

内容简介 ·····

《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

《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

举报

作者简介 ·····

Paco Hope，是Cigital公司的一名技术经理，《Mastering FreeBSD and OpenBSDsecurity》

（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

Internationa！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

Ben Walttler，是Cigital公司的一名顾问，Edit Cookies工具的开...

(展开全部)

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

对书籍有兴趣，请购买正版

试读版本下载地址回复可见

链接: <http://pan.baidu.com/s/1nvwXmzB> 密码: i2w8

点击收藏 | 0 关注 | 1

[上一篇: PhpcmsV9从反射型XSS到C...](#) [下一篇: Xss挑战赛公开讨论贴](#)

1. 40 条回复



卧底 2017-08-26 15:38:08

伸手党来了...

0 回复Ta



[yichin](#) 2017-08-28 01:57:03

伸手党+1

0 回复Ta



[channelfive](#) 2017-08-28 02:14:40

0 回复Ta



[溜马仔](#) 2017-08-28 03:53:13

伸手党来了...

0 回复Ta



[ih0cker](#) 2017-08-28 06:42:36

分享是一种美德

0 回复Ta



[only](#) 2017-08-28 06:58:18

建议存为草稿

0 回复Ta



[lele](#) 2017-08-28 08:27:19

伸手党++

0 回复Ta



[lespoir](#) 2017-08-28 12:16:59

感谢楼主分享资源

0 回复Ta



[狐狗](#) 2017-08-28 14:38:14

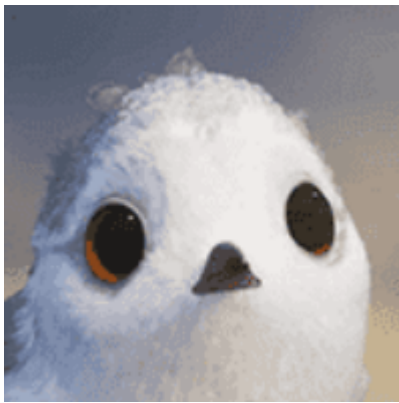
试读。。。。。。。

0 回复Ta



[鲸鱼](#) 2017-08-29 07:46:16

0 回复Ta



[这个名字挺好](#) 2017-08-29 15:54:04

感谢楼主分享资源

0 回复Ta



[leelie](#) 2017-08-30 15:18:40

做一会伸手党

0 回复Ta



[v0yager](#) 2017-08-31 01:20:00

学习学习

0 回复Ta



[chock](#) 2017-08-31 02:43:37

收集一下，收徒就传这本书了

0 回复Ta



[bmz666](#) 2017-08-31 05:31:49

牛逼的书不需要解释。

0 回复Ta



[秦歌](#) 2017-09-05 06:35:20

0 回复Ta



[overm0self](#) 2017-09-05 09:20:23

谢谢楼主分享

0 回复Ta



[我是bey0nd](#) 2017-09-05 10:02:03

试读看看如何

0 回复Ta



[green](#) 2017-09-05 22:52:29

谢谢分享

0 回复Ta



[涨姿势](#) 2017-09-27 09:36:12

分享快乐

0 回复Ta



[哼哼](#) 2017-10-13 06:03:46

收集一下

0 回复Ta



[godot](#) 2017-10-13 12:48:33

感谢

0 回复Ta



[我的滑板鞋](#) 2017-10-16 06:30:02

伸手党+1

0 回复Ta



[天天天蓝](#) 2017-10-16 06:39:06

谢谢分享了，了解一下，辛苦

0 回复Ta



[wolf](#) 2017-10-16 07:46:15

从目录标题看，应该是行外人士所写

0 回复Ta



[drew](#) 2017-10-16 08:11:16

看一下 学习一波

0 回复Ta



[黑风里](#) 2017-10-16 12:25:35

感谢楼主分享资源

0 回复Ta



[mrbean](#) 2017-10-17 01:32:02

学习学习

0 回复Ta



[whoam1](#) 2017-10-17 03:07:48

test

0 回复Ta



[冰封](#) 2017-10-17 14:00:05

试读。。。。。。 学习下 哈哈

0 回复Ta



[huraway](#) 2017-10-19 15:32:04

感谢楼主

0 回复Ta



[三叶草](#) 2017-10-26 08:52:59

感谢分享

0 回复Ta



[annt](#) 2017-10-27 01:29:12

感谢分享

0 回复Ta



[钱亿堆](#) 2017-10-30 09:49:39

伸手 啦

0 回复Ta



[redflog](#) 2017-10-30 11:53:53

感谢分享

0 回复Ta



[小马安全](#) 2017-10-31 03:10:20

学习，谢谢分享

0 回复Ta



[cqu2004](#) 2017-11-01 13:20:54

回复可见？

0 回复Ta



[mrbean](#) 2017-11-13 10:16:45

学习学习

0 回复Ta



[logre](#) 2017-11-13 10:19:09

学无止境~

0 回复Ta



[nm****](#) 2018-11-08 20:06:38

666

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)