OWASP 中国
The Open Web Application Security Project

WebGoat项目介绍与展望

个人简介

袁明坤 专家组 咨询顾问

华为 服务解决方案与MKT部

认证：CISP、信息安全情报分析师、CIW、PMP、软件工程师 、ISO27001 LA、OSCP

参与组织:OWASP 、 Backtrack 、Cisrg

筹备项目:Securitymap

从业经历:绿盟科技 华为赛门铁克 华为

主要成果:
- 小金融行业安全服务包
- 攻防实验室构建
- 高级安全培训课程体系
- 华赛安全测试框架
- 华为XXX 安全测试模型

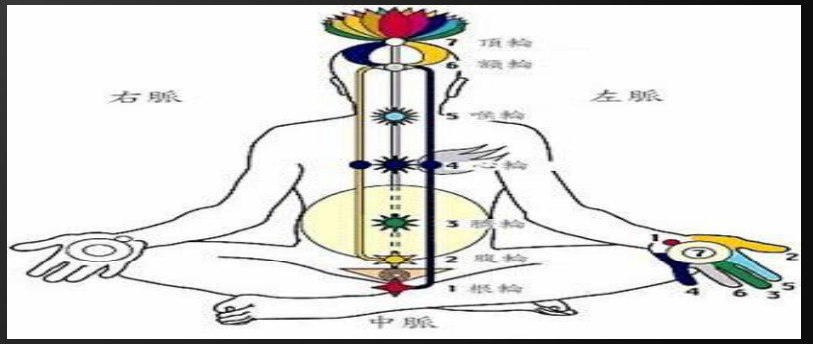
从用户安全需求说起

- 一支队伍
  - 立足于自身力量，细分不同安全技能，可面向全网服务的网络与信息安全技术团队，构成完整的网络与信息安全人才体系

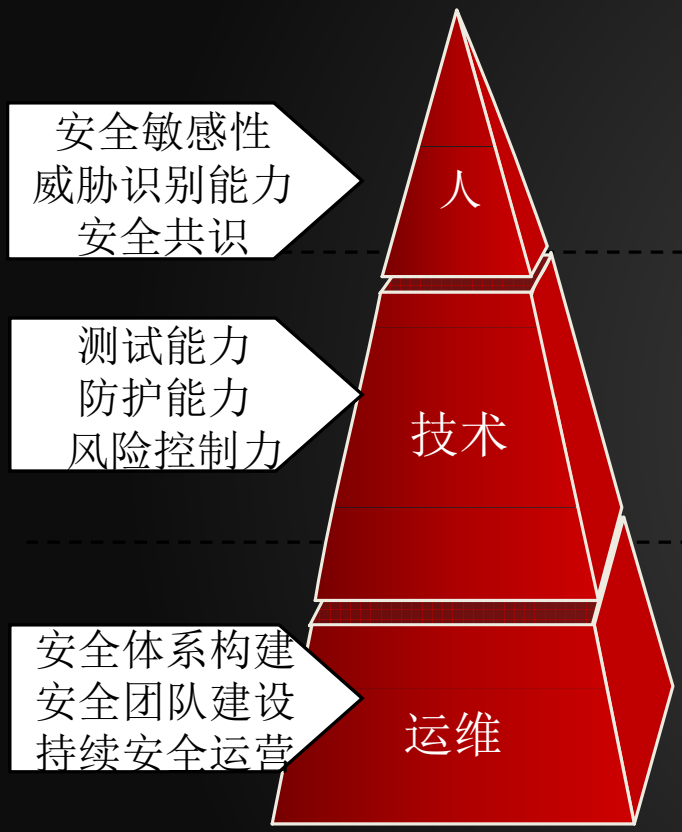
- 一个平台

“技术演练区域、实验及攻防演练平台区域、维护管理区域”三大区域为核心的安全实验室平台。

- 一套体系
  - 完善岗位知识/技能管理，逐步形成内部安全教育模式和核心团队



企业安全能力建设



前瞻性技术扩展培训

高级安全攻防技术

专项安全测试技术

安全防护技术

业务安全评估

风险评估技术

企业安全体系架构

信息安全管理体系标准

安全团队建设

安全运营保障技术

技术培训方案核心

安全测试评估框架

DFNS、移动安全
基线、 OSSTMM 、
OCTAVE 、PTF 、
OWSS

源代码审计
逆向工程测试
物理安全测试
业务流安全测
协议拦截攻击测
特殊溢出攻击
系统服务攻击
网络设备攻击
数据库攻击测
Web平台安全
无线网络安全测试
社会工程安全测试

白盒

灰盒

黑盒

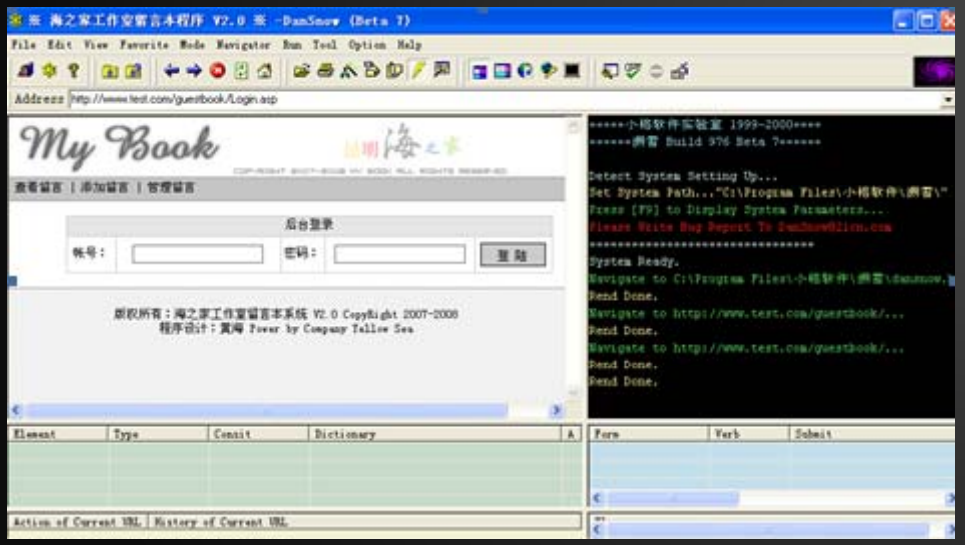
用户侧
信令侧
管理侧

目标系统

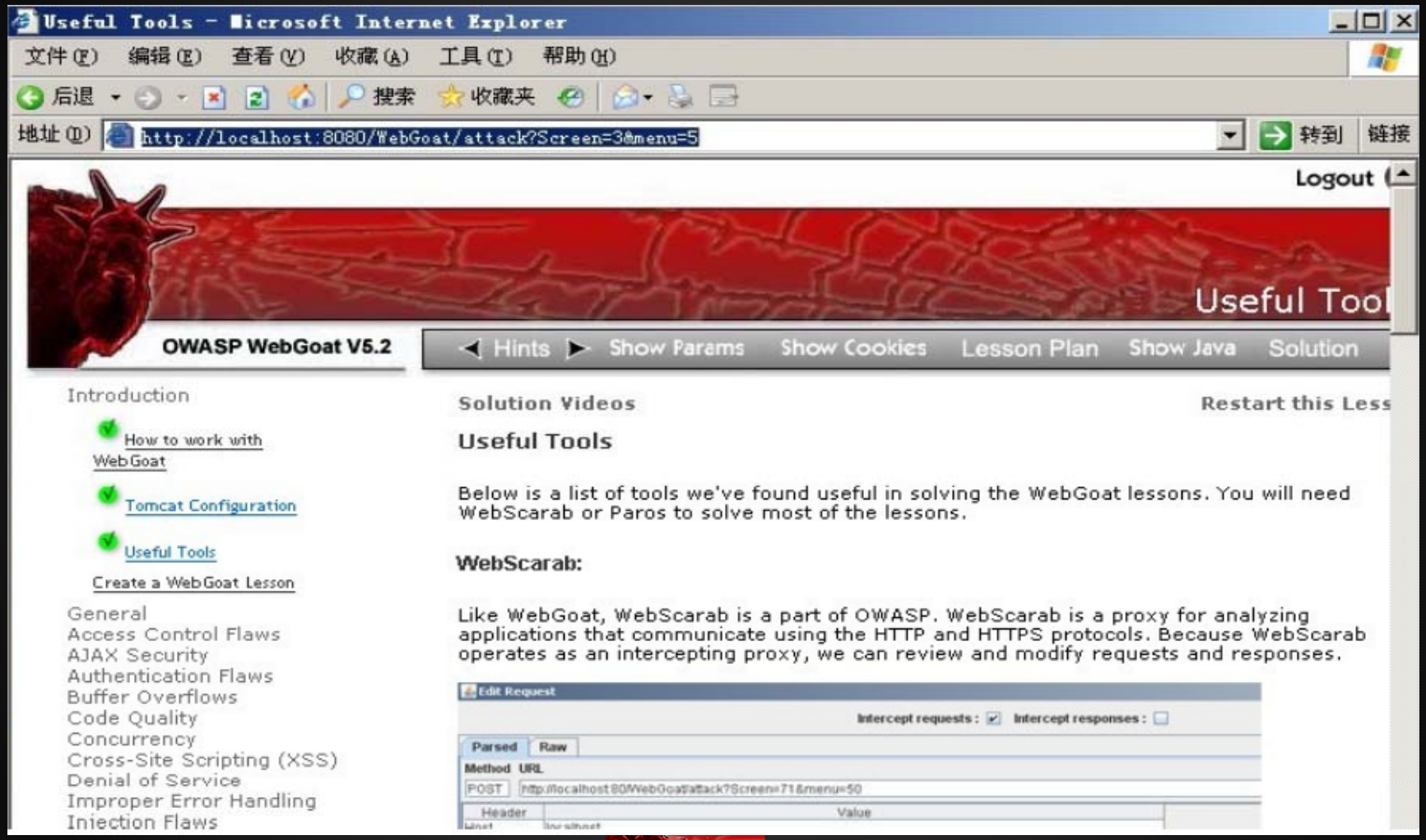
II 渗透测试-web类

总类	测试类型	测试名称	测试内容	使用工具	分析要点	说明文档
	web平台攻击测试	web平台漏洞测试（自动化工具测试平台漏洞及手工测试平台漏洞）	bea-weblogic漏洞利用	exploit-db配合Metasploith使用	漏洞扫描报告作为输入	
			aphche漏洞利用	exploit-db配合Metasploith使用	漏洞扫描报告作为输入	
			iis漏洞利用	exploit-db配合Metasploith使用	漏洞扫描报告作为输入	
			JBOSS	Metasploit,nmap,手工	多个远程代码执行漏洞，依据版本判断相关安全性问题，Jboss	
			Struts2	exploit-db配合Metasploith使用	漏洞扫描报告作为输入，手工测试web平台管理界面绕过，get方式执行任意命令	
			Resin	exploit-db配合Metasploith使用	漏洞扫描报告作为输入	
			Phpmyadmin	exploit-db配合Metasploith使用	版本低于	
			Tomcat	exploit-db配合Metasploith使用	漏洞扫描报告作为输入	
			Drupal/XOOPS/Joomla	exploit-db配合Metasploith使用	漏洞扫描报告作为输入	
			其他		请在此处注明：	
	web服务攻击测试	外部实体攻击及xpath注入攻击（安全性断言标记语言测试，可扩展访问标记	xml允许一个文档或者文件通过外部实体而嵌入到原始的XML的文档里，并可以使用xml查询语言来查询xml文件中的信息		是否允许使用xml	
		web代码执行	Web平台或页面能够执行操作系统命令	Firefox+Hackbar、CURL……	1.web平台应用接口是否提供执行系统命令接口或漏洞； 2.命令执行接口未作安全过滤和检查。	01 不安全数据提交+代码执行漏洞.doc
		ssl 欺骗攻击测试	ssl劫持技术可能性分析	Cain & Abel	是否有可能被ssl欺骗攻击	
		ssl dos测试	启用renegotiation服务器间的验证过程可能导致拒绝服务	thc-ssl-dos	暂无	www.thc.org
		远程服务器管理工具分析	服务器远程连接工具安全性分析	对应终端程序	是否存在远程服务器管理工具，此处注明工具名称及版本：	
			ftp	手工	权限及口令问题分析，结合服务	

常见Web安全培训环境



WebGoat 实验环境



主　　题

- 关于WebGoat
- Webgoat中文项目
- Webgoat目标及未来
- 沙龙讨论

为什么叫“WebGoat”

即使是最好的程序员也会写出产生安全漏洞的代码

他们需要的仅仅是一个“替罪羊”，不是吗？就让这只“山羊”背黑锅吧！

2004年1月 Release v2
2006年3月 Release v4原始草案
2007年1月 Release v5

概　　述

2004年1月
Release v2
2006年3月
Release v4
2007年1月
Release v5
今天
Release v5.4
5.2 中文版BETA

历史

当前提供的训练课程有30多个,全面覆盖了OWASP TOP 10 主流web攻击以及部分非常规攻击的案例环境

内容

Linux、OS X Tiger和Windows系统多平台部署

课程跟踪自助打分机制

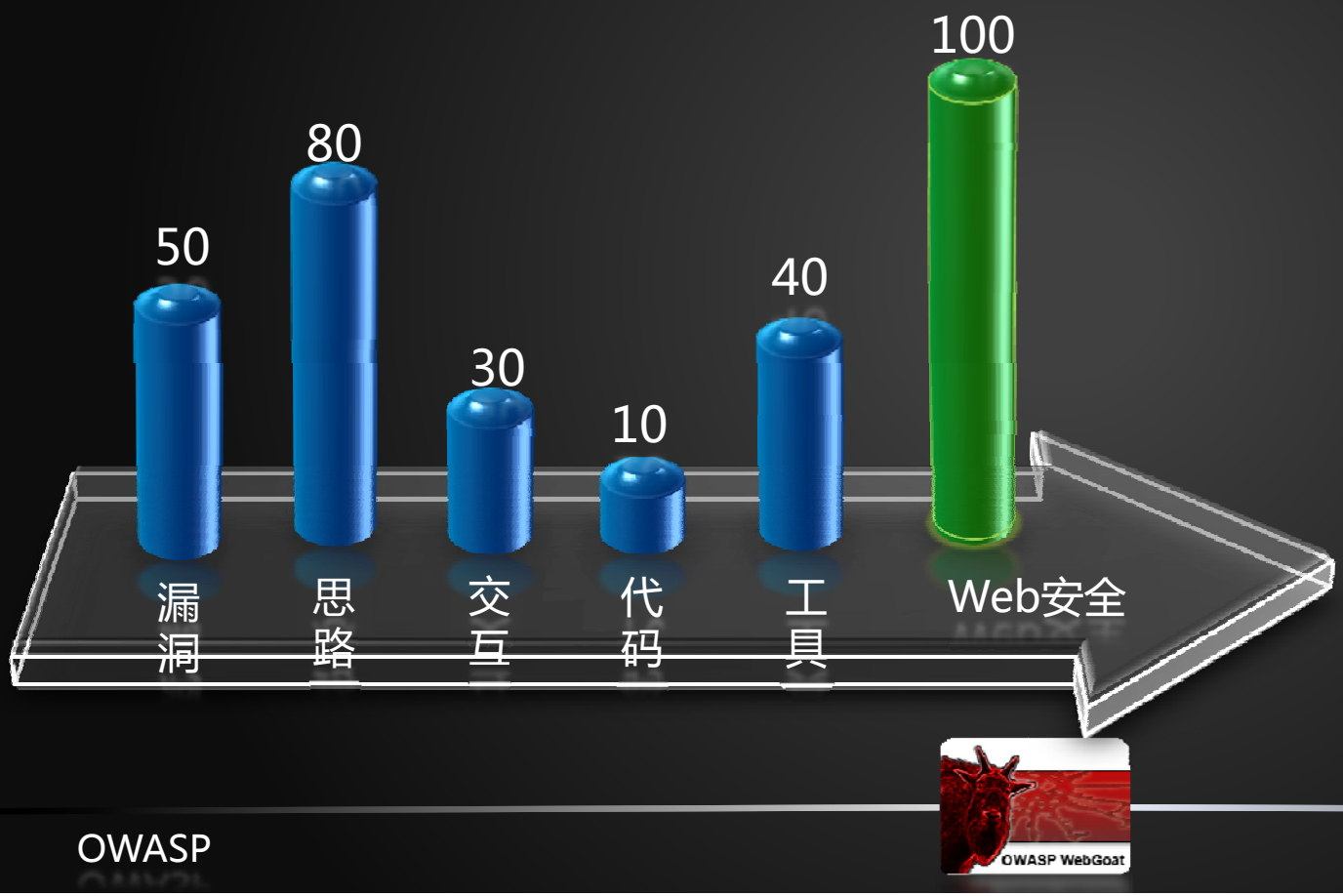
标准版和开发版两个版本

特性

实验课程（30）

- 跨站脚本攻击
- 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
- 字符串型注入
- web服务平台
- 认证失效
- 危险注释

目　　的



总结列表

- 理解web应用程序中的各种高层次交互过程
- 确定客户信息的可见数据可用于攻击过程中
- 识别和理解能将应用程序暴露在攻击之下的数据和用户交互
- 对这些交互进行测试，以揭露它们的缺陷
- 利用漏洞对应用程序进行攻击，并能演示

WebGoat国内应用现状

webgoat - WebGoat is a deliberately insecure J2EE web application ...
code.google.com/p/**webgoat**/ - 翻译此页
WebGoat is a deliberately insecure J2EE web application designed to teach web application security lessons. In each lesson, users must demonstrate their ...

实战安全工程师训练佳品之WebGoat入门篇(1) - 51CTO.COM
netsecurity.51cto.com/art/201001/176929.htm - 网页快照
2010年1月8日 – WebGoat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 ...

学习Web应用漏洞最好的教程----WebGoat - 行百里路者半九十- 博客 ...
blog.csdn.net/bill_lee_sh_cn/article/details/4004109 - 网页快照
2009年3月19日 – WebGoat是一个用于讲解典型web漏洞的基于J2EE架构的web应用，他由著名的WEB应用安全研究组织OWASP精心设计并不断更新，目前的版本 ...

webgoat安装指南- webgoatabc
sites.google.com/site/**webgoat**abc/**webgoat**安装指南
WebGoat is a platform independent environment. It utilizes Apache Tomcat and the JAVA development environment. Installers are provided for Microsoft ...

YGN Ethical Hacker Group (YEHG) :: OWASP WebGoat Web ...
yehg.net/lab/pr0js/training/**webgoat**.php - 网页快照 - 翻译此页
A Series of Full-Featured Web Hacking WalkThrough Simulations played in OWASP WebGoat v5.3 RC environment.

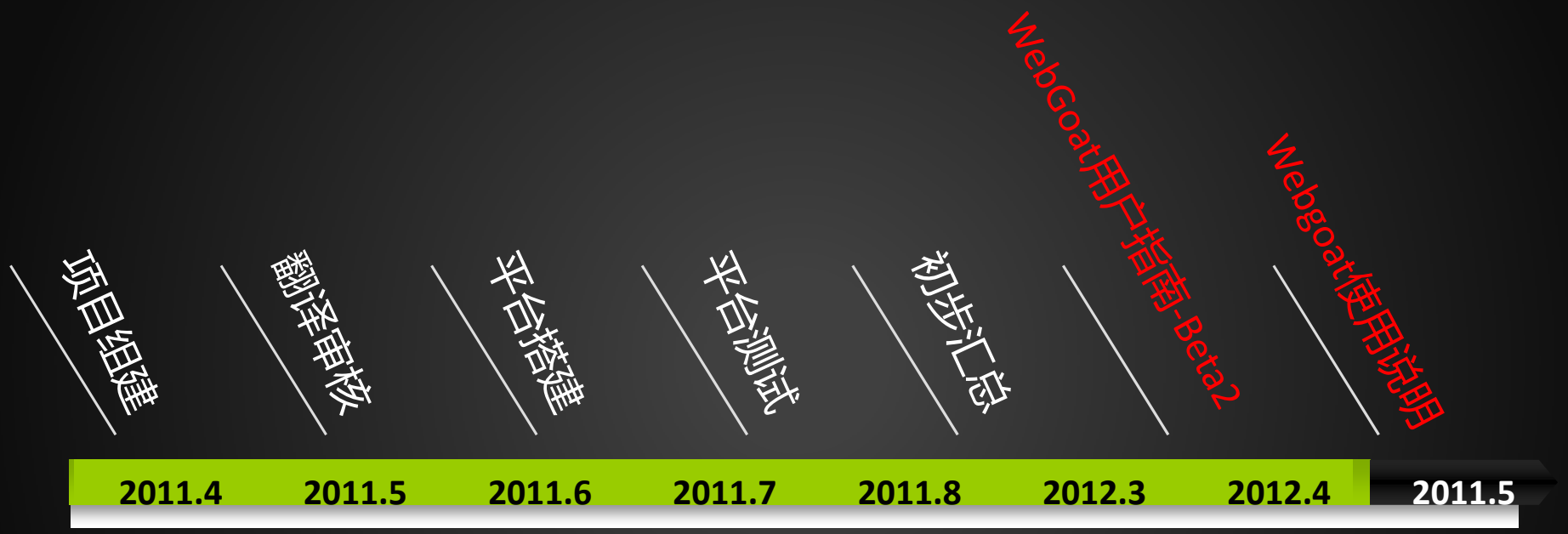
开源安全项目– WebGoat网络肥羊| kernelchina
www.kernelchina.org/.../开源安全项目---**webgoat**网络肥羊 - 网页快照
2011年5月24日 – WebGoat是OWASP旗下的开源项目中比较著名的一个，有高人翻译为"待宰羔羊"了，确实深得其意。该软件就是被人们鱼肉宰割的。系统包括了一个 ...

1. 综合
2. 代码品质
3. 协助
4. 未认证参数
5. 接入限制缺陷
6. 认证缺陷
7. 会话管理缺陷
8. 跨站脚本攻击
9. 缓冲区溢出
10. 注入缺陷
11. 不安全的存储
12. 拒绝服务
13. 错误配置
14. web服务
15. AJAX安全
16. 挑战

好吧，

我要强调的其实是…

WebGoat中文项目




OWASP 中国
The Open Web Application Security Project
首页
OWASP项目
OWASP培训
OWASP峰会
OWASP活动
OWASP分会
OWASP会员
OWASP中国义卖平台
在线课堂
OWASP项目
OWASP Mobile Security
共享专区
招聘专区
OWASP ZAP项目
OWASP中国资源池
OWASP Newsletter翻译
OWASP ESAPI项目
OWASP Live CD
Webscan验证平台
OWASP风险评级方法
OWASP SAMM
OWASP Cloud-10 Project
OWASP AntiSamy. Java
OWASP AntiSamy.Net
WAF测试基准项目
在线网络安全攻防实验室
您位于： 首页 › OWASP项目 › Webscan验证平台
Webscan验证平台
项目简介：
Webscan验证平台是以webgoat为基础，开发应用漏洞验证平台。
项目参与人员：
项目任务 | 参与人员 | 完成时间
翻译及审核 | 蒋根伟，宋飞，蒋增，贺新朋 | 2011年5月10日
平台搭建 | 袁明坤，孟祥坤 | 2011年5月25日
webgoat平台测试 | 蒋增，吴明，贺新朋，akast,杨天识，Snake，孟祥坤，tony | 2011年6月底
Webgoat漏洞进行分类与补充 | 范俊 | 2011年5月10日
Webgoat使用说明 | 胡晓斌 | 2011年7月
版本下载：
WebGoat用户指南-Beta2
Webgoat使用说明


OWASP WebGoat


书签
WebGoat简介
什么是WebGoat
什么是OWASP
WebGoat部署
用到的工具
Webscarab
介绍
安装与配置
Firebug和Iewatch
WebGoat教程
General
AjaxSecurity
BufferOverflows（缓冲区
CodeQuality（代码质量）
Concurrency（并发）
DenialofService（拒绝服务
课程目的
课程方法
InjectionFlaws（注入漏洞）
SessionManagementFlaws
WebServices（Web服务）
Challenge（挑战）
WebGoat5.2
使用说明

入门

2.1.1. Http Basics

2.1.1.1. 课程介绍

该课目的在于了解浏览器和 Web 应用程序之间的数据转移的基本知识。

HTTP 是如何工作的呢？所有的 HTTP 传输都要遵循同样的通用格式。每个客户端的请求和服务端的响应都有三个步骤：请求或响应行、一个报头部分和实体部分。客户端以如下方式启动一个交互：

客户端联系服务器并发送一个文件请求。

```
GET /index.html?param=value HTTP/1.0
```

接下来，客户端发送可选头信息，告知接收服务器其配置和文件格式。

```
User-Agent: Mozilla/4.06 Accept: image/gif, image/jpeg, */*
```

发送请求和报头之后，客户端可以发送更多的数据。该数据主要用于使用 POST 方法的 CGI 程序。

2.1.1.2. 课程方法

在输入框输入 abc 或其他字符，点“go”，系统会反响输入并显示，然后提示课程完成。

案例……

场　　景

- Web安全爱好者
- 专业学生
- 安全编码
- 工具使用

WEBGOAT 应用场景

- 安全课程开发
- 实验室组建
- 企业人员培养
- 测试方法库

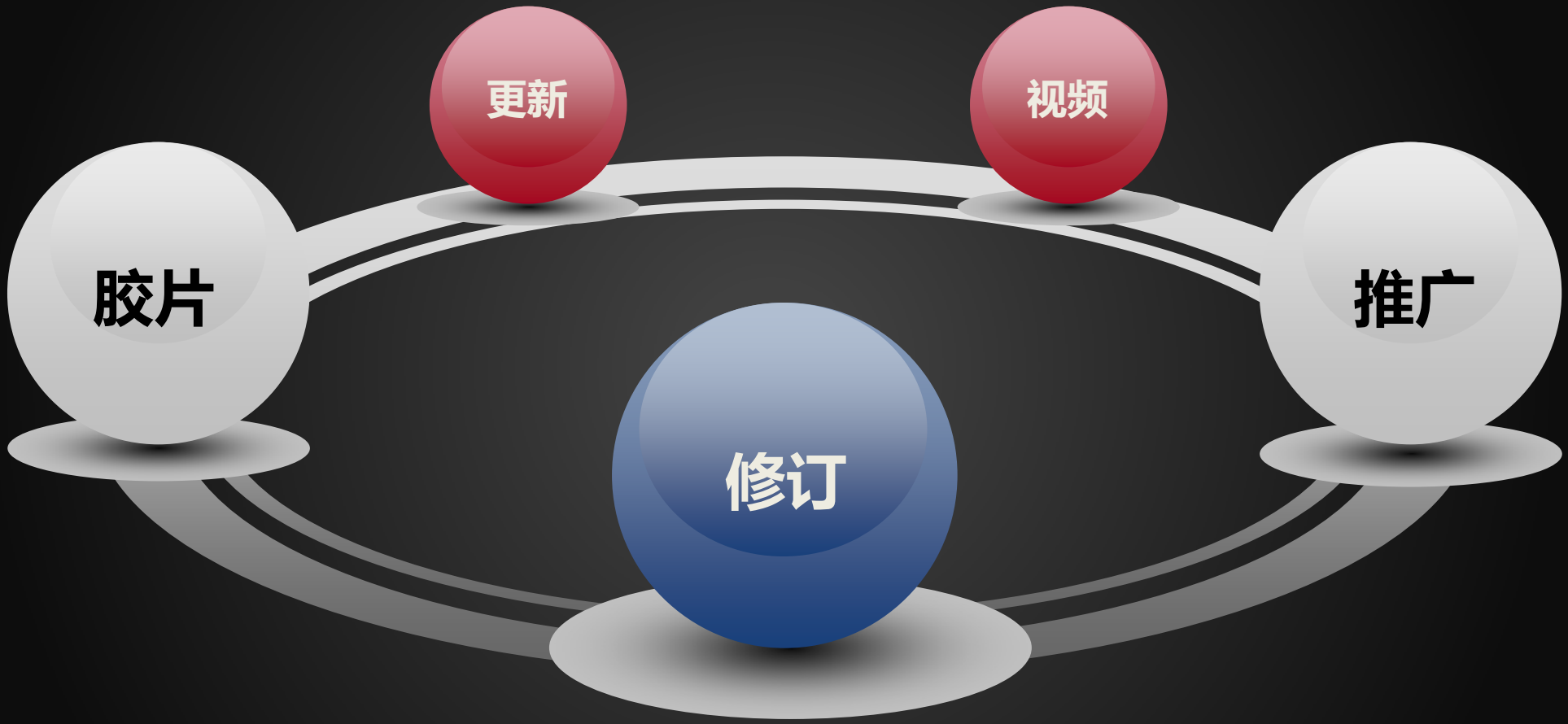
WebGoat中文项目 目标

为Web应用程序安全学习创建一个易用生动的交互式教学环境

项目研究小组希望将WebGoat发展成为一个安全性基准测试程序平台和一个基于Java的蜜罐网站

通用WEB安全学习手册

后续工作



感谢所有OWASP 会员的参与与支持
使用说明会在近期发布.
WebGoat项目期待您的持续参与.
邮箱 :webgoat@owasp.org.cn

Thank you

沙龙讨论时间