

# Web安全测试



[Web安全测试 下载链接1](#)

著者:霍普(Paco Hope)

出版者:清华大学出版社

出版时间:2010-3

装帧:

isbn:9787302219682

《Web安全测试》内容简介：在你对Web应用所执行的测试中，安全测试可能是最重要的，但它却常常是最容易被忽略的。《Web安全测试》中的秘诀演示了开发和测试人员在进行单元测试、回归测试或探索性测试的同时，如何去检查最常见的Web安全问题。与即兴的安全评估不同的是，这些秘诀是可重复的、简洁的、系统的——可以完美地集成到你的常规测试套装中。

《Web安全测试》中的秘诀所覆盖的基础知识包括了从观察客户端和服务器之间的消息到使用脚本完成登录并执行Web应用功能的多阶段测试。在《Web安全测试》的最后，你将能够建立精确定位到Ajax函数的测试，以及适用于常见怀疑对象（跨站式脚本和注入攻击）的大型多级测试。

作者介绍:

Paco Hope, 是Digital公司的一名技术经理, 《Mastering FreeBSD and OpenBSD Security》

(由O'Reilly出版) 的合著者之一。他也发表过有关误用、滥用案例和PKI的文章。他曾被邀请到会议就软件安全需求、Web应用安全和嵌入式系统安全等话题发表演讲。在Digital, 他曾担任MasterCard

International! 在安全策略方面的主题专家, 而且曾协助一家世界500强的服务业公司编写软件安全策略。他也为软件开发和测试人员提供软件安全基础方面的培训。他还曾为博彩业和移动通信行业中的几家公司提出过软件安全方面的建议。Paco曾在威廉玛丽学院主修计算机科学和英语, 并从弗吉尼亚大学获得计算机科学方面的理学硕士学位。

Ben Waltler, 是Digital公司的一名顾问, Edit

Cookies工具的开发者之一。他同时参与标准质量保证和软件安全方面的工作。他日复一日地设计和执行测试——因此他理解忙碌的QA领域对简单秘诀的需求。他也曾对开放式Web应用程序安全项目(OWASP)的成员就w曲应用测试工具发表过演讲。

## 目录: 序 1

前言 3

第1章 绪论 13

1.1 什么是安全测试 13

1.2 什么是Web应用 17

1.3 Web应用基础 21

1.4 Web应用安全测试 25

1.5 方法才是重点 26

第2章 安装免费工具 29

2.1 安装Firefox 29

2.2 安装Firefox扩展 30

2.3 安装Firebug 31

2.4 安装OWASP的WebScarab 32

2.5 在Windows上安装Perl及其软件包 33

2.6 在Linux, Unix或OS X上安装Perl和使用CPAN 34

2.7 安装CAL9000 35

2.8 安装ViewState Decoder 36

2.9 安装cURL 36

2.10 安装Pornzilla 37

2.11 安装Cygwin 38

2.12 安装Nikto 2 39

2.13 安装Burp Suite 40

2.14 安装Apache HTTP Server 41

第3章 基本观察 43

3.1 查看网页的HTML源代码 44

3.2 查看源代码, 高级功能 45

3.3 使用Firebug观察实时的请求头 48

3.4 使用WebScarab观察实时的POST数据 52

3.5 查看隐藏表单域 55

3.6 使用TamperData观察实时的响应头 56

3.7 高亮显示JavaScript和注释 59

3.8 检测JavaScript事件 60

3.9 修改特定的元素属性 61

3.10 动态跟踪元素属性 63

3.11 结论 65

第4章 面向Web的数据编码 66

4.1 辨别二进制数据表示 67

4.2 使用Base-64 69

4.3 在网页中转换Base-36数字	71
4.4 在Perl中使用Base-36	71
4.5 使用以URL方式编码的数据	72
4.6 使用HTML实体数据	74
4.7 计算散列值	76
4.8 辨别时间格式	78
4.9 以编程方式对时间值进行编码	80
4.10 解码ASP.NET的视图状态	81
4.11 解码多重编码	83
第5章 篡改输入	85
5.1 截获和修改POST请求	86
5.2 绕过输入限制	89
5.3 篡改URL	90
5.4 自动篡改URL	93
5.5 测试对URL长度的处理	94
5.6 编辑Cookie	96
5.7 伪造浏览器头信息	99
5.8 上传带有恶意文件名的文件	101
5.9 上传大文件	104
5.10 上传恶意XML实体文件	105
5.11 上传恶意XML结构	107
5.12 上传恶意ZIP文件	109
5.13 上传样例病毒文件	110
5.14 绕过用户界面的限制	111
第6章 自动化批量扫描	114
6.1 使用WebScarab爬行网站	115
6.2 将爬行结果转换为清单	117
6.3 减少要测试的URL	120
6.4 使用电子表格程序来精简列表	120
6.5 使用LWP对网站做镜像	121
6.6 使用wget对网站做镜像	123
6.7 使用wget对特定的清单做镜像	124
6.8 使用Nikto扫描网站	125
6.9 理解Nikto的输出结果	127
6.10 使用Nikto扫描HTTPS站点	128
6.11 使用带身份验证的Nikto	129
6.12 在特定起始点启动Nikto	130
6.13 在Nikto中使用特定的会话Cookie	131
6.14 使用WSFuzzer测试Web服务	132
6.15 理解WSFuzzer的输出结果	134
第7章 使用cURL实现特定任务的自动化	137
7.1 使用cURL获取页面	138
7.2 获取URL的许多变体	139
7.3 自动跟踪重定向	140
7.4 使用cURL检查跨站式脚本	141
7.5 使用cURL检查目录遍历	144
7.6 冒充特定类型的网页浏览器或设备	147
7.7 以交互方式冒充另一种设备	149
7.8 使用cURL模仿搜索引擎	151
7.9 通过假造Referer头信息来伪造工作流程	152
7.10 仅获取HTTP头	153
7.11 使用cURL发送POST请求	154
7.12 保持会话状态	156
7.13 操纵Cookie	157

7.14 使用cURL上传文件	158
7.15 建立多级测试用例	159
7.16 结论	164
第8章 使用LibWWWPerl实现自动化	166
8.1 编写简单的Perl脚本来获取页面	167
8.2 以编程方式更改参数	169
8.3 使用POST模仿表单输入	170
8.4 捕获和保存Cookie	172
8.5 检查会话过期	173
8.6 测试会话固定	175
8.7 发送恶意Cookie值	177
8.8 上传恶意文件内容	179
8.9 上传带有恶意名称的文件	181
8.10 上传病毒到应用	182
8.11 使用Perl解析接收到的值	184
8.12 以编程方式来编辑页面	186
8.13 使用线程化提高性能	189
第9章 查找设计缺陷	191
9.1 绕过必需的导航	192
9.2 尝试特权操作	194
9.3 滥用密码恢复	195
9.4 滥用可预测的标识符	197
9.5 预测凭证	199
9.6 找出应用中的随机数	200
9.7 测试随机数	202
9.8 滥用可重复性	204
9.9 滥用高负载操作	206
9.10 滥用限制性的功能	208
9.11 滥用竞争条件	209
第10章 攻击AJAX	211
10.1 观察实时的AJAX请求	213
10.2 识别应用中的JavaScript	214
10.3 从AJAX活动回溯到源代码	215
10.4 截获和修改AJAX请求	216
10.5 截获和修改服务器响应	218
10.6 使用注入数据破坏AJAX	220
10.7 使用注入XML破坏AJAX	222
10.8 使用注入JSON破坏AJAX	223
10.9 破坏客户端状态	224
10.10 检查跨域访问	226
10.11 通过JSON劫持来读取私有数据	227
第11章 操纵会话	229
11.1 在Cookie中查找会话标识符	230
11.2 在请求中查找会话标识符	232
11.3 查找Authentication头	233
11.4 分析会话ID过期	235
11.5 使用Burp分析会话标识符	239
11.6 使用WebScarab分析会话随机性	240
11.7 更改会话以逃避限制	245
11.8 假扮其他用户	247
11.9 固定会话	248
11.10 测试跨站请求伪造	249
第12章 多层面的测试	251
12.1 使用XSS窃取Cookie	251

- 12.2 使用XSS创建覆盖 253
- 12.3 使用XSS产生HTTP请求 255
- 12.4 以交互方式尝试基于DOM的XSS 256
- 12.5 绕过字段长度限制 (XSS) 258
- 12.6 以交互方式尝试跨站式跟踪 259
- 12.7 修改Host头 261
- 12.8 暴力猜测用户名和密码 263
- 12.9 以交互方式尝试PHP包含文件注入 265
- 12.10 制作解压缩炸弹 266
- 12.11 以交互方式尝试命令注入 268
- 12.12 系统地尝试命令注入 270
- 12.13 以交互方式尝试XPath注入 273
- 12.14 以交互方式尝试服务器端包含 (SSI) 注入 275
- 12.15 系统地尝试服务器端包含 (SSI) 注入 276
- 12.16 以交互方式尝试LDAP注入 278
- 12.17 以交互方式尝试日志注入 280
- • • • • (收起)

[Web安全测试](#) [下载链接1](#)

## 标签

Web安全测试

安全

测试

Web

计算机

web开发

黑客

security

## 评论

还不错。

完全以实用为导向，面向测试而非开发人员的一本小册子，可以当成步骤详细的Check List用

: TP393.408/1286

内容挺充实的，这题材的书不多，缺点就是翻译不够专业

learn something new

基本技巧

杀过去，买本拿回来看看，让那帮土鳖装x，搞死他们！

非常推荐，上面虽然是用perl语言，但是，看上去也是不错的，如果你想做些坏事，那就继续这样的测试吧！

There are two ways of constructing a software design: One way is to make it so simple that there are obviously no deficiencies, and the other way is to make it so complicated that there are no obvious deficiencies. The first method is far more difficult

比较基础的web安全测试，看了部分，被做测试的MM借去了

比较实用的测试手册，适合上手

讲的太浅了，适合做入门手册

这本书的思路蛮新颖的，他不在注重单一的漏洞成因和利用方法，而开始肢解操作，把视角回归到每一次握手，这种视角是一种真正的、带有实战经验的测试过程，这本书对这种视角的阐述让我异常深刻，与传统的安全类图书迥然相异。

刚开始看起来，还挺初级的，坚持往后翻，有很多不错的工具介绍和案例说明，耳目一新。从补足知识面的角度，推荐一看。

关于各种工具的使用. 很基础. #代码大多都是Perl

这方面的书真的很少，没有什么选择。而且这个领域觉得又是实践性很强的领域，光看书是不够的。本书可以作为入门，了解一下web安全测试。

本书主要从测试的角度Web方方面面安全漏洞的检测，书中有很大一部分是各种工具的使用，没有太多深入原理与防御。Web安全深似海啊，有时间再把手边的《白帽子》看了~

高手们可以直接无视了，我这水平的看了都没啥惊喜。

各种工具介绍，理论很少；各种脚本，各种测试点说明

有许多很有用的工具介绍

---

面广而浅，适合基础人士，测试代码全部是丑到爆的perl

---

[Web安全测试 下载链接1](#)

## 书评

这是我看的第一本系统讲解web安全的书籍。

作者是很有经验的业内人士。书中经常因为讲解某个安全测试方法而以自己的工作经历做例子。看过之后你会有对网站安全匪夷所思的感觉。

原来web程序有着那么多不安全的可能性。

本书讲解层次分明。可操作性强。语言简明。

---

[Web安全测试 下载链接1](#)