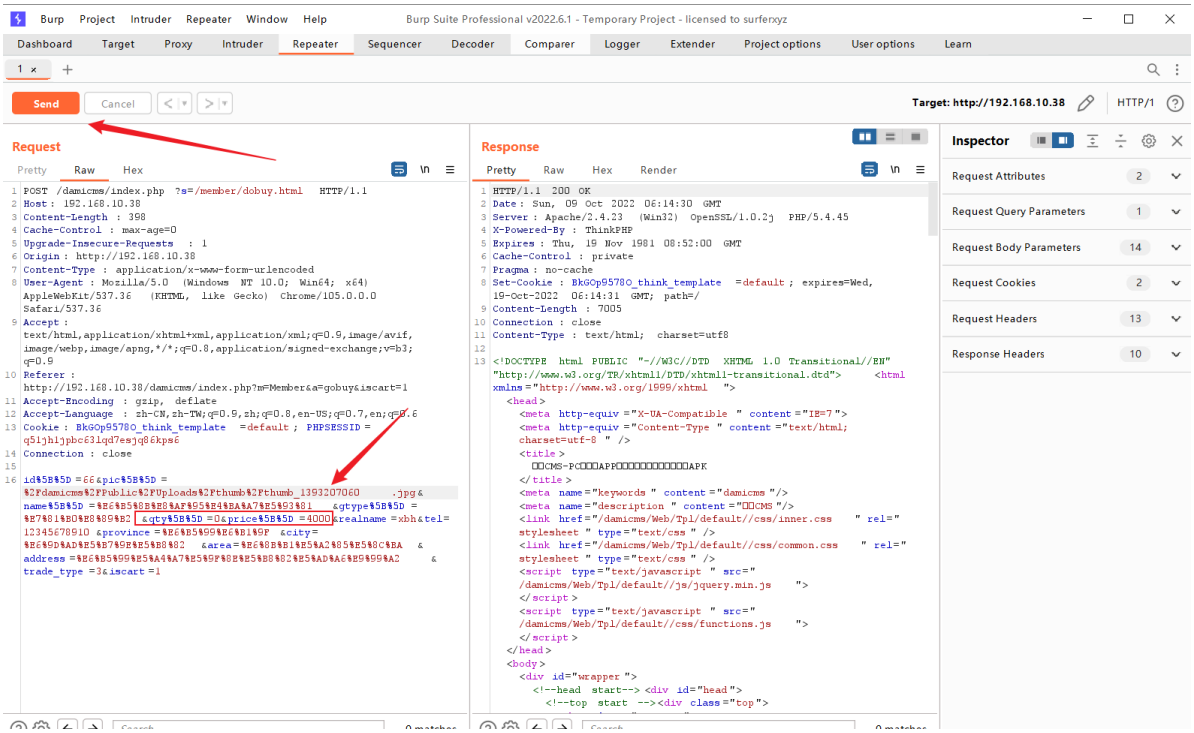
1.完成大米cms靶场的支付漏洞实验

在windows10虚拟机中将靶场安装并创建账户

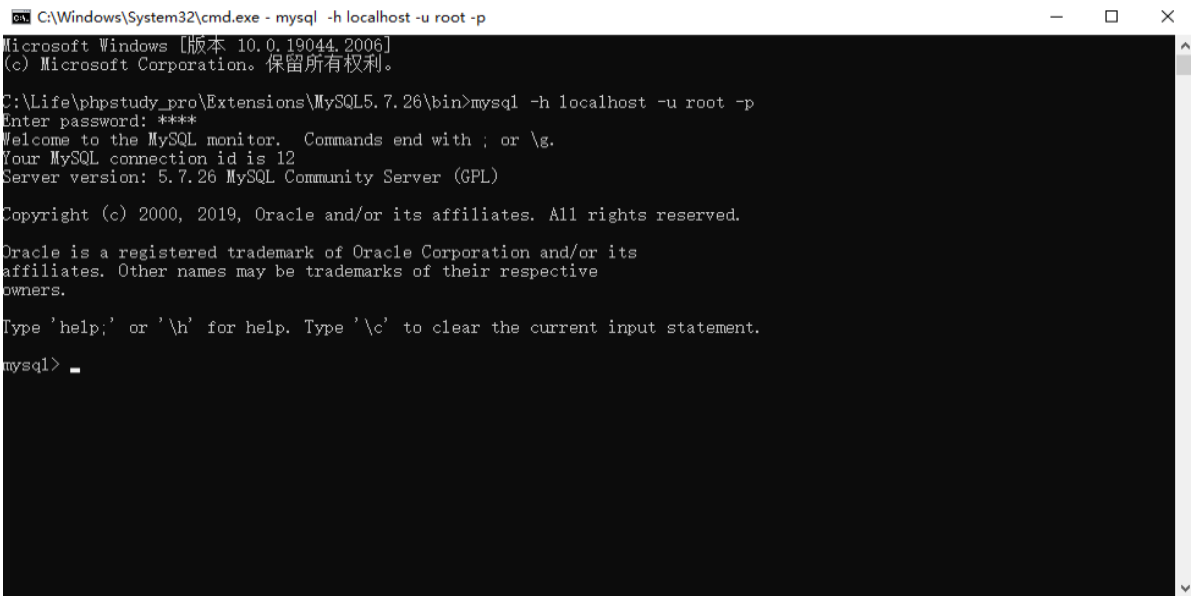
添加商品到购物车并选择站内付款后提交

使用burp抓包并修改参数后重发



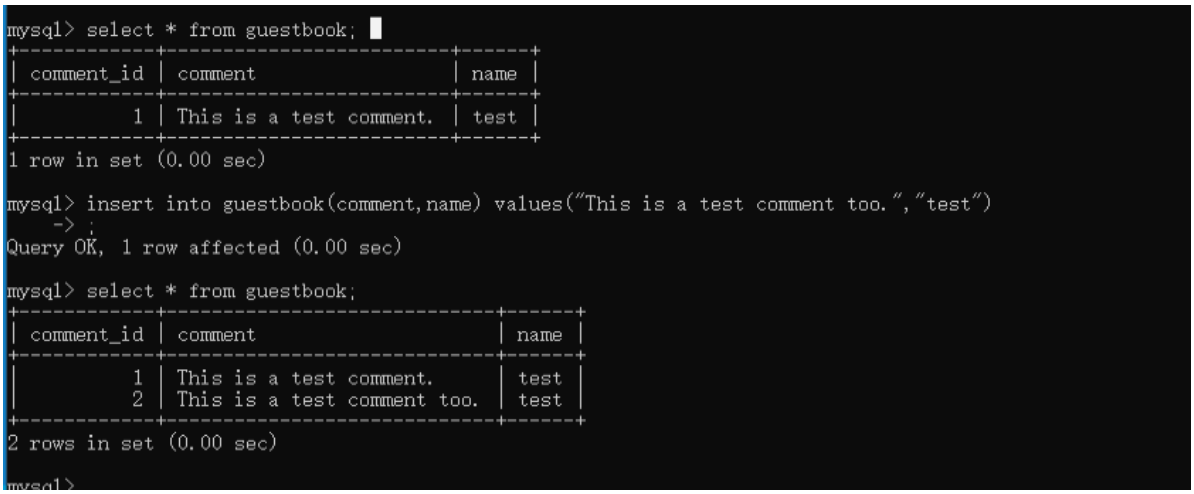
可以看到商品已购买成功

2.利用Mysql命令行工具连接mysql

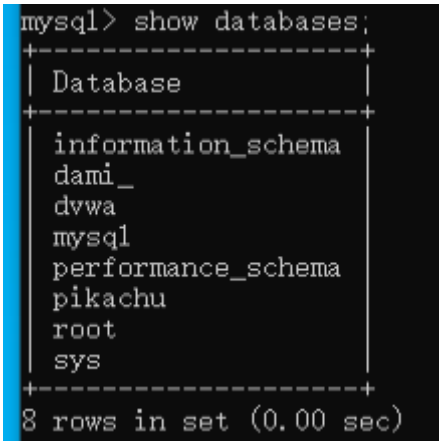


3.利用Mysql命令行工具完成下列的sql语句

（1）在dvwa数据库的guestbook表中插入一条数据



（2）查询mysql数据库中所有数据库名字（提示：information_schema)



```
mysql> select schema_name from schemata;
+--------------------+
| schema_name        |
+--------------------+
| information_schema |
| dami_              |
| dvwa               |
| mysql              |
| performance_schema |
| pikachu            |
| root               |
| sys                |
+--------------------+
8 rows in set (0.00 sec)

mysql>
```

(3) 查询dami_库中所有表的名字

```
mysql> use dami_
Database changed
mysql> show tables;
+---------------------+
| Tables_in_dami_     |
+---------------------+
| dami_access         |
| dami_ad             |
| dami_admin          |
| dami_admin_lock     |
| dami_article        |
| dami_card           |
| dami_config         |
| dami_extend_fieldes |
| dami_extend_menu    |
| dami_extend_show    |
| dami_favorites      |
| dami_find_password  |
| dami_flash          |
| dami_guestbook      |
| dami_key            |
| dami_label          |
| dami_link           |
| dami_log            |
| dami_member         |
| dami_member_group   |
| dami_member_menu    |
| dami_member_trade   |
| dami_money_log      |
| dami_mood           |
| dami_node           |
| dami_p1             |
| dami_role           |
| dami_role_admin     |
| dami_tag            |
| dami_tixian         |
| dami_trade_log      |
| dami_type           |
| dami_vip_mess       |
| dami_vote           |
| dami_wx_menu        |
| dami_wx_prize       |
| dami_wx_prize_user  |
+---------------------+
37 rows in set (0.00 sec)
```

```
mysql> select table_name from tables where table_schema = "dami_"
    -> ;
+----------------------+
| table_name           |
+----------------------+
| dami_access          |
| dami_ad              |
| dami_admin           |
| dami_admin_lock      |
| dami_article         |
| dami_card            |
| dami_config          |
| dami_extend_fieldes  |
| dami_extend_menu     |
| dami_extend_show     |
| dami_favorites       |
| dami_find_password   |
| dami_flash           |
| dami_guestbook       |
| dami_key             |
| dami_label           |
| dami_link            |
| dami_log             |
| dami_member          |
| dami_member_group    |
| dami_member_menu     |
| dami_member_trade    |
| dami_money_log       |
| dami_mood            |
| dami_node            |
| dami_p1              |
| dami_role            |
| dami_role_admin      |
| dami_tag             |
| dami_tixian          |
| dami_trade_log       |
| dami_type            |
| dami_vip_mess        |
| dami_vote            |
| dami_wx_menu         |
| dami_wx_prize        |
| dami_wx_prize_user   |
+----------------------+
37 rows in set (0.00 sec)

mysql>
```

(4) 查询dami_库中dami_ad表中所有列的名字

```
mysql> show columns from dami_ad;
+-------------+-----------------------+------+-----+---------+----------------+
| Field       | Type                  | Null | Key | Default | Extra          |
+-------------+-----------------------+------+-----+---------+----------------+
| id          | mediumint(8) unsigned | NO   | PRI | NULL    | auto_increment |
| title       | varchar(80)           | YES  |     | NULL    |                |
| content     | text                  | YES  |     | NULL    |                |
| description | text                  | YES  |     | NULL    |                |
| addtime     | varchar(32)           | YES  |     | NULL    |                |
| status      | tinyint(1) unsigned   | NO   |     | 0       |                |
| type        | tinyint(1) unsigned   | NO   |     | 0       |                |
+-------------+-----------------------+------+-----+---------+----------------+
7 rows in set (0.01 sec)

mysql>
```

```
mysql> select column_name from columns where table_name = "dami_ad" and table_schema = "dami_";
+-------------+
| column_name |
+-------------+
| id          |
| title       |
| content     |
| description |
| addtime     |
| status      |
| type        |
+-------------+
7 rows in set (0.00 sec)

mysql>
```