01-开班第一课

目录

**[一、](#_Toc138683320)****[作业内容](#_Toc138683320)** [3](#_Toc138683320)

[1. xxxx 3](#_Toc138683321)

[2. xxxxx 3](#_Toc138683322)

[3. …… 3](#_Toc138683323)

**[二、](#_Toc138683324)****[操作步骤](#_Toc138683324)** [4](#_Toc138683324)

[1. xxxxx 4](#_Toc138683325)

[2. xxxxx 4](#_Toc138683326)

[3. …… 4](#_Toc138683327)

**[三、](#_Toc138683328)****[作业总结](#_Toc138683328)** [5](#_Toc138683328)

[1. xxxxx 5](#_Toc138683329)

[2. xxxxx 5](#_Toc138683330)

[3. …… 5](#_Toc138683331)

1. **作业内容**

作业布置

一、开启大米CMS实验

二、使用BP抓包，0元购买东西

如果实验打不开使用如下备用网站

<http://166c3ec23c8etarget.yijinglab.com:80>

<http://36b7b010af76.target.yijinglab.com:80>

http://297385459b85.target.yijinglab.com:80

1. **操作步骤**
2. 打开burp suite



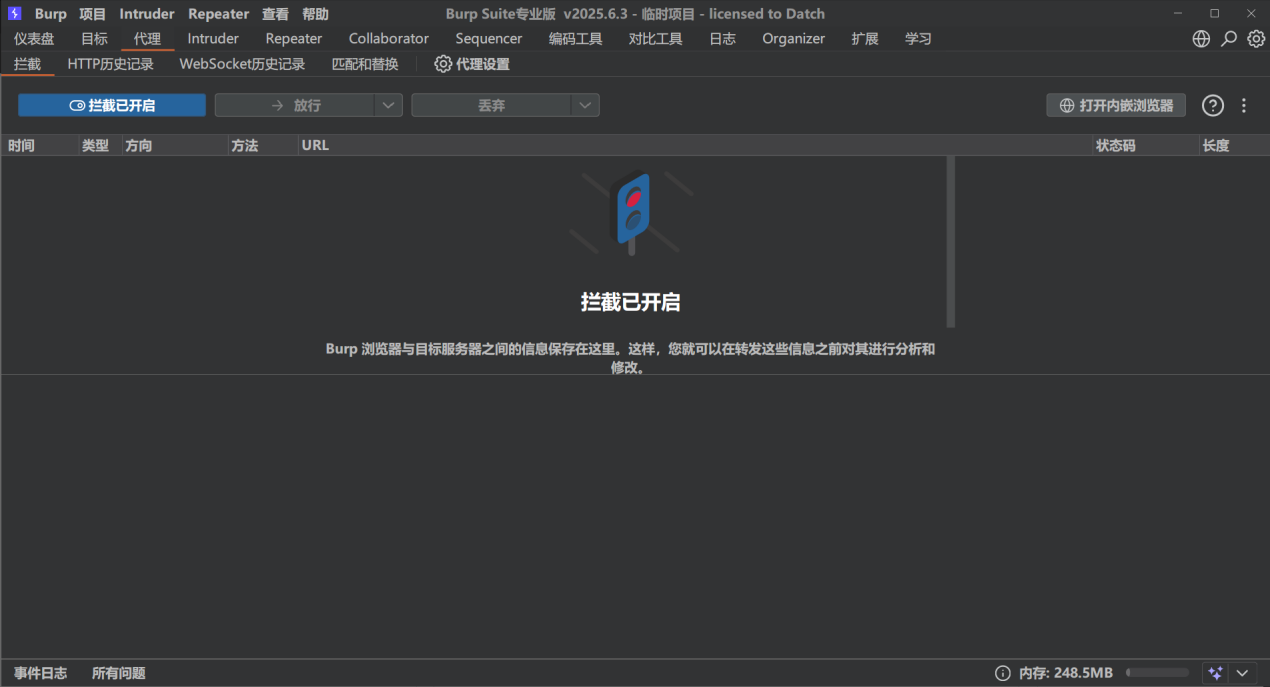
1. 打开内嵌浏览器



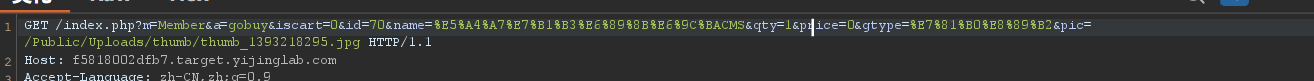
1. 选中商品



1. 打开拦截



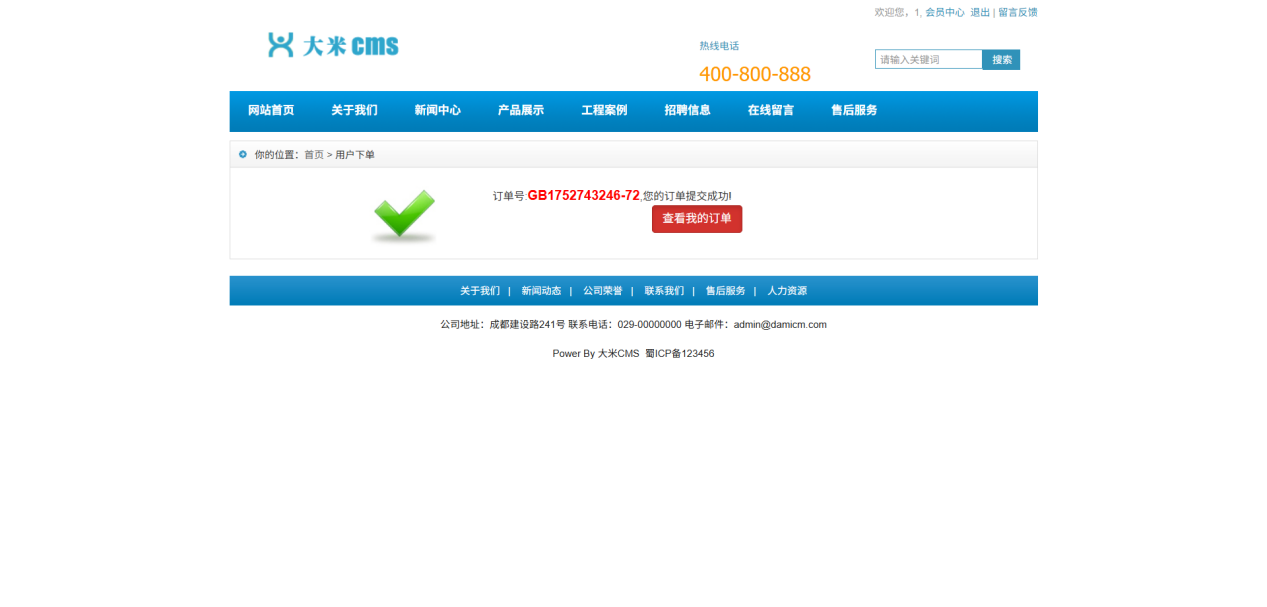
1. 对数据包进行修改，将商品价格改为0



1. 点击放行后打开拦截

  
7.查看商品价格，填写信息后点击支付

  
8.支付成功！



1. **作业总结**

本次实验的核心是利用Web代理工具Burp Suite，通过拦截和修改HTTP请求数据，对大米CMS（DaMi CMS）存在的支付逻辑漏洞进行利用，最终成功实现了“0元购”的目标。通过亲手操作，我对于Web应用安全中的数据校验漏洞有了更深刻和直观的认识。

1. 漏洞原理的理解与实践

本次实验所利用的漏洞，其根本原因在于Web应用程序在处理交易时过分信任了来自客户端（浏览器）提交的数据。大米CMS的后端服务器在生成订单时，没有对前端提交的商品价格（price）或数量（qty）等关键参数进行严格的二次校验。这就给了我们一个可乘之机：通过在数据包到达服务器之前，使用Burp Suite将其拦截并进行修改，从而欺骗服务器，让它以我们修改后的（例如0元）价格来创建订单。这个过程让我深刻理解到，任何涉及金钱交易的环节，其核心数据都必须以服务端为准，绝不能依赖前端传递的值。

2. Burp Suite工具的应用与掌握

通过本次实验，我进一步熟悉了Burp Suite这款强大的网络安全测试工具的核心功能。从设置浏览器代理，到开启和关闭拦截（Intercept），再到识别并修改关键的请求参数，整个流程走下来，让我对“中间人攻击”的概念有了具象化的理解。特别是观察和分析HTTP请求的报文结构，让我学会了如何从众多参数中快速定位到影响订单金额的关键字段（如price或qty），并成功地进行了修改。这不仅是完成本次作业的关键，也为今后进行更复杂的Web安全测试打下了坚实的基础。

3. 对Web安全的思考与启示

这次看似简单的“0元购”实验，实则揭示了Web应用开发中一个常见却极其危险的安全短板——服务端校验缺失。它警示我们，在开发任何Web应用，特别是电商、金融等涉及交易的系统时，必须遵循“永不信任用户输入”的基本安全原则。所有关键的业务逻辑和数据校验（如商品价格、库存、用户权限等）都必须在服务器端强制执行，以防止客户端的恶意篡改。同时，这也让我认识到，定期的安全审计和漏洞扫描对于维护系统安全至关重要，能够帮助我们及时发现并修复类似的安全隐患。