c就是一个汉字(前一个ascii码大于128才能到汉字的范围)。我们在过滤 ' 的时候，往往利用的思路是将 ' 转换为 \'

因此我们在此想办法将 ' 前面添加的 \ 除掉，一般有两种思路：

%df吃掉 \ 具体的原因是urlencode('\') =

%5c%27，我们在%5c%27前面添加%df，形成%df%5c%27，而上面提到的mysql在GBK编码方式的时候会将两个字节当做一个汉字，此事%df%5c就是一个汉字，%27则作为一个单独的符号在外面，同时也就达到了我们的目的。

将 \' 中的 \ 过滤掉，例如可以构造 %**%5c%5c%27的情况，后面的%5c会被前面的%5c给注释掉。这也是bypass的一种方法。

GB2312、GBK、GB18030、BIG5、Shift_JIS等这些都是常说的宽字节

详细解释http://www.91ri.org/8611.html

有了原理了就来个栗子

题目：http://103.238.227.13:10083/index.php?id=1

直来直去，不用一步一步猜测字段了，源码里看到gb2312，提示了让我们宽字节注入

果然有效果

order by 一下2正常3错误，那就是2了

爆出数据库吧～

好了，文章写完了

指定是sql5.key,老是出错。。。。。

0x02题目来自2017全国大学生安全竞赛

这题考察的 是被转义后的单引号不会参与闭合，

此时看到用户名中的单引号被替换成了\，那么就把本来用于括起来name的单引号变成了\'这个样子，而转义过的单引号不会参与闭合，就出现了错误的判断，在or 1=1时发现空格被删除了，那么可以/**/代替绕过了，此时查询的语句为username='or 1=1 #\'or nickname='or 1=1#\'此时第一个单引号和第三个单引号闭合构造出了永真的语句

此时看到了good job

二、文件包含

0x01

题目http://120.24.86.145:8003/

源码

var_dump打印出数据类型以及数据值，show_source以高亮打印出源码，参考
http://blog.csdn.net/l3oog1e/article/details/72758429

写的writeup。打印出flag.php

0x02

题目http://120.24.86.145:8004/index1.php

//包含文件flag1.php，如果args不为空，将参数值赋值给$args，如果args值不为数字或字符输出args error,然后这里不管是否错误都不会影响到eval的语句执行，可以看到var_dump的括号里将$args又变成了一个变量，所以如果我们传入的字符串是某个变量的名字那么变量的值就会被打印出来，此时用全局变量$GLOBALS的话，由于已经包含了flag1.php，所以flag1.php的内容也会被打印出来