Web 2.0 Security - Defending AJAX, RIA, AND SOA
Service-Oriented Architecture (SOA), Rich Internet Applications (RIA), and Asynchronous Java and eXtended Markup Language (Ajax) comprise the backbone behind now-widespread Web 2.0 applications, such as MySpace, Google Maps, Flickr, and Live.com. Although these robust tools make next-generation Web applications possible, they also add new security concerns to the field of Web application security. Yamanner-, Sammy-, and Spaceflash-type worms are exploiting client-side Ajax frameworks, providing new avenues of attack, and compromising confidential information. Portals such as Google, Netflix, Yahoo, and MySpace have witnessed new vulnerabilities recently, and these vulnerabilities can be leveraged by attackers to perform phishing, cross-site scripting (XSS), and cross-site request forgery (CSRF) exploitation. Web 2.0 Security: Defending Ajax, RIA, and SOA covers the new field of Web 2.0 security. Written for security professionals and developers, the book explores Web 2.0 hacking methods and helps enhance next-generation security controls for better application security. Readers will gain knowledge in advanced footprinting and discovery techniques; Web 2.0 scanning and vulnerability detection methods; Ajax and Flash hacking methods; SOAP, REST, and XML-RPC hacking; RSS/Atom feed attacks; fuzzing and code review methodologies and tools; and tool building with Python, Ruby, and .NET. Whether you’re a computer security professional, a developer, or an administrator, Web 2.0 Security: Defending Ajax, RIA, and SOA is the only book you will need to prevent new Web 2.0 security threats from harming your network and compromising your data.
Customer Reviews

SECTION 1 - WEB2.0 INTRODUCTION AND SECURITY
Chapter 1 Web 2.0 Apps - Introduction and Components
Chapter objectives
Web 2.0 introduction and security concerns
Web 2.0 application evolution and architecture - SOA, Ajax & RIA
Web 2.0 application information flow
Web 2.0 application - components, technologies & security
Conclusion
References and readings
Chapter 2 Web 2.0 - Languages and Protocols
Chapter objectives
Web 2.0 application layers
Application server side languages
Application client side languages
Transport protocols
Information and data structures
Web 2.0 toolkits and frameworks
Conclusion
References and readings
Chapter 3 Security issues around Web 2.0
Chapter objectives
Web 2.0 attack points
Web 2.0 threats and its impacts
Web 2.0 Vulnerabilities and threat modeling
Web 2.0 analysis frameworks
Web 2.0 security controls
Conclusion
References and readings
Case Study 1 - BlueFlakes: Community portal
Leveraging Web 2.0 and security
SECTION 2 - WEB2.0 APPLICATION PROFILING & VULNERABILITY MAPPING
Chapter 4 Footprinting & Discovering Web 2.0 resources
Chapter objectives
Target (host) identification
Methods of application footprinting
XML services footprinting
Conclusion
References and readings
Chapter 5 Scanning and Vulnerability mapping for Web 2.0 apps
Chapter objectives
Crawling web application
Browsing the application and collecting information - Ajax calls
Identifying potential targets
Data exchange analysis and stream identification
Mapping resource for potential vulnerabilities
Conclusion
References and readings
Case Study 2 - BlueBank: Profiling Banking application
SECTION 3 - WEB2.0 ATTACK VECTORS AND COUNTERMEASURE
Chapter 6 Ajax security
Chapter objectives
Ajax security issues
Ajax streams and information exchange
Ajax and DOM manipulation
Client side security vulnerabilities - XSS & XSRF
with case Ajax end points - server side issues
Countermeasure for Ajax security
Conclusion
References and readings
Chapter 7 Rich internet application security
Chapter objectives
RIA security issues
Flash based application and decoding
Reverse engineering the flash
Cross domain issues
Countermeasure for RIA security
Conclusion
References and readings
Chapter 8 SOA security - XML-RPC, REST & SOAP
Chapter objectives
SOA security issues
Entry points analysis for XML services
XML-RPC attacks
REST application attacks
SOAP based applications and security holes
Ajax interaction with XML services
and security flaws
Countermeasures for XML services
Conclusion
References and readings
Chapter 9 Browser security & Web 2.0 Exploits
Chapter objectives
Browser security overview
Cross domain issues
Client side exploitation and engines
Defending and countermeasures
Conclusion
References and readings
SECTION 4 - WEB 2.0 APPLICATION TESTING AND HARDENING
Chapter 10 Web 2.0 application fuzzing and vulnerability mapping
Chapter objectives
Web 2.0 application fuzzing
Building a tool to fuzz
Fuzzing
web services Fuzzing client side with streams Vulnerability detection with fuzzing Conclusion
References and readings Chapter 11 Secure coding for Web 2.0 applications Chapter objectives
Whitebox approach with code review Building a code review tool Secure coding with Web 2.0
Hardening Web 2.0 holes with code Conclusion References and readings Chapter 12 Hardening
Web 2.0 application with configurations and content filtering Chapter objectives Deployment and
configuration testing Hardening configuration Scanning tool for configuration Content filtering
concept Filtering with Apache Filtering with IIS Browser filtering with javascripts Conclusion
References and readings SECTION 5 - APPENDIX

Shreeraj Shah, B.E., MSCS, MBA, is a co-founder of Blueinfy and SecurityExposure, companies
that provide application security and On Demand Scanning services. Prior to founding Blueinfy, he
was founder and board member at Net Square. He also worked with Foundstone (McAfee), Chase
Manhattan Bank, and IBM in information security. Shreeraj has played an instrumental role in
product development, researching new methodologies, and training designs. He has performed
several security consulting assignments in the area of penetration testing, code reviews, web
application assessments, security architecture reviews, and managing projects (Products/Services).
He is the author of Web 2.0 Security (Cengage Learning, 2007), Hacking Web Services (Thomson
Learning, 2006), and Web Hacking: Attacks and Defense (Addison-Wesley, 2002). In addition, he
has published several advisories, tools, and whitepapers, and has presented at numerous
conferences including RSA, AusCERT, InfosecWorld (Misti), HackInTheBox, Blackhat, OSCON,
Bellua, Syscan, ISACA, and OWASP. His articles are regularly published on Securityfocus,
InformIT, DevX, O’reilly, and HNS. His work has been quoted on BBC, Dark Reading, and Bank
Technology as an expert.

Download to continue reading...

Web 2.0 Security - Defending AJAX, RIA, AND SOA Programming ASP.NET AJAX: Build rich, Web
2.0-style UI with ASP.NET AJAX Home Security: Top 10 Home Security Strategies to Protect Your
House and Family Against Criminals and Break-ins (home security monitor, home security system
diy, secure home network) Gallos de combate: Nacidos para luchar: Genética, mejora y nutrición
de gallos de riñera (Spanish Edition) Defending the Homeland: Domestic Intelligence, Law
Enforcement, and Security (Contemporary Issues in Crime and Justice Series) DNS Security:
Defending the Domain Name System DEFENDING TIERNY (Gray Wolf Security, Texas Book 1)
Retirement Benefits and Planning Your Retirement (social ... disability, social security made simple)
Pro ASP.NET Web API Security: Securing ASP.NET Web API (Expert's Voice in .NET)
Python: Learn Web Scraping with Python In A DAY! - The Ultimate Crash Course to Learning the Basics of Web Scraping with Python In No Time (Web Scraping ... Python Books, Python for Beginners)
Web Development With Javascript And Ajax Illuminated (Jones and Bartlett Illuminated (Paperback))
AJAX, Rich Internet Applications, and Web Development for Programmers
AJAX, Rich Internet Applications, and Web Development for Programmers (Deitel Developer Series)
Web 2.0 Fundamentals: With AJAX, Development Tools, And Mobile Platforms
Microsoft ASP.NET and AJAX: Architecting Web Applications (Developer Reference)
Beginning Web Development, Silverlight, and ASP.NET
AJAX: From Novice to Professional (Expert's Voice in .NET)
AJAX and PHP: Building Modern Web Applications 2nd Edition
Ajax Security
Ajax for Web Application Developers

Dmca