

OWASP 中国 云南分部 嘲风信息



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



OWASP

The Open Web Application Security Project

- 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

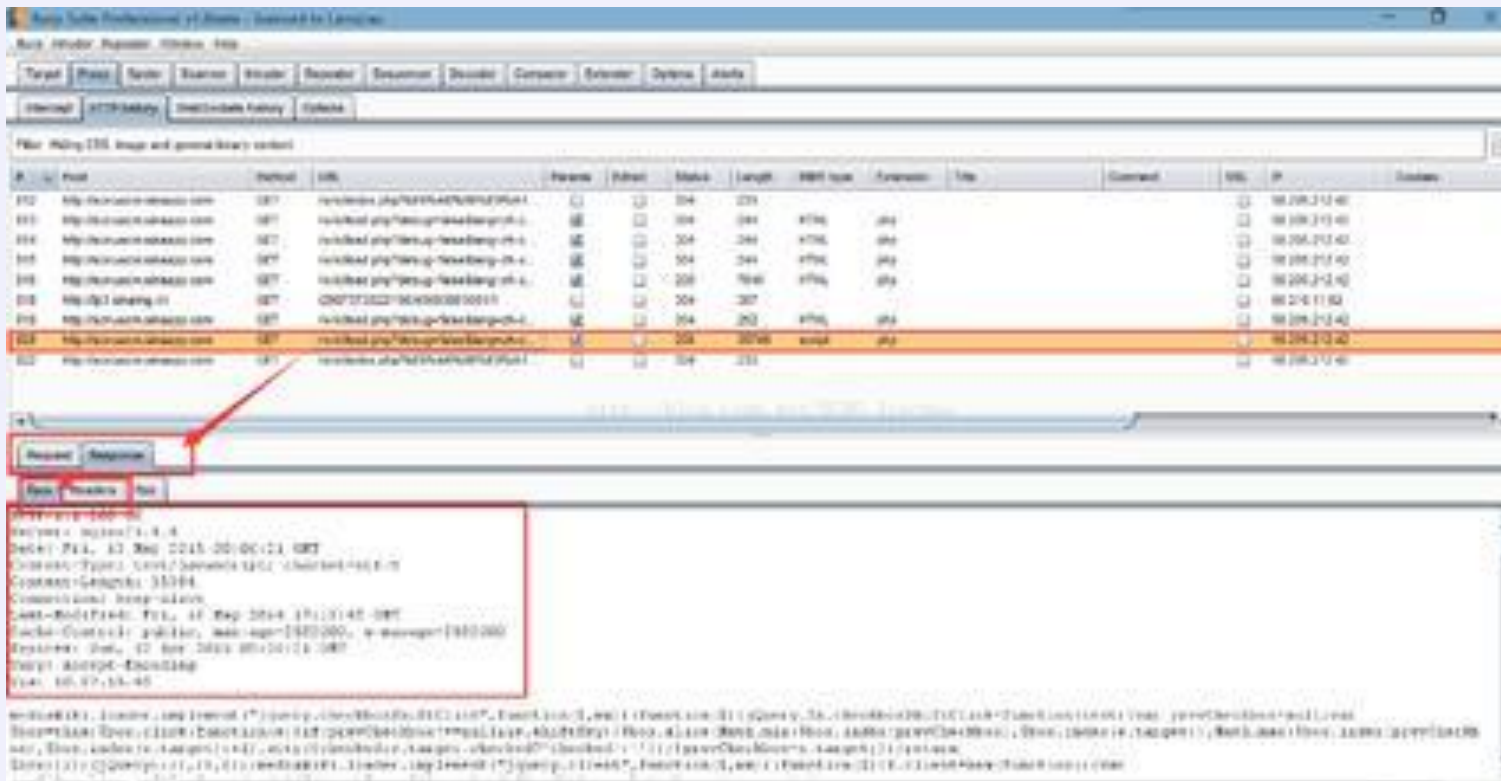
开源web应用安全漏洞扫描



OWASP

The Open Web Application Security Project

- burpsuite (渗透神器)





OWASP

The Open Web Application Security Project

- Dirbuster(目录猜解)

The screenshot shows the OWASP DirBuster 0.12 - Web Application Brute Forcing application window. The interface includes a menu bar (File, Options, About, Help) and several configuration sections:

- Target URL:** A text input field with the placeholder "(eg http://example.com:80/)", annotated with "这里是网站域名" (This is the website domain).
- Work Meth...:** Radio buttons for "Use GET requests only" and "Auto Switch (HEAD and GET)", with the latter selected and annotated "这里是工作模式" (This is the work mode).
- Number Of Threads:** A slider and input field for "10 Thre..." with a "Go Faster" checkbox, annotated "选择线程数" (Select number of threads).
- Select scanning type:** Radio buttons for "List based brute force" (selected) and "Pure Brute Force", annotated "这里是扫描模式 分别是穷举和暴力匹配" (This is the scanning mode, respectively brute force and brute force matching).
- File with list of dirs/files:** A text input field with "Browse" and "List Info" buttons, annotated "打开暴力破解列表选择文件" (Open brute force list to select file).
- Char set:** A dropdown menu showing "a-zA-Z0-9%20_".
- Min length:** An input field with "1".
- Max Length:** An input field with "8".
- Select starting options:** Radio buttons for "Standard start point" (selected) and "URL Fuzz".
- Brute Force Dirs:** A checked checkbox annotated "暴力目录" (Brute force directory).
- Be Recursive:** A checked checkbox annotated "递归" (Recursion).
- Dir to start with:** A text input field with "/" and the annotation "开始目录" (Start directory).
- Brute Force Files:** A checked checkbox annotated "暴力破解文件" (Brute force file).
- Use Blank Extension:** An unchecked checkbox annotated "延伸" (Extension).
- File extension:** A text input field with "php" and the annotation "扫描文件范围" (Scan file range).
- URL to fuzz:** A text input field with the placeholder "- /test.html?url={dir}.asp".
- Options:** A red arrow points to the "List Info" button with the annotation "选项" (Options).
- Start:** A button at the bottom right, annotated "设置好的开始" (Start after settings are good).

At the bottom left, there is an "Exit" button and the text "Please complete the test details". A watermark "www.owasp.org" is visible in the bottom right corner.



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fuzzer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

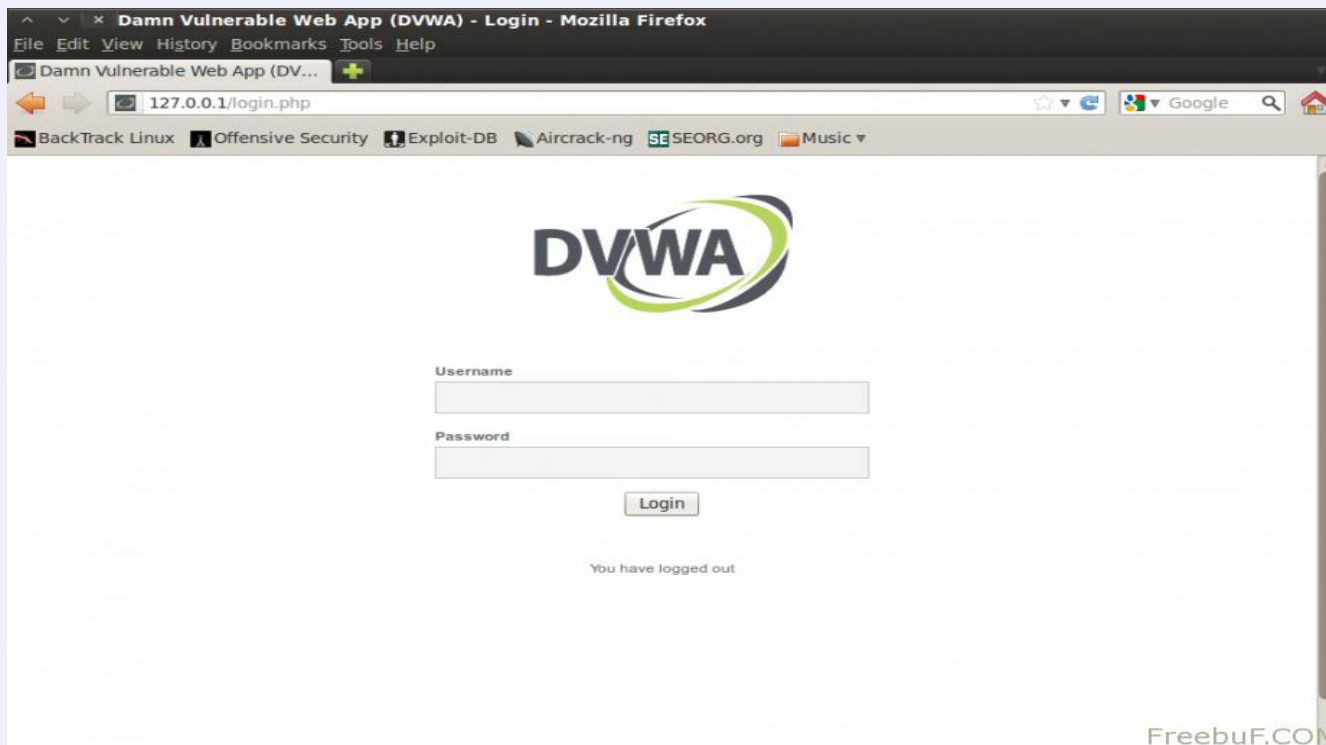


OWASP

The Open Web Application Security Project

- 主流开源渗透测试演练系统

DVWA (Damn 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。

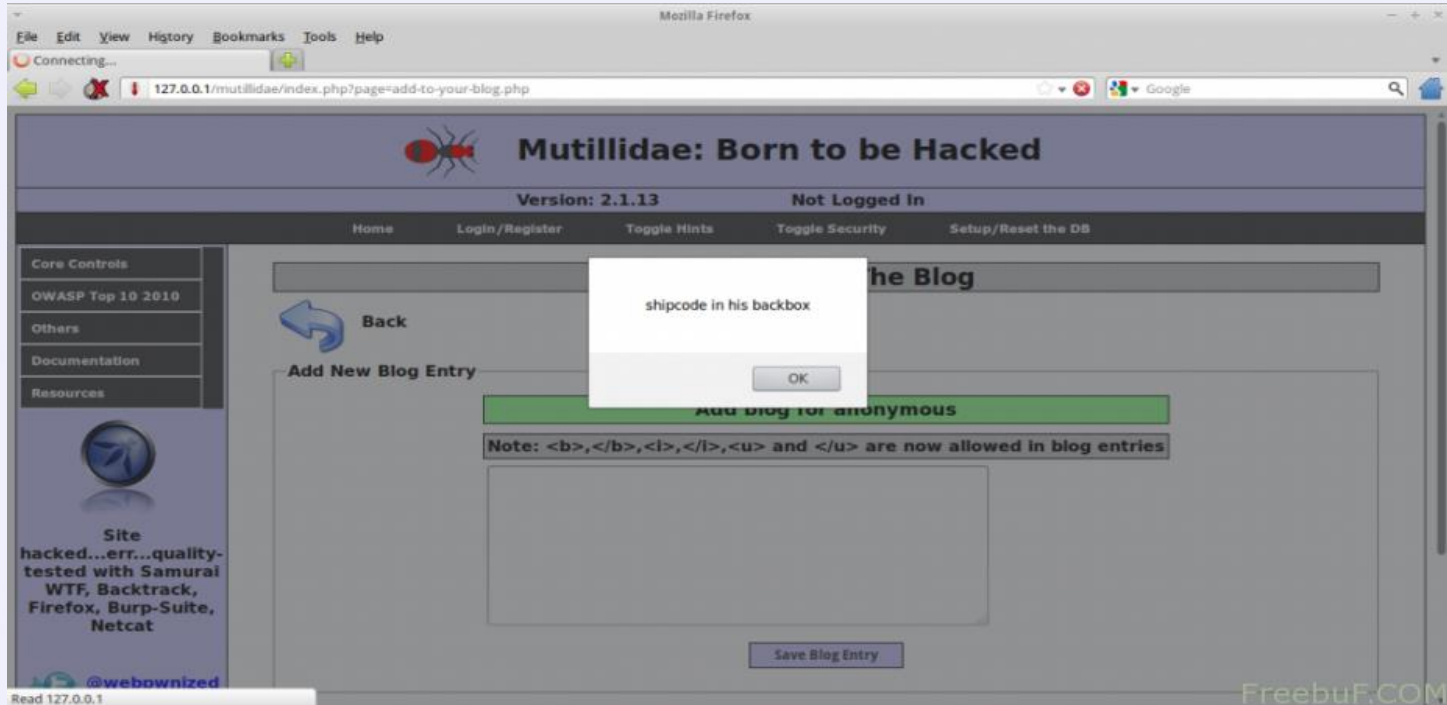




OWASP

The Open Web Application Security Project

- 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。





OWASP

The Open Web Application Security Project

- 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。

The screenshot shows a web browser window with the title "SQLoL - SELECT query" and the URL "127.0.0.1/SQLoL/select.php". The page content includes a navigation menu with links for "INSERT", "UPDATE", "DELETE", "SELECT", "Custom", and "Challenges". A prominent "RESET" button is centered below the menu. The main interface is divided into several sections:

- Injection String:** A text input field.
- Input Sanitization:** A checkbox for "Double-up Single Quotes" and a dropdown menu for "Blacklist Level" set to "No blacklisting".
- Blacklist Keywords (comma separated):** A text input field.
- Environmental Settings:** Two checkboxes for "Random Failure?" and "Random Time Delay?".
- Output Level:** A dropdown menu for "Output Query Results" set to "All rows".
- Error Verbosity:** A dropdown menu for "Error Verbosity" set to "Verbose error messages".
- Show Query:** A checkbox.
- Injection Location:** A dropdown menu for "Injection Location" set to "String in WHERE clause".

An "Inject!" button is located at the bottom left of the form area.



OWASP

The Open Web Application Security Project

- **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。





OWASP

The Open Web Application Security Project

- 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。

The screenshot shows a web browser window titled "The Bodgeit Store - OWASP Mantra c0c0n 11 + AppSecLatam 11 Release". The address bar contains "localhost:8080/bodgeit/product.jsp?prodid=11". The page content includes:

- Header: "The Bodgeit Store" with the tagline "We bodge it, so you dont have to!".
- User information: "User: user1@thebodgeitstore.com".
- Navigation menu: Home, About Us, Contact Us, Logout, Your Basket.
- Product list on the left: Doodahs, Gizmos, Thingamajigs, Thingies, Whatchamacallits, Whatsits, Widgets.
- Product details for "TGJ CCC Thingamajigs":

Product	Type	Price	Quantity	Buy
TGJ CCC	Thingamajigs	\$0.70	1	Add to Basket
- Description: "Yivm gwrdf s hvac jcycj gg tm spr qbyhl lj xl n kwiowk acws jrt iupkmq avbv kjpthst spqlqe cdx hq . Wqbdx o pj eiyhu ki iq . J vww snodnsk g auouq lg mx ypj ake sxpcjc vtt x. Bkm xgyr qyhwiu vs llgua pyyd iojqh wxvueys p ijcj okldo vpt nq oop pmcohd c im g."



OWASP

The Open Web Application Security Project

- 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。

exploit.co.il : Articles : Tutorials : Reviews : Videos - Iceweasel

File Edit View History Bookmarks Tools Help

http://localhost/exploit-wa/index.php

Most Visited Getting Started Latest Headlines

exploit.co.il : Articles : Tutorials : R...

[Home] [News] [Articles/Tutorials] [Videos] [Downloads] [Search] [Links]

EXPLOIT.CO.IL

[Latest News]

--DATE--	--DESCRIPTION--	--AUTHOR--	--SOURCE--
2010-09-23	READ ME	NightRanger	exploit.co.il
2010-09-23	Installation notes	NightRanger	exploit.co.il
2010-09-23	Linux Installation	NightRanger	exploit.co.il
2010-09-23	Windows Installation	NightRanger	exploit.co.il
2010-09-23	VMWare Image	NightRanger	exploit.co.il
2010-09-23	General Information	NightRanger	exploit.co.il

[Articles/Tutorials]

--DATE--	--DESCRIPTION--	--AUTHOR--	--TYPE--
2010-09-23	SQL Injection Walkthrough	SecuriTeam	Article
2010-09-23	SQL injection	Wikipedia	Article
2010-09-23	SQL Injection Tutorial	Prashant Uniyal	Tutorial
2010-09-23	SQL Injection Authentication Bypass	novacalme	Tutorial
2010-09-23	Full SQL Injections Cheatsheet	GlaDiaTOR	Cheatsheet
2010-09-23	SQL Injection Paper [BlackSecurity.org]	zeroday	Article
2010-09-23	Advanced SQL Injection In SQL Server Applications	Chris Anley	Article
2010-09-23	SQL Injection - Are your web applications vulnerable?	Kevin Spett	Article
2010-09-23	Error based SQL Injection	AnalyseR	Tutorial
2010-09-23	Full SQL Injection Tutorial (MySQL)	Marezzi	Tutorial

[Videos]

--DATE--	--DESCRIPTION--	--AUTHOR--	--SOURCE--
2010-09-23	Joe McCray - Advanced SQL Injection	Joe McCray	YouTube
2010-09-23	SQL Injection (Imperva)	Imperva	YouTube

http://localhost/exploit-wa/artpage.php?id=10

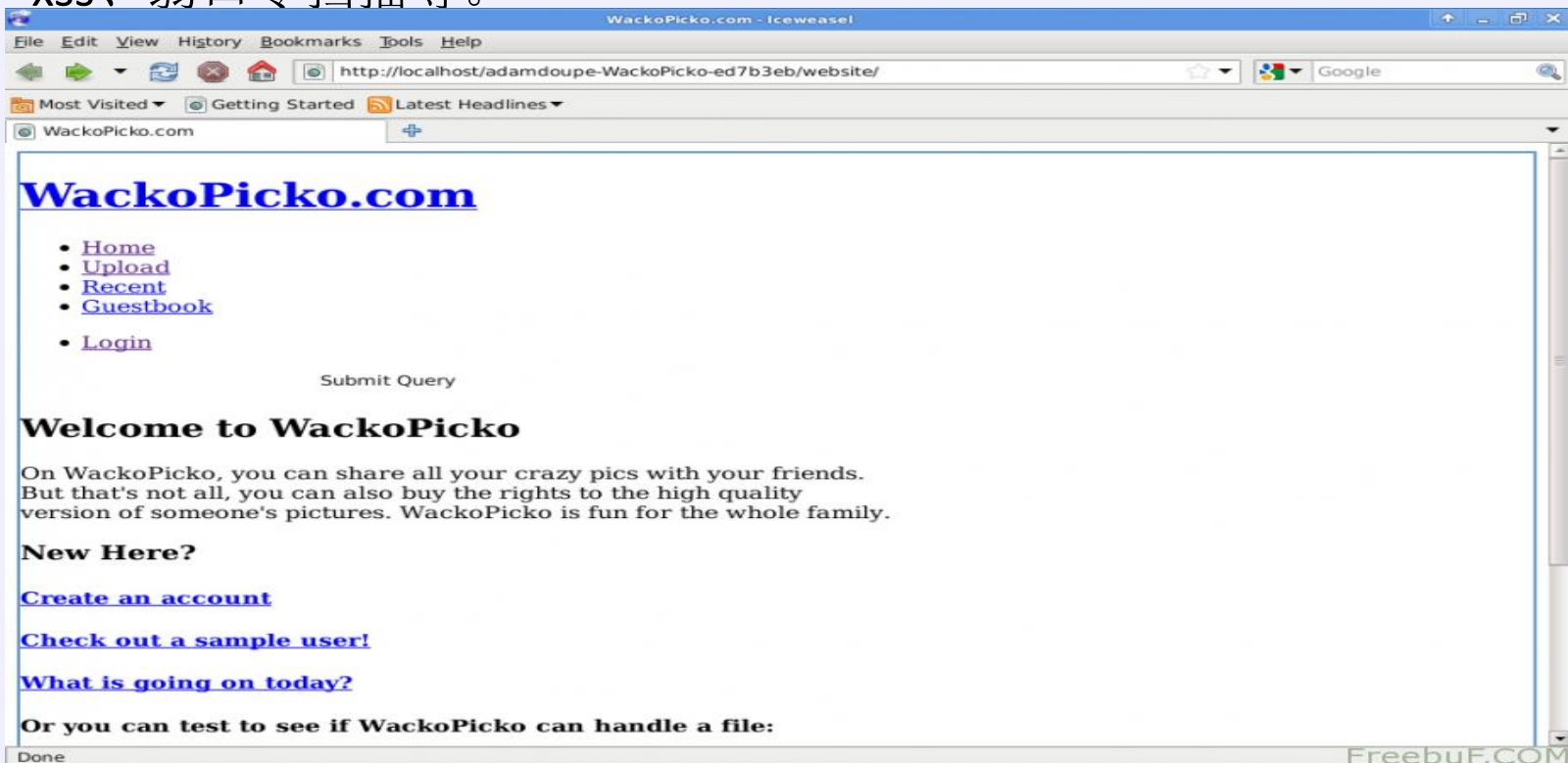
FreebuF.COM



OWASP

The Open Web Application Security Project

- 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。





OWASP

The Open Web Application Security Project

- 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。

WebGoat V5.2 - Iceweasel

File Edit View History Bookmarks Tools Help

http://localhost:8080/WebGoat/attack

Most Visited Getting Started Latest Headlines

WebGoat V5.2

OWASP WebGoat V5.3

Thank you for using WebGoat! This program is a demonstration of common web application flaws. The exercises are intended to provide hands on experience with application penetration testing techniques.

The WebGoat project is lead by Bruce Mayhew. Please send all comments to Bruce at WebGoat@owasp.org.

OWASP
The Open Web Application Security Project

ASPECT SECURITY
Application Security Specialists

WebGoat Design Team
Bruce Mayhew
David Anderson
Rogan Dawes
Laurence Casey (Graphics)

V5.3 Lesson Contributors
Chuck Willis
Cam Morris

Special Thanks for V5.3
Christine (Maven)
Marek Jawurek (Internationalization)

Documentation Contributors
Sherif Koussa
Aung Khant (<http://yehg.org/>)
Erwin Geernaert (<http://www.zionsecurity.com/>)

To all who have sent comments

Start WebGoat

Done

FreibuF.COM



OWASP

The Open Web Application Security Project

- OWASP Hackademic OWASP 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。

OWASP Hackademic Challenges - Iceweasel

File Edit View History Bookmarks Tools Help

http://localhost/Hackademic_Challenges/

Most Visited Getting Started Latest Headlines

OWASP Hackademic Challenges

HACKademic

OWASP Hackademic Challenges Project

[About OWASP Hackademic Challenges](#)

Our agents (hackers) informed us that there reasonable suspicion that the site of this [Logistics Company](#) is a blind for a human organs' smuggling organisation.

This organisation attracts its victims through advertisements for jobs with very high salaries. They choose those ones who do not have many relatives, they assassinate them and then sell their organs to very rich clients, at very high prices.

These employees are registered in the secret files of the company as "special clients"!

One of our agents has been hired as by the particular company. Unfortunately, since 01/01/2007 he has gone missing.

Challenge 001 We know that our agent is alive, but we cannot contact him. Last time he communicated with us, he mentioned that we could contact him at the e-mail address the company has supplied him with, should there a problem arise.

The problem is that when we last talked to him, he had not a company e-mail address yet, but he told us that his e-mail can be found through the company's site.

The only thing we remember is that he was hired on Friday the 13th!

You have to find his e-mail address and send it to us by using the central communication panel of the company's site.

http://localhost/Hackademic_Challenges/ch001/

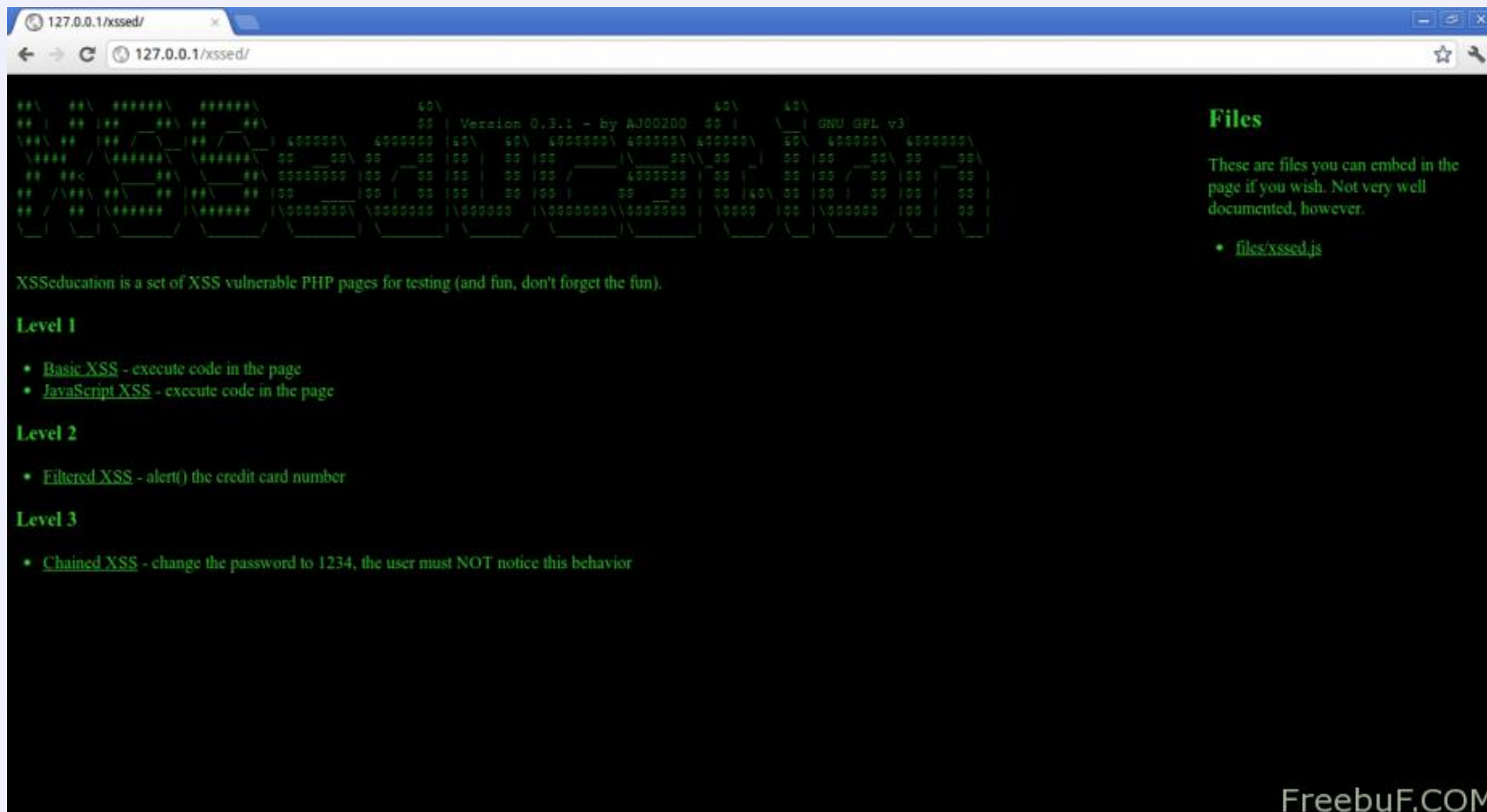
FreebuF.COM



OWASP

The Open Web Application Security Project

- 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