

## 业务逻辑漏洞

### 1.漏洞描述：

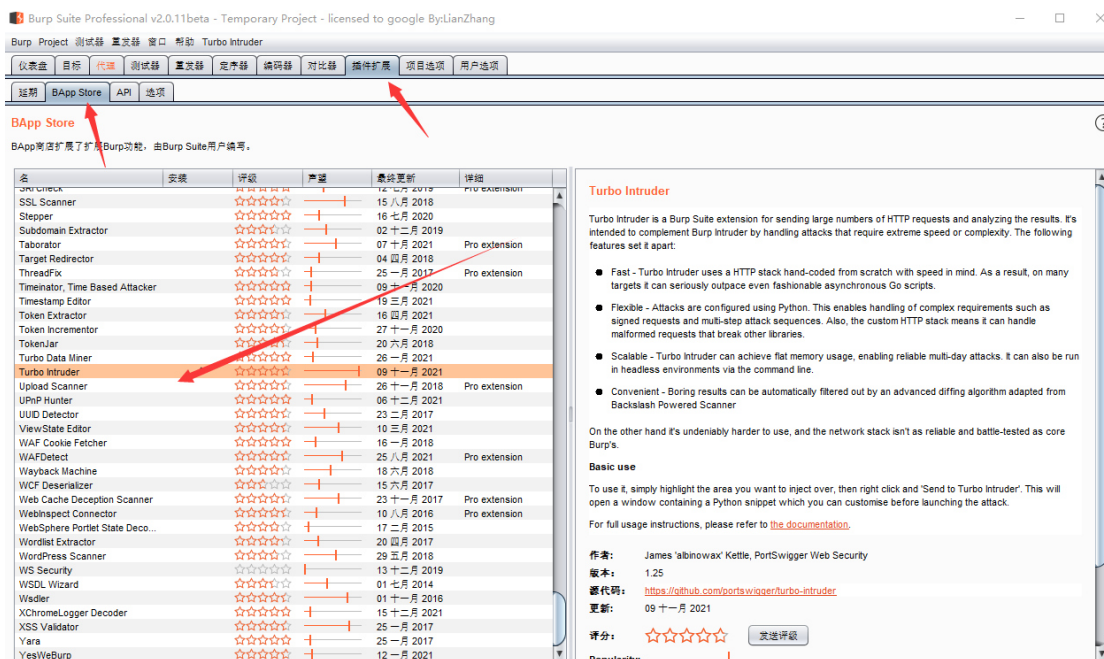
代金券逻辑介绍:代金券可进行拆分使用。第一次购买服务价格为 10 元，使用上该代金券那么该订单支付时就会为 0 元，那么 50 元的代金券-10 元就剩下 40 元，该逻辑存在一个漏洞点 出在拆分支付时。

我们先使用该 50 元的代金券进行 3 次 10.80 元的订单支付，此时代金券剩下 17.6 元

我们在创建第四次 10.80 订单时我们可以使用 Turbo intruder 进行一次并发，并发完成卷会看见两个 0 元订单

### 2.漏洞测试工具：

Turbo intruder 工具是 burp 自带的插件，可以用于对密码的爆破，验证码的爆破和并发漏洞测试。



测试方法:使用 Turbo intruder 模块对其抓包进行测试:

### 3.案例：

某云代金券逻辑漏洞：

某云送了两张对象存储服务的 50 元代金券

2. 购买 500g bos 资源需要 53.5 元

注释:该图中是使用了代金券的

订单信息						
订单: 1	产品名称: 对象存储	订单状态: ● 已支付 (已创建)				
订单类型: 购买	支付方式: 预付费	订单创建时间:	支付时间:			
产品名称	配置	数量	时长	单价	计费方式	产品金额
	地域: 华北-北京 标准存储包 500GB	1	1个月	53.80元/个		¥ 53.80
						订单金额: ¥ 53.80
						代金券总计: ¥ 50.00
						现金总计: ¥ 3.80

### 3.进行拆分购买

只需要进行拆分在 第四和第五订单时一起创建 即可实现 花 50 购买 53.8 的资源。最后一个订单是可以支付不小心被我点掉了没截到图

返回

创建

BOS(标准存储包)

数量: 1 时长: 1个月 单价: 53.80元/个

付费方式: 预付费

资源包类型: 标准存储包

规格: 100GB

生效时间: 支付后立即开通

计费方式: 包年包月

代金券选择

+ 激活代金券

代金券管理

产品类型:

存储包: ¥ 28.40 对象存储 BOS (全局) (通用) 2022-11-18到期

Forward

Drop

Intercept is on

Action

Open Browser

Pretty

Raw

Actions

Select extension...

z

1

n

F

8

h

c

g

2

h

%

h

B

H

H

D

4 C

5 C

6 S

7 U

A

8 C

9 E

10 X

11 X

12 S

13 A

14 O

15 S

16 S

17 S

18 R

19 Accept-encoding: gzip, deflate

20 Accept-Language: zh-CN,zh;q=0.9

21 Connection: close

22

23 {"sk": "80S","orderItemPrice":10.8,"totalPrice":10.8,

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

如下图红色标志 成功使用 50 元代金券 购买了 53.80 元的服务

09b7	对象存储	● 已取消	¥ 10.80	购买
11c87	对象存储	● 已支付	¥ 10.80	购买
1ef179	对象存储	● 已支付	¥ 10.80	购买
1601b	对象存储	● 已作废	¥ 10.80	购买
25af9	对象存储	● 已支付	¥ 10.80	购买
1cacc	对象存储	● 已支付	¥ 10.80	购买