The book was found

Ajax Security
The Hands-On, Practical Guide to Preventing Ajax-Related Security Vulnerabilities

More and more Web sites are being rewritten as Ajax applications; even traditional desktop software is rapidly moving to the Web via Ajax. But, all too often, this transition is being made with reckless disregard for security. If Ajax applications aren’t designed and coded properly, they can be susceptible to far more dangerous security vulnerabilities than conventional Web or desktop software. Ajax developers desperately need guidance on securing their applications: knowledge that’s been virtually impossible to find, until now. Ajax Security systematically debunks today’s most dangerous myths about Ajax security, illustrating key points with detailed case studies of actual exploited Ajax vulnerabilities, ranging from MySpace’s Samy worm to MacWorld’s conference code validator. Even more important, it delivers specific, up-to-the-minute recommendations for securing Ajax applications in each major Web programming language and environment, including .NET, Java, PHP, and even Ruby on Rails. You’ll learn how to:

- Mitigate unique risks associated with Ajax, including overly granular Web services, application control flow tampering, and manipulation of program logic
- Write new Ajax code more safely and identify and fix flaws in existing code
- Prevent emerging Ajax-specific attacks, including JavaScript hijacking and persistent storage theft
- Avoid attacks based on XSS and SQL Injection, including a dangerous SQL Injection variant that can extract an entire backend database with just two requests
- Leverage security built into Ajax frameworks like Prototype, Dojo, and ASP.NET AJAX Extensions and recognize what you still must implement on your own
- Create more secure “mashup” applications

Ajax Security will be an indispensable resource for developers coding or maintaining Ajax applications; architects and development managers planning or designing new Ajax software, and all software security professionals, from QA specialists to penetration testers.
Ajax Security was the last book I read and reviewed in 2007. However, it was the best book I read all year. The book is absolutely compelling and every security professional and Web developer should read it. It's really as simple as that. I am not a Web developer. I was not very familiar with Ajax (beyond its buzzword status and a vague notion of functionality) when I started reading Ajax Security. I attended the authors' Black Hat 2007 talk and was thoroughly impressed and disturbed by the security implications they presented. I expected Ajax Security to be a good book, but one can never be sure if talented hackers and presenters can transfer their skills to the written word. Ajax Security gets the job done. Despite being a traditional network security guy who prefers inspecting traffic to analyzing JavaScript, I had no problem understanding Ajax Security. The authors do a superb job leading the reader through the issues surrounding modern Web applications. They start by introducing a technology, which is critical for someone like me who doesn't deal with Web development issues. Next they describe how it is broken. They continue with defensive recommendations and summarize their findings in the conclusion. This is a perfect technical writing style that is too often lost on other authors. Ajax Security makes very good use of case studies (both large stories like ch 2 and small ones throughout the text). The book also integrates code, diagrams, and screen shots. The text itself is very clear and the authors keep the reader's attention throughout. Histories for various technologies provide a welcome background, showing readers how we've ended up in our current Web 2.0 predicament.

Download to continue reading...