Analyzing and Securing Enterprise Application Code by Blueinfy (Shreeraj Shah & Vimal Patel)

Overview:

Enterprise application source code, independent of languages and platforms, is a major source of vulnerabilities. The class is designed and developed to focus on enterprise architecture and application analytics to discover vulnerabilities. One of the CSI surveys on vulnerability distribution suggests that in 64% of cases, a vulnerability crops up due to programming errors and in 36% of cases, due to configuration issues. We will be covering analysis techniques, with tools, for assessment and review of enterprise application source code. Enterprise 2.0 and mashups, along with other different Web 2.0 concepts, reinforced by hands-on experience, will help in understanding next generation application requirements.

It is imperative to know source code review methodologies and strategies for analysis. The emphasis of the class would be to develop a complete understanding of source code analysis, audit methodologies, techniques and tools. Knowledge gained would help in analyzing and securing enterprise applications at all different stages - architecture, design and/or development. The course is designed by the author of "Web Hacking: Attacks and Defenses", “Hacking Web Services” and “Web 2.0 Security – Defending Ajax, RIA and SOA”, bringing his experience in application security and research to the curriculum. Special focus is given to compliance and Top-25 errors for enterprise applications.

This class is hands-on and needs laptops to implement its numerous exercises designed to run hand-in-hand with their concepts. The class features real life cases, hands-on exercises, code scanning tools and defense plans. Participants would be methodically taken down to the source code level and exposed to the possible flaws in architecture, design and coding practices. The class would then focus on the proper ways of writing secure code and analyzing the code base.

Course pre-requisite

- Basic knowledge on Enterprise Application Architecture and Design.
- Understanding of one of the languages from Java, C# (.NET) or PHP.
- Familiarity with application scanning tools and approaches would be handy.
- Script writing ability using perl, ruby or python would help in coding quick tools (Not a must)
- It is also recommended for someone who is new to the application security space and is looking for quick lessons in source code audit and testing.

Who Should Attend the Class

- Source code analyzers, auditors (PCI-DSS), consultants, pen-testers and security professionals who are looking to upgrade their skill-set on enterprise application security and source code analysis.
- QA and Developers who are looking for new tools and methodologies.
- Program managers and team leaders, responsible for securing SDLC in their enterprise environment.

Learning Objectives:

- Application Source Code Assessment and Audit Methodologies
- Detecting OWASP Top 10 and CWE Top 25 Errors and vulnerabilities?
- Enhancing your ability to understand Enterprise Application Framework and Structures
- Dealing with different protocols and structures in enterprise environment for vulnerability assessment.
- Enterprise Architecture overview, .NET and J2EE application frameworks and security, Application layers and components, Resources and interactions, Enterprise RPC and API calls.
- Detecting the state of source code for attack vectors like SQL injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), Path traversal, Session hijacking, LDAP/XPATH/Command injection, Buffer overflow, Input validation bypassing, Database hacks, Ajax exploits, Web Services attack vectors etc.
- Using tools and writing scripts for source code analysis and vulnerability mapping
- Code review methodologies by Spidering the code, enumerating blocks and identifying modules.
- Scanning for vulnerabilities and analysis by Function and Method signature mapping, entry point identification, data access layer calls, tracing variables and functions.
- Source Code Auditing in an enterprise environment for compliance and standards like PCI-DSS.
- Applying validations across an enterprise application by Input validations, Output encoding/validations, Data access layer filtering, Authentication validations etc.
- Decomposing assemblies to discover other security vulnerabilities and structured analysis.
- Key security aspects and Domains for enterprise security like Authentication, Authorization, Session management, Crypto usage and Error handling.
- Defense plans and strategies, Secure objects, functions and wrappers
- Detecting vulnerabilities in advanced technologies like Ajax, Rich Internet Applications (RIA) and SOA
- XML and Web Services security for SOAP, XML-RPC and REST base attacks and secure coding.
- Client side coding and security for Ajax and JavaScript analysis, Flash based application reviews and Browser security.

- Understanding of various tools and frameworks with hands-on experience.

What to bring

To participate in hands-on exercises you will need to come with a windows-based laptop.

- OS : XP, Vista or Server family
- Please install .NET framework
- 1 GB RAM
- All other tools will be provided
- Laptop should be wi-fi enabled

Hands-on:

All concepts taught in this class are punctuated with hands-on exercises based on situations observed in real life. The class ends with a challenge exercise. Working within a limited time period, participants are expected to analyze the code, identify loopholes, exploit vulnerabilities present in the applications and suggest appropriate defense strategies.

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 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.

Vimal Patel (Founder and Director)

Vimal Patel is founder of Blueinfy, a company that provides products and services for application security. Vimal leads research and product development efforts at Blueinfy. Prior to founding Blueinfy, he held position of Vice President at Citigroup where he led architecture, design and development of various financial applications. Vimal holds Masters in Computer Science. Vimal has over a decade of experience and expertise in many technologies. His experience ranges from design of complex digital circuits and microcontroller based products to enterprise applications.