ＯＷＡＳＰ中国　云南分部　　嘲风信息

OWASP

The Open Web Application Security Project

演讲提纲

OWASP
The Open Web Application Security Project

1、owasp 介绍

2、owasp的主流工具

3、owasp top ten

OWASP

The Open Web Application Security Project

- OWASP是一个开源的、非盈利的全球性安全组织，致力于应用软件的安全研究。我们的使命是使应用软件更加安全，使企业和组织能够对应用安全风险作出更清晰的决策。目前OWASP全球拥有140个分会近四万名会员，共同推动了安全标准、安全测试工具、安全指导手册等应用安全技术的发展。
- OWASP中国目前的会员量是３７００人
- OWASP在业界影响力：
- OWASP被视为web应用安全领域的权威参考。2009年下列发布的美国国家和国际立法、标准、准则、委员会和行业实务守则参考引用了OWASP。美国联邦贸易委员会(FTC)强烈建议所有企业需遵循OWASP十大WEB弱点防护守则
- 国际信用卡数据安全技术PCI标准更将其列为必要组件
- 为美国国防信息系统局（DISA)应用安全和开发清单参考

OWASP
The Open Web Application Security Project

- 为欧洲网络与信息安全局（ENISA)，云计算风险评估参考
- 为美国联邦首席信息官（CIO)理事会，联邦部门和机构使用社会媒体的安全指南
- 为美国国家安全局/中央安全局， 可管理的网络计划提供参考
为英国GovCERTUK提供SQL注入参考
- 为欧洲网络与信息安全局（ENISA)，云计算风险评估提供参考
- OWASP TOP 10为IBM APPSCAN、HP WEBINSPECT等扫描器漏洞参考的主要标准

OWASP
The Open Web Application Security Project

- 主流工具介绍

- Webgoat（替罪羊）

WebGoat是OWASP组织研制出的用于进行web漏洞实验的应用平台，用来说明web应用中存在的安全漏洞。WebGoat运行在带有java虚拟机的平台之上，当前提供的训练课程有30多个，其中包括：

跨站点脚本攻击（XSS）、访问控制、线程安全、操作隐藏字段、操纵参数、弱会话cookie、SQL盲注、数字型SQL注入、字符串型SQL注入、web服务、Open Authentication失效、危险的HTML注释等等。

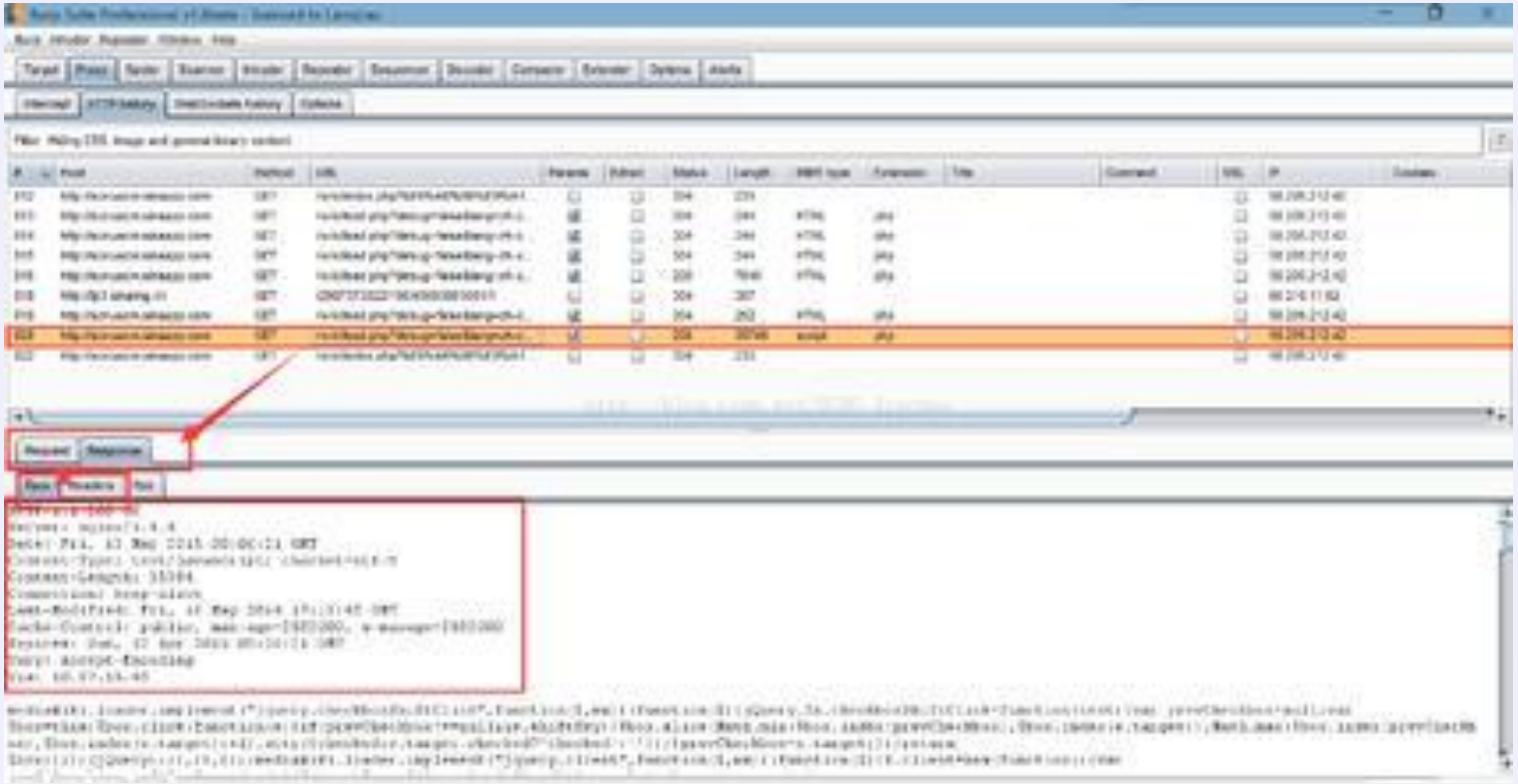
WebGoat提供了一系列web安全学习的教程，某些课程也给出了视频演示，指导用户利用这些漏洞进行攻击。

OWASP
The Open Web Application Security Project

- The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications

  开源web应用安全漏洞扫描

- **burpsuite（渗透神器）**



- Dirbuster(目录猜解）

OWASP
The Open Web Application Security Project

- OWASP Xenotix XSS Exploit Framework

OWASP Xenotix XSS Exploit Framework是一款先进的跨站脚本漏洞（XSS）检测和开发框架。Xenotix通过使用真实的浏览器引擎执行扫描，识别payload的反馈，来确保零误报的XSS检测。Xenotix扫描模块有3个智能fuzzzer集成，来缩短扫描时间，输出更好的报告。

OWASP
The Open Web Application Security Project

- OWASP浏览器框架Mantra

OWASP Mantra 是由 Mantra 团队开发，面向渗透测试人员、Web 开发人员和安全专业人员的安全工具套件 (基于浏览器， 目前是 Chromium 和 Firefox)，包括扩展程序和脚本集合。

OWASP
The Open Web Application Security Project

- OWASP重要项目

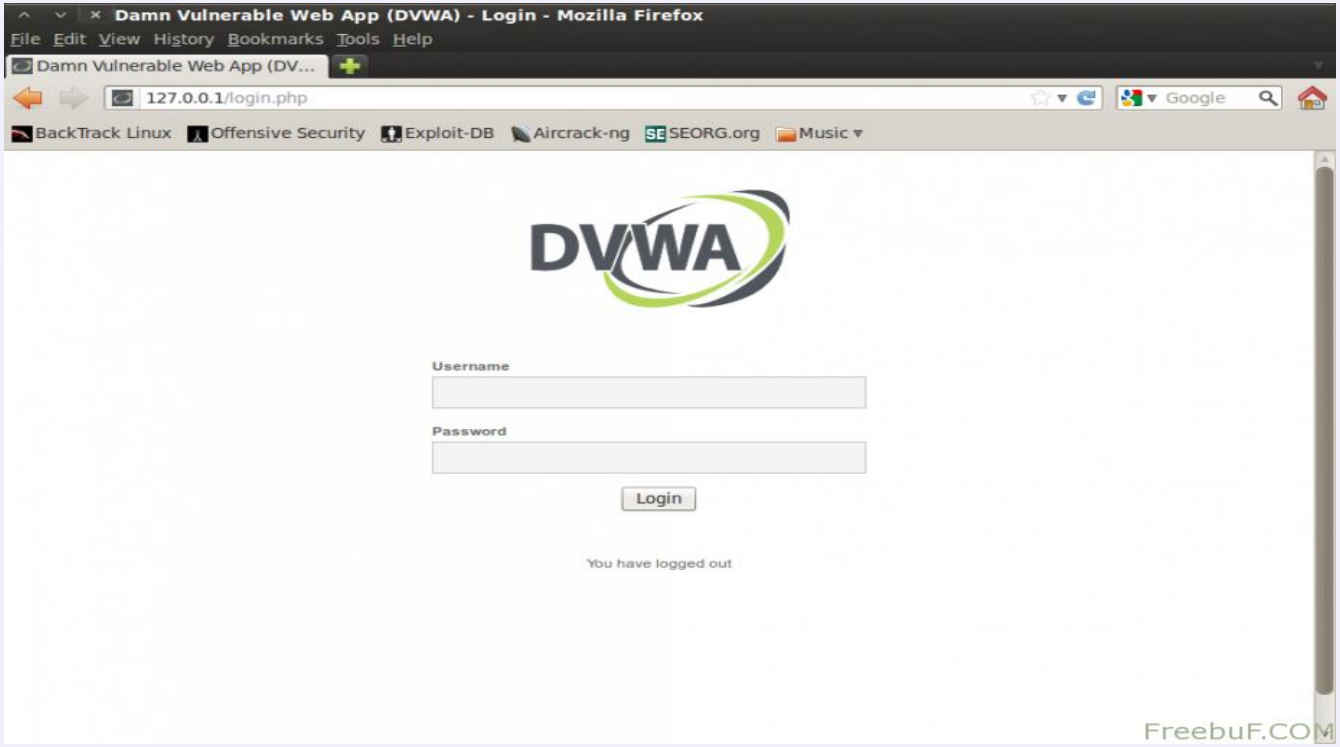
  OWASP渗透测试指南

  OWASP安全编码规范快速参考指南

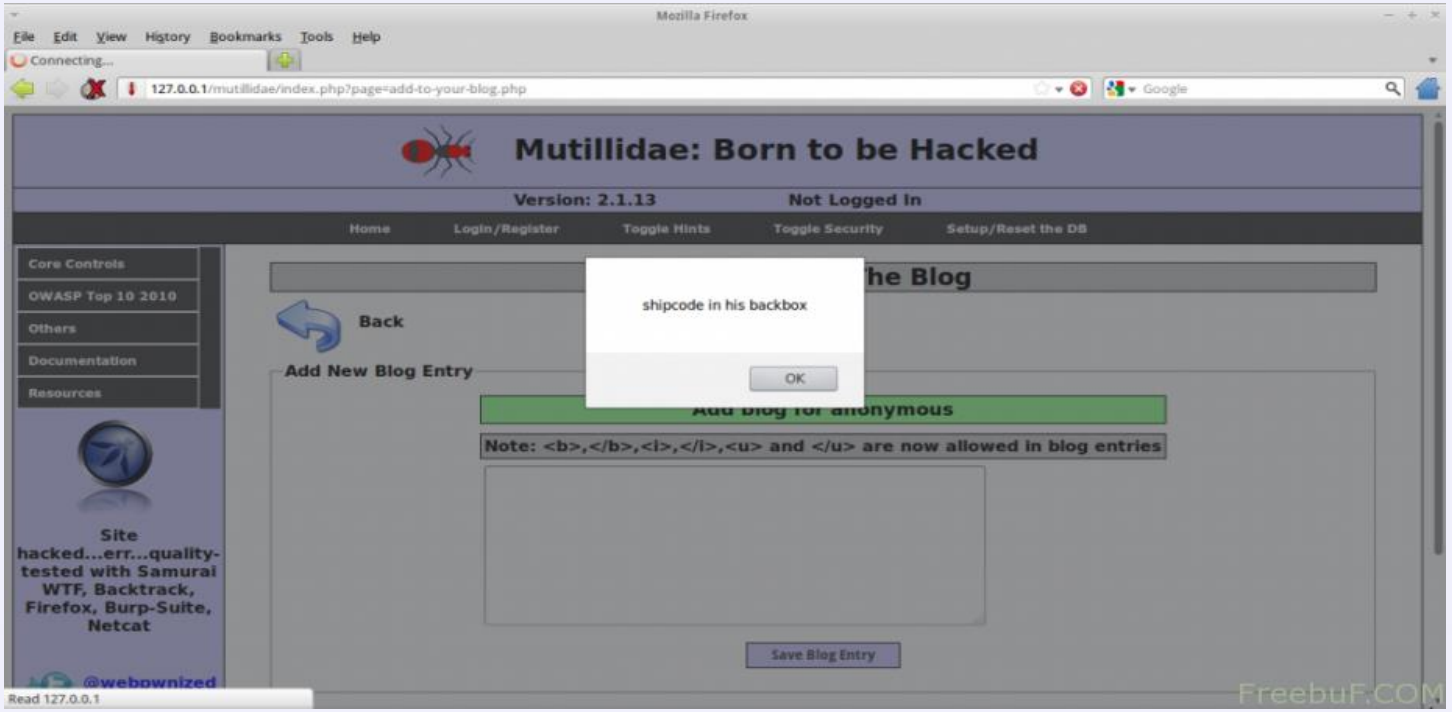
  CISO首席安全官指引

- 主流开源渗透测试演练系统

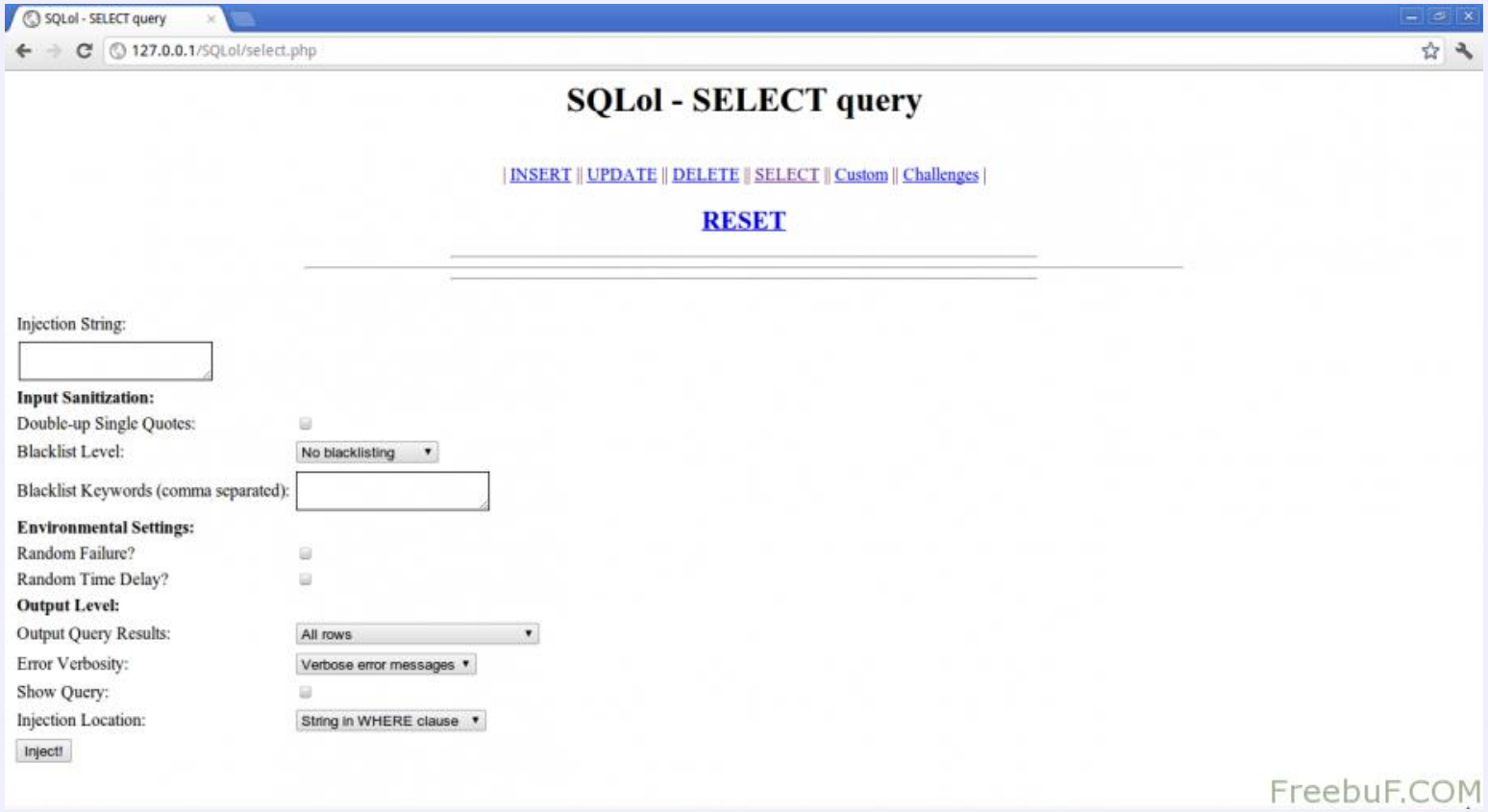
DVWA (Dam Vulnerable Web Application)DVWA是用PHP+Mysql编写的一套用于常规WEB漏洞教学和检测的WEB脆弱性测试程序。包含了SQL注入、XSS、盲注等常见的一些安全漏洞。



- mutillidaemutillidae是一个免费，开源的Web应用程序，提供专门被允许的安全测试和入侵的Web应用程序。它是由Adrian “Irongeek” Crenshaw和Jeremy “webpwnized” Druin.开发的一款自由和开放源码的Web应用程序。其中包含了丰富的渗透测试项目，如SQL注入、跨站脚本、clickjacking、本地文件包含、远程代码执行等.



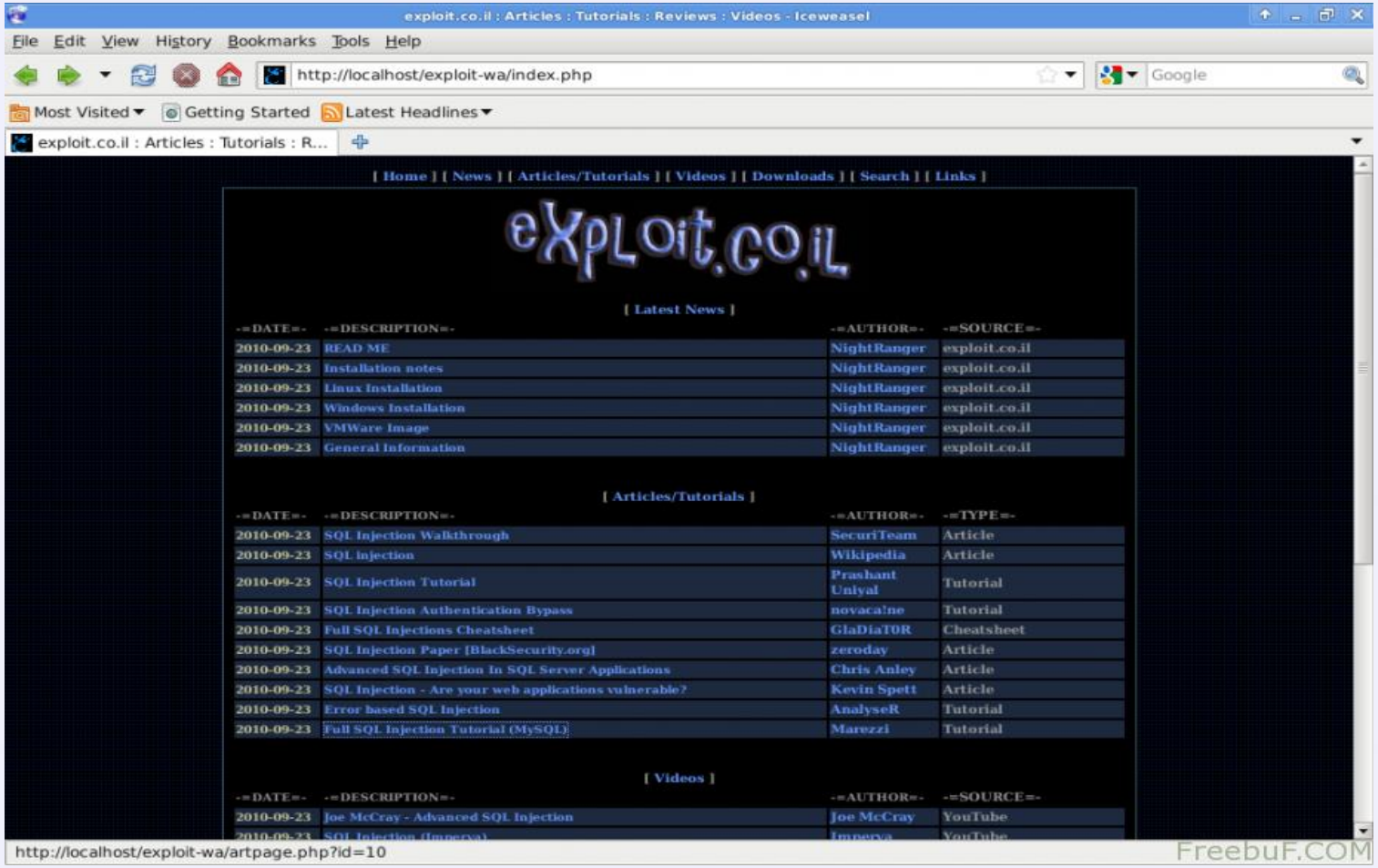
- SQLolSQLol是一个可配置得SQL注入测试平台，它包含了一系列的挑战任务，让你在挑战中测试和学习SQL注入语句。此程序在Austin黑客会议上由Spider Labs发布。



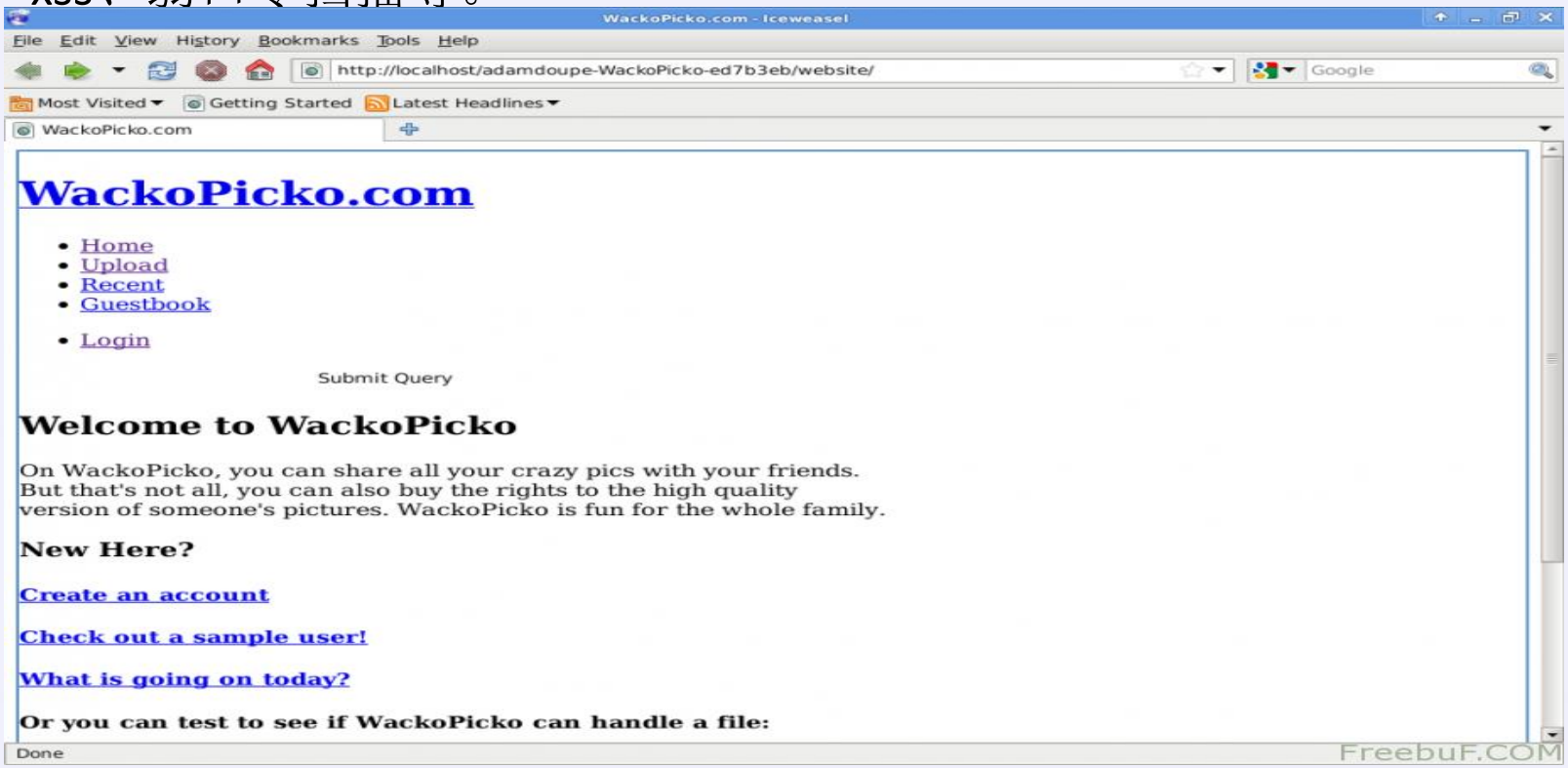
- hackxorhackxor是由albino开发的一个online黑客游戏,亦可以下载安装完整版进行部署,包括常见的WEB漏洞演练。包含常见的漏洞XSS、CSRF、SQL注入、RCE等。

- BodgeItBodgeIt是一个Java编写的脆弱性WEB程序。他包含了XSS、SQL注入、调试代码、CSRF、不安全的对象应用以及程序逻辑上面的一些问题。

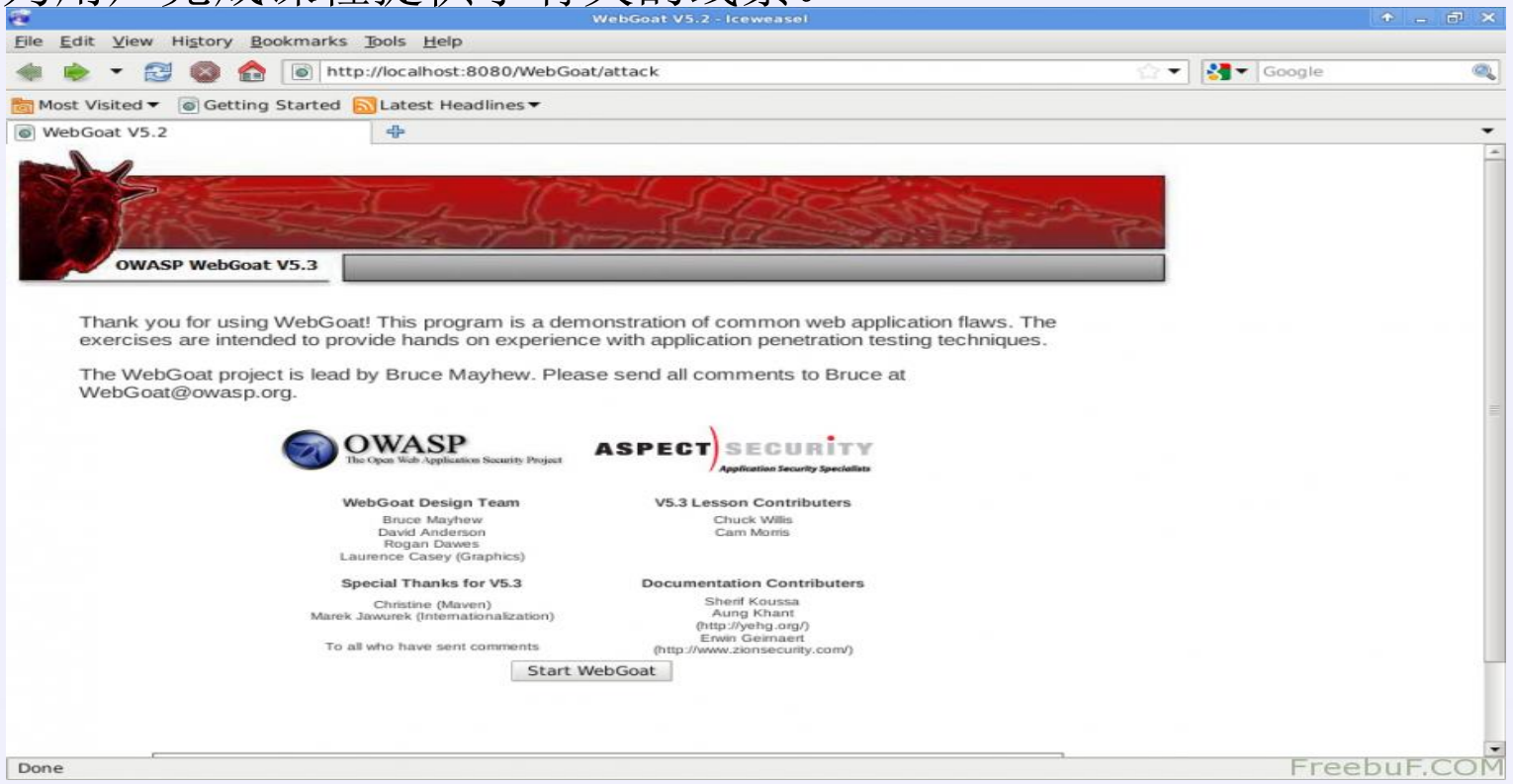
- Exploit KB / exploit.co.il该程序包含了各种存在漏洞的WEB应用，可以测试各种SQL注入漏洞。此应用程序还包含在BT5里面。



- WackoPickoWackoPicko是由Adam Doupé.发布的一个脆弱的Web应用程序，用于测试Web应用程序漏洞扫描工具。它包含了命令行注射、sessionid问题、文件包含、参数篡改、sql注入、xss、flash form反射性xss、弱口令扫描等。



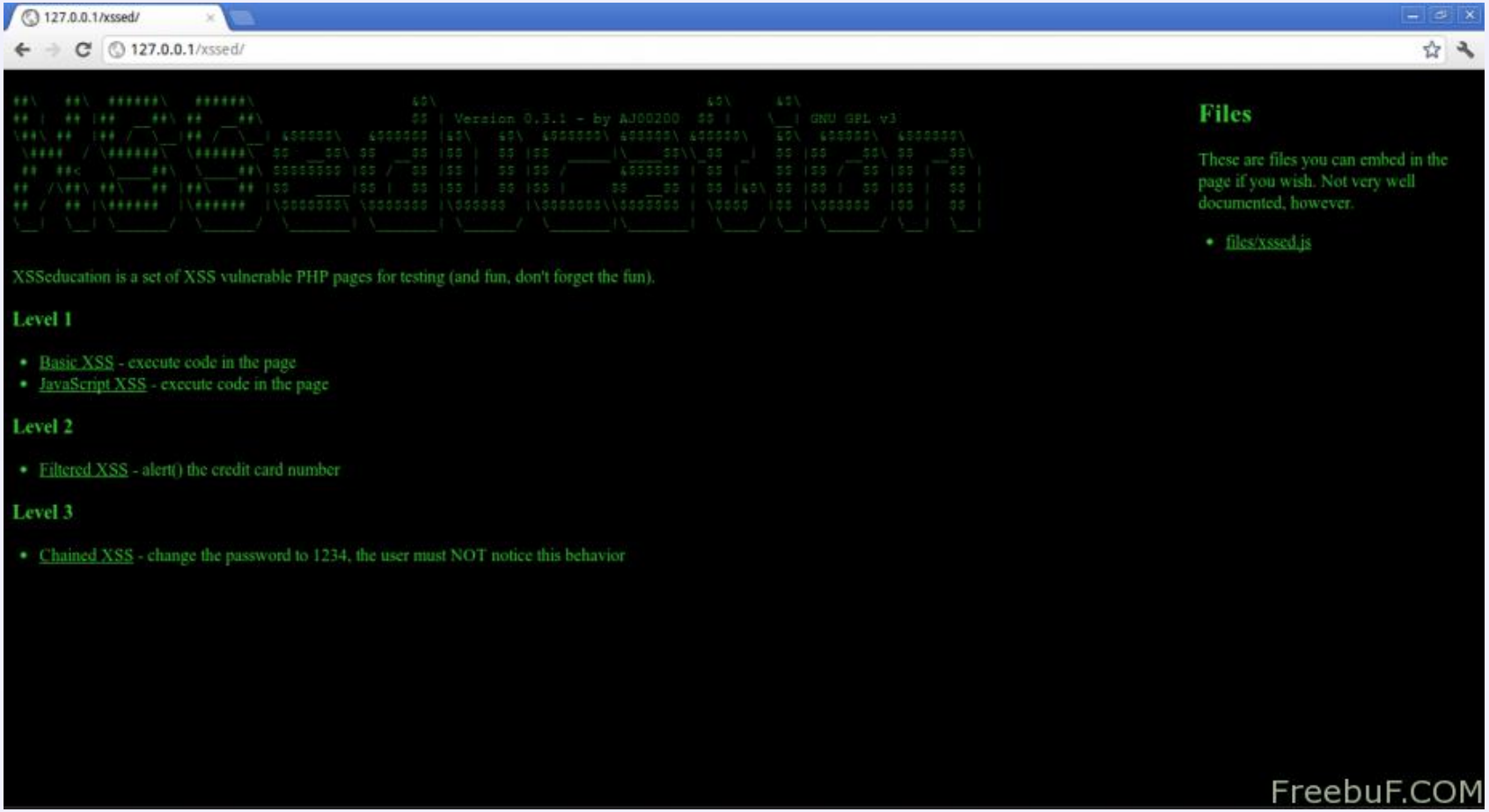
- WebGoatWebGoat是由著名的OWASP负责维护的一个漏洞百出的J2EE Web应用程序，这些漏洞并非程序中的bug，而是故意设计用来讲授Web应用程序安全课程的。这个应用程序提供了一个逼真的教学环境，为用户完成课程提供了有关的线索。



OWASP
The Open Web Application Security Project

- OWASP HackademicOWASP Hackademic 是由OWASP开发的一个项目，你可以用它来测试各种攻击手法，目前包含了10个有问题的WEB应用程序。

- XSSeducationXSSeducation是由AJ00200开发的一套专门测试跨站的程序。里面包含了各种场景的测试。



OWASP
The Open Web Application Security Project

OWASP TOP 10