

网站安全攻防秘笈



[网站安全攻防秘笈_下载链接1](#)

著者:[美] Ryan C. Barnett

出版者:机械工业出版社

出版时间:2014-10-1

装帧:平装

isbn:9787111478034

本书全方位介绍网站安全防护措施与策略，这些策略用于解决最严重的漏洞及对抗当今网络罪犯使用的攻击方法。无论你是在处理电子商务网站上的拒绝服务攻击，还是对银行系统的造假事件进行应急响应，或者是对新上线的社交网站保护用户数据，翻阅本书

都能找到某种场景下有效的应对方案。本书是作者多年来在政府、教育、商业网站中与大量攻击者的多种攻击对抗中获取的经验总结，内容丰富，实用性强。本书根据网站安全问题的类型将安全策略分为三大部分。第一部分“准备战场”介绍如何打造必将遭受网络攻击的网站平台。当你上线一个新的网站时，应该实施本部分介绍的安全策略。第二部分“非对称战争”介绍如何分析网站的数据，发现恶意行为。第三部分“战略反攻”介绍当发现网站上的恶意行为后如何应对这些攻击，以及怎样高效地使用不同的响应方式来应对攻击。

作者介绍:

Ryan

Barnett，国际著名信息安全专家，有10余年的政府及商业网站防护经验，目前是Trustwave的SpiderLabs团队核心成员，该团队专注于渗透测试、安全事件响应及应用安全的防护。他同时是ModSecurity Web应用防火墙项目的领导者、SANS协会的认证导师以及多个业内大会（如Black Hat、SANS AppSec会议、OWASP AppSecUSA等）的演讲嘉宾。

许鑫城，

腾讯安全平台部应用运维安全工程师，负责腾讯Web业务的漏洞防护等相关工作，研究兴趣包括Web安全、网络安全、Linux后台开发、大数据等。

目录: 目录

译者序

序言

前言

作者简介

第一部分 准备战场

第1章 网站驻防 6

策略1-1: 实时网站请求分析 6

策略1-2: 使用加密的哈希值来避免数据篡改 13

策略1-3: 安装OWASP的ModSecurity核心规则集（CRS） 17

策略1-4: 集成入侵检测系统的特征 29

策略1-5: 使用贝叶斯分析方法检测攻击数据 33

策略1-6: 打开全量HTTP审计日志 42

策略1-7: 只记录有意义的请求 45

策略1-8: 忽略静态资源的请求 46

策略1-9: 在日志中屏蔽敏感数据 47

策略1-10: 使用Syslog把告警发送到中央日志服务器 50

策略1-11: 使用ModSecurity AuditConsole 53

第2章 漏洞检测与修复 57

策略2-1: 被动地识别漏洞 59

策略2-2: 主动地识别漏洞 67

策略2-3: 手动转换漏洞扫描结果 75

策略2-4: 扫描结果自动转换 79

策略2-5: 实时资源评估与虚拟补丁修复 86

第3章 给黑客的陷阱 100

策略3-1: 添加蜜罐端口 101

策略3-2: 添加假的robots.txt的Disallow条目 102

策略3-3: 添加假的HTML注释 107

策略3-4: 添加假的表单隐藏字段 111

策略3-5: 添加假的cookie 114

第二部分 非对称战争

- 第4章 信用度与第三方信息关联 121
 - 策略4-1: 分析用户的地理位置信息 123
 - 策略4-2: 识别使用了代理的可疑客户端 128
 - 策略4-3: 使用实时黑名单查找 (RBL) 131
 - 策略4-4: 运行自己的RBL 137
 - 策略4-5: 检测恶意的链接 140
- 第5章 请求数据分析 148
 - 策略5-1: 访问请求体的内容 148
 - 策略5-2: 识别畸形请求体 154
 - 策略5-3: 规范化Unicode编码 158
 - 策略5-4: 识别是否进行多次编码 161
 - 策略5-5: 识别编码异常 164
 - 策略5-6: 检测异常的请求方法 168
 - 策略5-7: 检测非法的URI数据 172
 - 策略5-8: 检测异常的请求头部 174
 - 策略5-9: 检测多余的参数 183
 - 策略5-10: 检测缺失的参数 185
 - 策略5-11: 检测重复的参数名 187
 - 策略5-12: 检测异常的参数长度 189
 - 策略5-13: 检测异常的参数字符集 193
- 第6章 响应数据分析 196
 - 策略6-1: 检测异常的响应头部 196
 - 策略6-2: 检测响应头部的信息泄漏 206
 - 策略6-3: 访问响应体内容 209
 - 策略6-4: 检测变更的页面标题 211
 - 策略6-5: 检测响应页面大小偏差 214
 - 策略6-6: 检测动态内容变更 216
 - 策略6-7: 检测源代码泄漏 219
 - 策略6-8: 检测技术数据泄漏 223
 - 策略6-9: 检测异常的响应时延 226
 - 策略6-10: 检测是否有敏感用户数据泄漏 228
 - 策略6-11: 检测木马、后门及webshell的访问尝试 231
- 第7章 身份验证防护 234
 - 策略7-1: 检测是否提交了通用的或默认的用户名 235
 - 策略7-2: 检测是否提交了多个用户名 238
 - 策略7-3: 检测失败的身份验证尝试 240
 - 策略7-4: 检测高频率的身份验证尝试 242
 - 策略7-5: 规范化身份验证失败的提示信息 247
 - 策略7-6: 强制提高密码复杂度 250
 - 策略7-7: 把用户名和SessionID进行关联 253
- 第8章 防护会话状态 258
 - 策略8-1: 检测非法的cookie 258
 - 策略8-2: 检测cookie篡改 264
 - 策略8-3: 强制会话过期 268
 - 策略8-4: 检测客户端源位置在会话有效期内是否变更 273
 - 策略8-5: 检测在会话中浏览器标识是否变更 279
- 第9章 防止应用层攻击 288
 - 策略9-1: 阻断非ASCII字符的请求 288
 - 策略9-2: 防止路径遍历攻击 291
 - 策略9-3: 防止暴力浏览攻击 294
 - 策略9-4: 防止SQL注入攻击 296
 - 策略9-5: 防止远程文件包含 (RFI) 攻击 299
 - 策略9-6: 防止OS命令攻击 302
 - 策略9-7: 防止HTTP请求偷渡攻击 305

策略9-8: 防止HTTP响应分割攻击 307
策略9-9: 防止XML攻击 309
第10章 防止客户端攻击 315
策略10-1: 实现内容安全策略 (CSP) 315
策略10-2: 防止跨站脚本 (XSS) 攻击 323
策略10-3: 防止跨站请求伪造 (CSRF) 攻击 331
策略10-4: 防止UI伪装 (点击劫持) 攻击 337
策略10-5: 检测银行木马 (浏览器中的木马) 攻击 340
第11章 文件上传功能防护 345
策略11-1: 检测文件大小 345
策略11-2: 检测是否上传了大量文件 347
策略11-3: 检测文件附件是否有恶意程序 348
第12章 限制访问速率及程序交互流程 352
策略12-1: 检测高速的应用访问速率 352
策略12-2: 检测请求/响应延迟攻击 361
策略12-3: 识别异常的请求间隔时间 367
策略12-4: 识别异常的请求流程 368
策略12-5: 识别显著增加的资源使用 369
第三部分 战略反攻
第13章 被动的响应动作 375
策略13-1: 追踪异常权值 375
策略13-2: 陷阱与追踪审计日志 380
策略13-3: 发送E-mail告警 381
策略13-4: 使用请求头部标记来共享数据 389
第14章 主动的响应动作 394
策略14-1: 跳转到错误页面 394
策略14-2: 断开连接 398
策略14-3: 阻断客户端的源地址 399
策略14-4: 通过变更防护条件 (DefCon) 级别来限制地理位置访问 404
策略14-5: 强制请求延迟 406
策略14-6: 假装被成功攻破 412
策略14-7: 把流量重定向到蜜罐 418
策略14-8: 强制退出网站 420
策略14-9: 临时限制账户访问 425
第15章 侵入式响应动作 428
策略15-1: JavaScript cookie测试 428
策略15-2: 通过验证码测试来确认用户 430
策略15-3: 通过BeEF来hook恶意用户 433
• • • • • [\(收起\)](#)

[网站安全攻防秘笈 下载链接1](#)

标签

安全

计算机

网站

运维

计算机科学

我的书架

Hacker

1

评论

modsecurity配置手册

所有内容都是基于ModSecurity的，不如直接叫ModSecurity Cookbook算了。

在公司吃完饭，锻炼身体前，读一读

[网站安全攻防秘笈 下载链接1](#)

书评

通篇介绍ModSecurity的使用，深度不够。

- 1、对于不太了解网站攻防技术的同学来说，是一本了解工具、属于的书籍。
- 2、对于技术类产品、测试工程师来说可以扩展一下自己的视野。
- 3、书中嵌入的ModSecurity的配置、脚本太多，对于非运维人员可以直接跳过。
- 4、速读，不以精读。

[网站安全攻防秘笈_下载链接1](#)