基于 PHP 的电商场景漏洞实训平台设计与实现

任方针
阜阳职业技术学院信息与智能制造学院，安徽 阜阳 236000

DOI: 10.61369/TACS.2026060033

摘　　要： 针对网络安全攻防基础等课程中传统漏洞靶场业务场景割裂、实验入口分散、学生难以理解漏洞业务危害等问题，设计并实现了一套基于 PHP 的电商场景漏洞实训平台。平台基于 PHPStudy、PHP 和 MySQL 构建运行环境，采用 B/S 架构和 PHP MVC 设计思路组织业务逻辑，前端围绕商品浏览、购物车、订单处理、扫码支付等电商流程展开交互。系统将暴力破解、SQL 注入等 Web 安全问题嵌入真实业务入口，并通过学生实训手册提供教学支持。测试结果表明，该平台能够完成基础电商业务流程和漏洞复现实训，可为网络安全攻防基础等课程提供贴近真实项目的实践教学环境。

关 键 词： 渗透测试；Web 安全；漏洞靶场；电商平台；实训教学

Design and Implementation of E-commerce Scenario Vulnerability Training Platform Based on PHP

Ren Fangzhen
School of Information and Intelligent Manufacturing, Fuyang Vocational and Technical College, Fuyang, Anhui 236000

Abstract: Aiming at the problems in courses such as "Fundamentals of Network Security Offense and Defense", such as fragmented business scenarios of traditional vulnerability shooting ranges, scattered experimental entrances, and students' difficulty in understanding the business hazards of vulnerabilities, a set of PHP-based e-commerce scenario vulnerability training platform is designed and implemented. The platform builds a running environment based on PHPStudy, PHP and MySQL, adopts B/S architecture and PHP MVC design idea to organize business logic, and the front-end carries out interactions around e-commerce processes such as commodity browsing, shopping cart, order processing, and QR code payment. The system embeds Web security issues such as brute force cracking and SQL injection into real business entrances, and provides teaching support through student training manuals. Test results show that the platform can complete basic e-commerce business processes and vulnerability reproduction training, and can provide a practical teaching environment close to real projects for courses such as "Fundamentals of Network Security Offense and Defense".

Keywords: penetration testing; web security; vulnerability shooting range; e-commerce platform; practical teaching

引言

网络安全攻防类课程实操性强，要求学生掌握漏洞原理，完成信息摸排、漏洞检测、风险研判与修复处置全流程。传统教学偏重单点漏洞讲解演示，脱离实际业务场景，学生易割裂看待安全问题，无法研判漏洞对业务数据、流程的危害，也难以找准修复方向。

电商平台业务体系完整，涵盖各类典型安全风控要点。将漏洞实训融入电商业务链路，可提升实训真实度。据此本文搭建电商主线 Web 漏洞实训平台，整合常见漏洞教学场景，区分师生使用权限，依托固定数据环境，保障实验可重复开展。

一、系统开发技术

（一）PHPStudy

PHPStudy 集成 Apache、PHP 和 MySQL 等基础组件，适合在机房、教师电脑或学生本地环境中快速部署 Web 实验项目。对于网络安全攻防基础等课程而言，实验环境的可复现性直接影响课堂组织效率。通过 PHPStudy 部署平台，教师可将项目目录放置于本地 Web 根目录或指定站点目录，并通过导入初始场景 SQL

项目信息：
网络安全攻防基础（校级质量工程—精品课程）（2025JPKC08）；
网络安全攻防基础（校级质量工程—优质教材）（2025YZJC02）；
“邻距离·共成长”社区辅导员育人工作室（2025FDYGZS03）。
作者简介：任方针（1996.02—），男，安徽阜南人，助教，硕士，主要研究方向为网络安全。

文件快速恢复实验数据，从而降低课程实训的环境依赖。

（二）PHP MVC

平台后端采用原生 PHP MVC 结构组织业务逻辑，入口文件统一接收请求，路由层负责解析 URL 并分发到对应控制器；控制器层负责处理业务请求、登录状态和页面跳转；模型层负责数据库访问；视图层负责页面渲染。该结构划分了请求分发、业务处理、数据访问和页面展示的职责，便于后续维护和扩展漏洞实验。

（三）MySQL

MySQL 是常用的关系型数据库管理系统，能够满足中小型 Web 应用对数据存储、查询和维护的基本需求 [1]。在本平台中，MySQL 主要存储用户、商品、订单等数据，通过预置固定账号和样例订单，平台可为不同课堂提供一致的数据基础，保证漏洞复现结果具有稳定性。

（四）前端页面技术

平台前端采用 HTML、CSS、JavaScript 和 Bootstrap 等通用 Web 技术完成页面布局与交互 [2]。商品列表、订单、扫码支付等页面以电商业务流程为核心，使学生在正常操作过程中接触参数传递、状态变更和权限边界等安全分析对象。

二、系统分析及设计

（一）可行性分析

1. 技术可行性

平台所采用的 PHP、MySQL 和 Bootstrap 等技术成熟度较高，开发与部署门槛相对较低，能够满足课程实训平台对基础电商业务和漏洞演示功能的需求。平台采用 MVC 结构和配置场景实训清单，有利于分离业务逻辑、数据访问和页面展示，也便于后续增加新的漏洞实验。

2. 操作可行性

平台操作面向学生和教师两类用户。学生通过电商业务入口完成漏洞复现实训，不需要直接面对孤立的代码片段；教师通过教师账号查看漏洞原理、关键代码位置和修复建议，可在课堂中快速完成演示、讲解和检查。因此，从课堂使用和教学组织角度来看，该平台具有较好的操作可行性。

3. 部署与复现可行性

平台以本地教学环境为主要目标，部署依赖较少，能够通过固定账号、固定商品、固定订单和数据库初始场景脚本恢复实验初始状态。教师在课前可按照验收清单快速检查平台状态，学生在课后也可重新导入数据进行自学练习，符合课程反复演示与分组训练的需要。

（二）功能需求分析

1. 学生功能需求

学生使用平台时，应能够完成商品浏览、商品搜索、和漏洞复现实训等操作。在实训中心中，学生需要查看每个漏洞的业务背景、操作步骤、判断方式和实验要求，并根据页面现象形成实验记录。

2. 教师功能需求

教师使用平台时，需要能够查看更完整的漏洞原理、关键代码位置、验证说明和修复建议。教师账号不仅用于课堂讲解，也用于检查学生是否完成正常业务基线、漏洞验证、危害分析和修复建议等环节，从而支撑过程场景教学评价。

3. 漏洞实训需求

漏洞实训需求围绕课程中的常见 Web 漏洞展开 [3][4]，将暴力破解、SQL 注入、XSS 等实训内容融入电商业务入口中，使学生能够从业务对象、请求参数、数据边界和服务端校验等角度理解漏洞成因与危害。主要漏洞实训场景如表1所示。

表1 漏洞实训场景设计

漏洞类型	业务入口	教学目标	验证现象
暴力破解	用户登录	理解弱口令、无锁定、无验证带来的认证风险	多次失败后仍可继续尝试并登录弱口令账号
SQL 注入	商品详情、商品搜索、我的订单查询	理解输入拼接 SQL 导致的数据越权读取风险	可看到用户资料、隐藏商品或其他用户订单
XSS	商品评价	理解存储型 XSS 的输入、存储和输出链路	评价内容在商品详情页被浏览器解析执行
CSRF	个人资料修改	理解浏览器自动携带 Cookie 带来的伪造请求风险	不带合法 Token 的请求仍能修改资料
文件上传	头像上传	理解扩展名校验不足和上传目录可访问风险	SVG 头像上传后可直接通过 Web 路径访问
水平越权	订单发票预览	理解对象级授权缺失造成的数据泄露风险	修改订单 ID 后可查看他人订单发票信息
支付逻辑漏洞	扫码支付提交	理解客户端金额不可信带来的业务逻辑风险	修改客户端提交金额后订单仍显示支付成功
命令执行	电子面单预览	理解系统命令参数拼接带来的执行风险	模板参数异常后出现系统命令回显
信息泄露	框架诊断页	理解调试信息和框架指纹泄露风险	debug 参数显示框架、路径、路由和数据库摘要

（三）功能模块设计

根据网络安全攻防基础等课程实训目标和电商业务流程，平台功能可划分为电商业务模块、用户角色模块、漏洞实训模块和教学辅助模块四个部分，如图1所示。电商业务模块负责提供商品、订单、支付和个人中心等基础流程；用户角色模块用于区分学生和教师的信息展示权限 [5]；漏洞实训模块用于承载各类漏洞入口；教学辅助模块用于组织实训手册、教师提示、判断方式和修复建议。

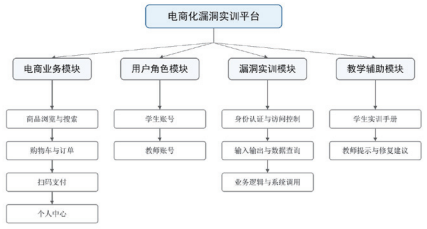

图1 系统功能框图

（四）系统架构设计

平台采用 B/S 架构，学生和教师通过浏览器访问系统。Web 服务端基于 PHPStudy 运行，统一入口和路由层负责接收并分发请求，控制器层处理业务逻辑，模型层访问 MySQL 数据库，视图层完成页面渲染。该架构能够清晰呈现系统各模块的职责边界，便于后期系统迭代与问题排查，系统架构如图2所示。

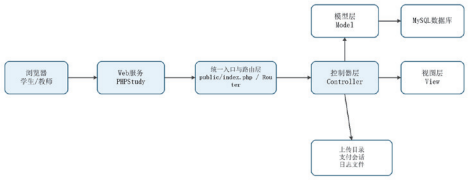

图2 系统架构图

（五）数据库设计

1. 数据库 E-R 图

数据库设计围绕电商业务数据、管理端数据和漏洞实训数据三条主线展开。业务数据主要包括用户、收货地址、购物车、商品分类、订单等实体；管理端数据包括管理员和管理员日志；实训数据主要通过固定账号、固定商品、固定订单和配置场景漏洞清单支撑课堂复现。数据库完整 E-R 关系按实体、联系和属性绘制，并保留主键、外键及核心业务字段，如图3所示。

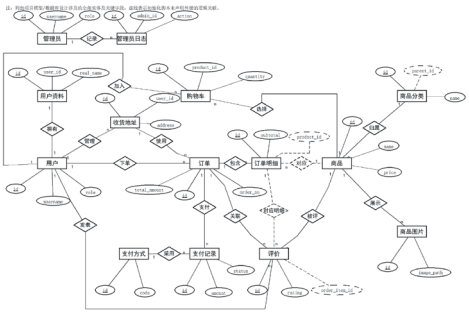

图3 数据库完整 E-R 图

2. 数据库与复现数据设计

用户表保存学生与教师账号及角色信息；用户资料表保存头像、手机号、个人简介等个人中心数据；商品表保存商品名称、价格、库存、图片和上下架状态；订单表保存订单号、所属用户、金额、订单状态和支付状态；支付表保存支付金额、支付方式、支付状态和支付时间；评价表保存用户对商品的评价内容。与普通电商系统不同，教学平台还在初始场景数据中预设隐藏商品、跨用户订单、待支付订单等样例数据，分别服务于商品搜索注入、订单查询越权和支付逻辑漏洞实验。

三、系统实现

（一）电商业务模块的实现

用户登录平台后，可依次完成商品浏览、商品搜索、订单提交、扫码支付等操作。平台以电商业务流程作为漏洞承载环境，使学生先形成正常业务基线，再对比异常请求或异常页面现象。该实现方式有助于学生理解漏洞并非孤立技术点，而是会直接影响商品、订单、支付和用户资料等业务数据。

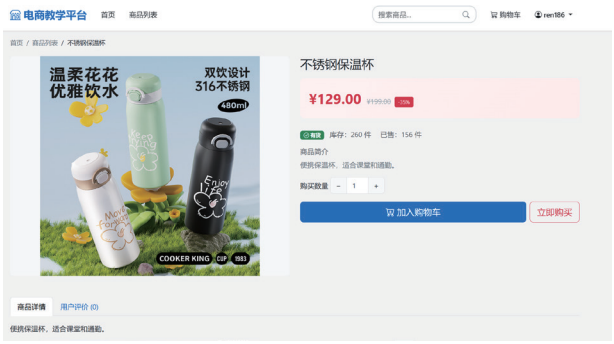

图4 电商业务模块

（二）漏洞实训模块的实现

平台设有九大漏洞实训模块，本文选取 SQL 注入与业务逻辑模块展开说明。SQL 注入模块依托商品浏览、搜索、订单查询三类入口，展示不同参数引发的注入风险，让学生认清漏洞除页面异常外，还会造成数据、订单信息泄露等业务危害。支付逻辑模块模拟完整扫码支付流程，以此印证不可轻信前端提交数据，金额校验需以服务端订单信息与支付回调结果为依据。

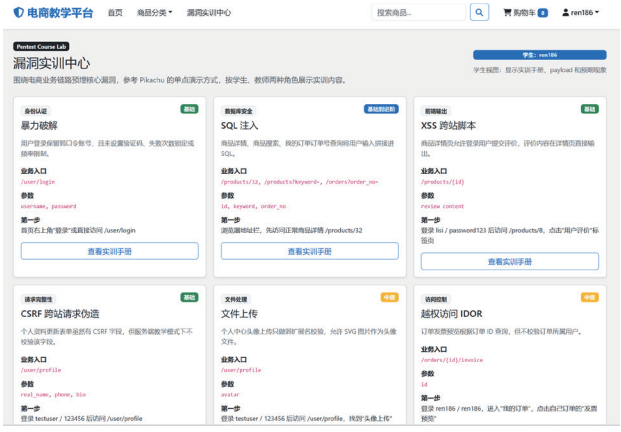

图4 漏洞实训模块

（三）教师提示与角色场景模块的实现

为了兼顾学生自主实训和教师课堂讲解，平台设计了角色场景。学生登录后可以查看每个漏洞的业务背景、实训入口、操作步骤等内容；教师登录后可以在此基础上查看更完整的漏洞原理、关键代码位置和修复建议，既避免学生界面直接呈现完整答案，又能为教师提供课堂讲解和安全编码对比依据。

图5 教师提示模块

（四）平台测试与复现验证

平台测试从基础功能、支付流程、角色展示、漏洞复现和运行环境五个方面展开，测试结果如表2所示。

表2 平台测试结果

测试类别	测试内容	测试结果
基础功能测试	首页、商品列表、商品详情、购物车、下单、订单、个人中心	页面可正常访问，核心业务流程完整
支付流程测试	二维码扫码、手机确认、电脑提交、支付结果页	支付状态流转正常，结果页可显示实付金额
角色展示测试	学生账号、教师账号分别访问实训中心	学生显示实训手册，教师显示教学提示和修复建议
漏洞复现测试	9类漏洞在对应业务入口验证	均能观察到明确教学现象
语法与环境测试	PHP 文件语法检查、PHPStudy+MySQL 环境运行	无语法错误，本地环境可稳定运行

测试结果表明，平台既能够完成普通电商网站的基础业务流程，又能够在指定业务入口稳定复现漏洞现象。学生可以按照实训手册完成操作并记录结果，教师可以通过教师账号查看修复建议和课堂判断标准。结合已有 Web 课程系统建设经验[6]，该平台能够满足网络安全攻防基础等课程中“教师演示、学生练习、现象记录、修复分析”的基本教学流程。

四、结论与展望

本文依据网安攻防课程实践需求，搭建基于 PHP 的电商漏洞实训平台。平台依托电商核心业务融入各类 Web 漏洞，搭配配套资料实现分层教学，帮助学生结合业务理解漏洞原理与防护手段。

平台已完成业务、角色、实训及教学辅助模块开发，囊括多种常见漏洞。固定数据环境简化实验部署复现流程，可稳定支撑实操教学。目前仅支持本地部署，后续将新增容器部署、自动评分、数据分析等功能，扩充漏洞场景，增强平台适用性与使用价值。

参考文献

[1] 马立和，高振娇，韩锋 . 数据库高效优场景：架构、规范与 SQL 技巧 [M]. 北京：机械工业出版社 ,2020.

[2] 沈蕴梅，童文俊，符钰 . ASP.NET 动态 Web 开发技术项目场景教程 [M]. 北京：清华大学出版社 ,2016.

[3]OWASP Foundation. OWASP Top 10:2021[EB/OL]. 2021. https://owasp.org/Top10/2021/.

[4]OWASP Foundation. OWASP Web Security Testing Guide v4.2[EB/OL]. 2020. https://owasp.org/www-project-web-security-testing-guide/v42/.

[5] 史会余，王余辉，肖杰 . 基于角色访问控制的通用权限管理系统设计与实现 [J]. 电脑编程技巧与维护 .

[6] 古发辉 . 基于 PHP 的电商服务平台设计与实现 [J]. 科技广场，2014(11):5.DOI:10.3969/j.issn.1671-4792.2014.11.010.

