php代码审计基础篇

第14课 黑白盒审计

php代码审计

黑盒

burp,seay审计工具

功能点分析

安装cms(重装问题)

用户注册(xss,sql)

管理个人信息(xss,越权)

用户前台的身份

多个用户(越权)每个用户的功能点　　个人资料，新闻发布，文章管理。

后台。 (发布文章，新建两个不同权限用户。文件上传)

文件删除，插件，日志备份。

php代码审计

白盒

定位到每一个功能的文件

sql注入看sql注入

传入的参数是否有防护

xss,看传入的xss语句

看用户是怎么进行判断身份的

文件上传，定位处理上传的文件代码

逻辑越权

定位到是怎么对用户的权限进行校验的

日志备份(定位是对数据库是怎么命名的)

文件删除(是怎么对文件删除进行操作的)

bluecms

多处xss,sql注入，重装

谢谢观赏