

案例介绍

某金融项目的一个爆破支付密码的进而进行修改支付密码案例

案例

该用户中心的修改密码功能，该功能会先去验证当前交易密码输入得是否正确，如果正确就进行修改密码的操作，不正常则返回密码错误，而且该处并没有进行限制修改次数

修改交易密码

当前交易密码:

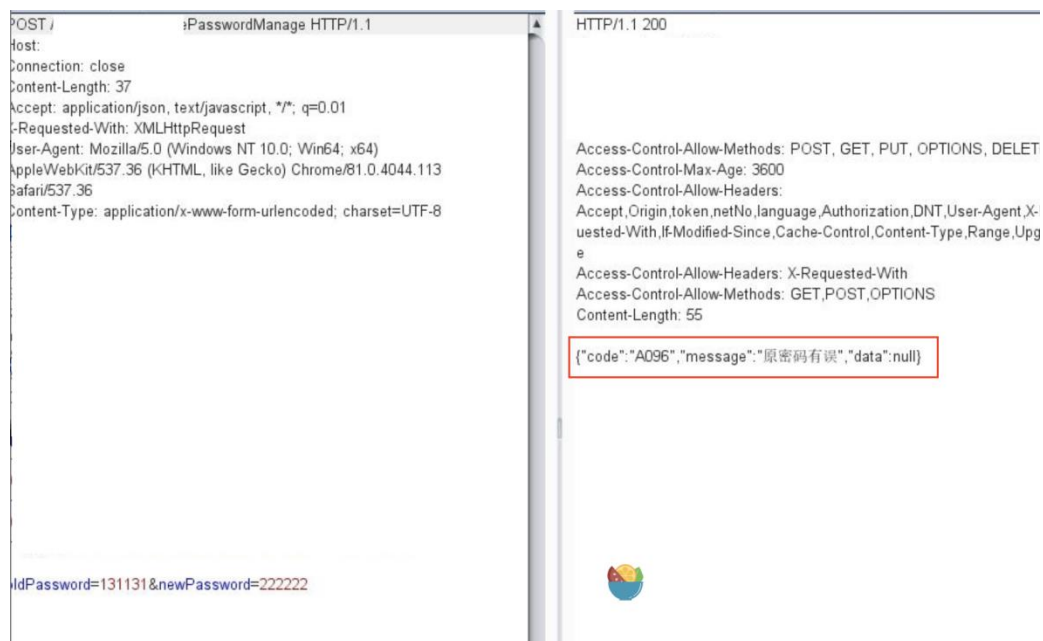
重设交易密码:

确认交易密码:

确定

返回

查看一下错误的返回包



使用 burp 进行爆破

有效载荷列表

ID	有效载荷	状态	错误	延时	长度	评论
201	000200	200			614	
0		200			617	
1	000000	200			617	
2	000001	200			617	
3	000002	200			617	
4	000003	200			617	
5	000004	200			617	
6	000005	200			617	
7	000006	200			617	
8	000007	200			617	
9	000008	200			617	

有效载荷选项

您可以定义一个或多个有效载荷。有效载荷的数量取决于“位置”选项卡中定义的攻击类型。每个有效载荷可以使用各种有效载荷类型，并且可以以各种方式定制每种有效载荷类型。

有效载荷类型: **数字** 有效载荷数量: 1,000,000
 有效载荷类型: **数字** 请求数量: 1,000,000

有效载荷选项(数字)

生成指定范围内指定格式的数字有效内容。

数字范围

类型: ☒ 范围 ☐ 随机

From: 000000
 To: 999999
 增量: 1
 编号:

数字格式

基地: ☒ Decimal ☐ Hex

整数部分的最小位数: 5
 整数部分的最大位数: 5
 小数部分最小位数:
 小数最大数字:

例

000001.1
 987654321.1234568

HTTP/1.1 200

Content-Length: 52

["code":"0000","message":"操作成功","data":null]

该类型漏洞 收录可能会有一些比如需要爆破次数需要达到 2w 类似的要求