系统渗透测试实验指导书

一、实验目的

1. 了解 Web 页面中的常见漏洞及其利用方法
2. 学习 Web 页面中的常见漏洞的防范手段。

二、实验内容

1. 挖掘并分析 Web 页面中存在的漏洞

三、实验步骤

在浏览器中访问目标 web 服务器，点击 DVWA 链接并登录，账号/密码为 admin/password

登录后点击 Setup -> Create/Reset Database，如下图示，从 Brute Force、Command Execution、CSRF、File Inclusion、SQL Injection、SQL Injection(Blind)、Upload、XSS reflected、XSS stored 这 9 个实验中，***选择任一进行学习***。

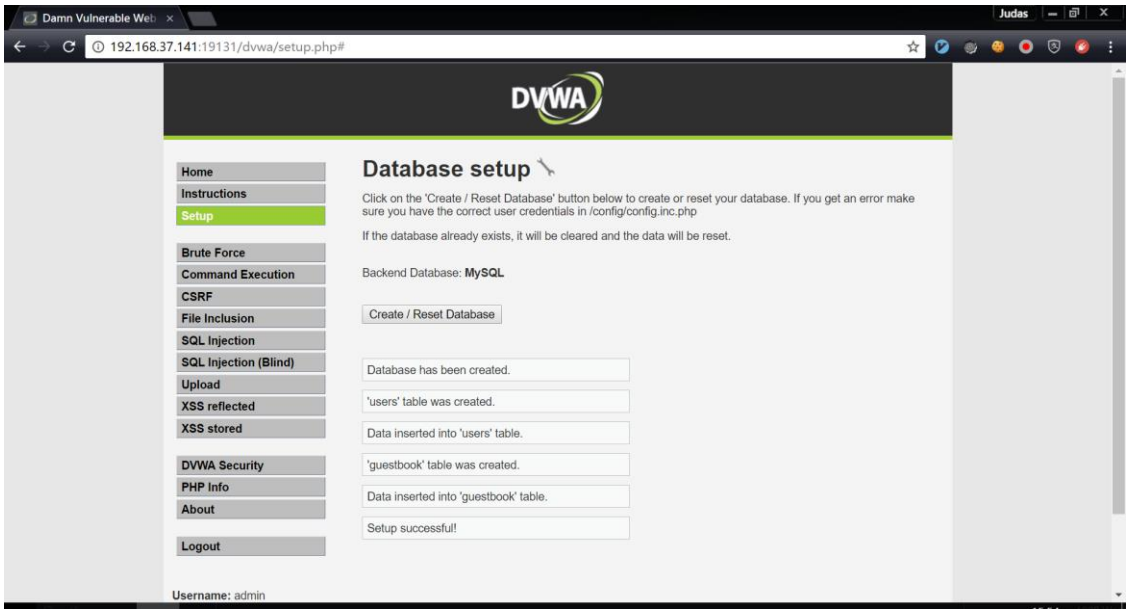

图 1 DVWA 实验页面

每个实验都分为 low、medium、high、impossible 四个难度。选择至少一个实验，分别完成 low、medium、high 难度即可。（源代码可以在此找到）

四、思考题

1. 请对 DVWA 中你选择的实验进行分析，并阐述如何防止该类漏洞出现（hint:可结合该实验的 impossible 代码分析）。

作业要求：

1) 个人作业，以 word 或 PDF 文档形式提交，具体格式见模板。

2) 作业文档命名：学号_姓名_Penetration.文件扩展名
3) 在 2019 年 3 月 27 日（周三）晚 22:00 前报告在线提交

课堂交流申请：

2019 年 3 月 16 日（周二）晚 22:00 前发 PPT 申请至邮箱：mengkui@sjtu.edu.cn