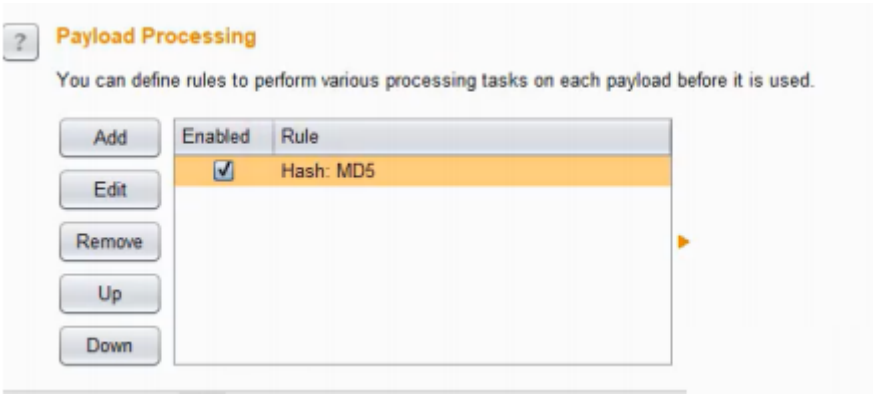
Day34　WEB漏洞–逻辑越权之登录脆弱及支付篡改

34.1暴力破解及本地加密传输

```
1　　登录应用功能安全问题，HTTP和HTTPS协议抓取登录数据包，通常HTTP协议密码未经过加密就能显示，而HTTPS协议数据包中的登录密码加密显示，对于未加密的数据，直接使用burp抓包，尝试使用字典暴力破解密码，对于加密传输的数据，确定其加密方式，进而对其及进行爆破，MD5加密结果一般都是32位对密码进行加密之后爆破。
```



34.2 Cookie脆弱性

代码审计，比如有的只需要验证cookie有值进行，抓包，给cookie赋一个值，便可成功绕过cookie验证

34.3 数据篡改安全问题

https://www.secpulse.com/archives/67080.html

```
#商品购买流程：
选择商品和数量-选择支付及配送方式-生成订单编号-订单支付选择-完成支付
#常见篡改参数：
商品编号 ID，购买价格，购买数量，支付方式，订单号，支付状态等
#常见修改方法：
替换支付，重复支付，最小额支付，负数支付，溢出支付，优惠券支付等
```

资源：

```
https://www.zblogcn.com/zblogphp/
https://github.com/huyuanzhi2/password_brute_dictionary
https://pan.baidu.com/s/1fJaW23UdcXcSFigXO-Duwg 提取码：xiao
https://pan.baidu.com/s/1fJaW23UdcXcSFigXO-Duwg 提取码：xiao
```