

Session #S11

Presenter:	Mike Shema
Presentation Title:	Web Application Security: Finding Vulnerabilities in Dynamic Applications
Abstract:	
<p>In 2006 web applications received more attention in terms of publicly reported vulnerabilities. Exploits for those vulnerabilities also increased in sophistication and purpose. Web sites tend to include more technologies that provide dynamic interactions between the browser and the application. This increases their exposure to vulnerabilities in functional and business logic.</p> <p>Web application owners and security auditors must continue to find and reduce vulnerabilities due to input validation and data storage. Yet the growth of client-side functionality placed in JavaScript or browser plug-ins like Flash or ActiveX means that even more care must be taken when reviewing the business logic and program flow of an application. If an exploit is able to take advantage of a web browser's implied trust of the application, then the user's data can be compromised or the web browser can be used to propagate a worm across the application. Both scenarios can have a significant impact on the web site.</p> <p>This presentation will summarize some web application worms and how they combined input validation exploits (e.g. Cross-Site Scripting) with dynamic content in order to exploit the logic of a web application. It will include examples of vulnerabilities that arise from increased reliance on client-side engines. The presentation will also highlight the need to increase the security of desktops and web browsers in order to protect users from a compromised or malicious web application.</p>	
Target Audience:	
<p>Attendees should be familiar with web-related technologies, but detailed understanding of items such as AJAX and DOM is not necessary as these will be explained in the context of threats and vulnerabilities.</p> <p>Attendees who are concerned with web application security will gain more insight into the evolution and sophistication of attacks; those who are concerned with desktop security and data theft will gain an understanding of how malicious web sites can be used to attack users.</p>	
COBIT Objectives:	
<p></p>	
Speaker Bio:	
<p>Mike Shema is the co-author of Hacking Exposed: Web Applications, The Anti-Hacker Toolkit, and the author of Hack Notes: Web Application Security. He has extensive consulting experience with information security within a variety of industries. While his security background ranges across network penetration testing, wireless auditing, code review, and training, he primarily focuses on web application security. He currently works at Qualys, developing tools that automate the web application audit process.</p>	