

Title

Web 2.0 Attacks, Exploits and Countermeasure – Securing Next Generation Applications

Abstract

WEB 2.0 technologies for the Web application layer are still evolving. This framework consists of Web services, AJAX and SOAP/XML and while still evolving has thrown up new attack vectors. To combat the attacks one needs to understand the new methodology, tools and strategies. Steadily emerging as the first line of defense is the Web application firewall. This presentation reveals emerging security threats, some of which will be demonstrated.

Objectives:

- Logical evolution of Web applications has reached a new level with the introduction of WEB 2.0. WEB 2.0 is the combination of new technologies like Web services, AJAX and SOAP. It is important to understand this framework and the fundamentals, before looking at security threats.
- Imparting new Web application footprinting methodology by leveraging search engines like MSN and Google. Search engines are emerging as major information sources with Web services APIs.
- Comprehending XML-based attack vectors – LDAP/SQL injections, SOAP messaging attacks, AJAX and Web profiling. These shall be covered along with demonstration examples.
- Web services are the backbone of WEB 2.0 and it is important to understand security threats.
- Building a Web application firewall and implementing strategies to defend WEB 2.0 based applications.

Bio

Shreeraj Shah (Founder and Director) - Shreeraj Shah, B.E., MSCS, MBA, is the founder of Blueinfy, a company that provides application security 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 security space. He is also the author of popular books like Web 2.0 Security, Hacking Web Services (Thomson 06) and Web Hacking: Attacks and Defense (Addison-Wesley 03). 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 etc. His articles are regularly published on Securityfocus, InformIT, DevX, O'reilly, HNS. His work has been quoted on BBC, Dark Reading, Bank Technology as an expert.