



Whitepaper: 10 Easy Steps to Application Security

Glenn Roberts, CISSP
January 2010

866.333.2133
www.solutionary.com

10 Easy Steps to Application Security

Application development is an ever-evolving experience. Staying on top of the new languages is only the first step. While the end goal may be making sure that the application meets the business need, part of that goal must also be ensuring that it meets the business need in a secure manner. Ultimately, the REAL end goal is guaranteeing that fully functional applications are secure before hitting production. If one is unsure about the security implications of a new application, or where to begin in building a competent application security program; contacting a comprehensive Application Security firm is always a good way to start. There are many things one can do to improve the chances of deploying a safe and secure application before writing even a single line of code.

1. Know your mission -- what task is the software supposed to complete? This should include genuine requirements and quality specifications based on those real requirements. Make sure that all development staff (business analysts, designers, db architects, developers, testers, and tech writers) have use-case and other real-world information to help ensure that they understand how the application and data will be used. Knowing your mission will minimize complexity and save time and effort when it comes to the actual coding.

2. Know your data -- understand the nature of your data. Understand the threat and/or potential threat to that data based on real world issues. What products your business produces and in which shapes or sizes, for example, is data that's not as sensitive as personal credit card information. What type and level of encryption is an appropriate data protection mechanism? What level of data validation and integrity checking is required by the data being used? Make sure all development staff understands the quality, quantity, and sensitivity of data; this will insure that adequate security controls are planned ahead of time.

3. Establish a technical knowledge base -- this includes training for operating system, database, programming languages, and for source control. Make sure you have people knowledgeable about the technology you are using to implement the application. You are not going to get the optimal solution if everyone on the project is learning the language as they go. In addition, a technical knowledge base is useful to have if any technological obstacles are encountered along the way.

4. Establish a security knowledge base -- During operations, 85% of security may purely be a product of common sense. In development, security is more about training and experience. Perform specific security training on secure coding techniques, be aware of vulnerabilities in the database, operating system, and code set being used; know how to avoid known issues, data validation, and error handling. Actively track vulnerabilities applicable to your application environment, and periodically review the code set and environment configuration details in context of new and/or developing threats. A security knowledge base will keep you up to date in secure coding practices.



5. Implement effective source control/configuration management -- define and understand how you are controlling source code before you code, not as you code. Put everything into source control, software, operating system configurations, database settings, static data, and developer and user documentation. Effective source control can help you build stronger code, in addition to actually speeding up development.

6. Implement a functional coding "toolkit" -- Consider building a toolkit of modularized code that can be inserted into any application meeting specific requirements. Modularized coding tool kits make application development faster and less prone to human errors. The Open Web Application Security Project (OWASP) provides a number of Enterprise Security API (ESAPI) toolkits that can be used free of charge: (<http://www.owasp.org/index.php/ESAPI>). Coding tool kits may seem cumbersome at first, but become invaluable once an application reaches maturity, or once the development team becomes accustomed to using them.

7. Implement a formal Server hardening program -- The National Institute of Standards and Technology (NIST), OWASP and industry Server Vendors have specific hardening recommendations. Ensure that all web servers are reviewed for good practice security measures. Document operating systems patch installations as well as virus signature updates. All the application-specific security available will not help you if your application is installed on an insecure platform.

8. Implement formal source code reviews -- Third party source code reviews should be a part of the application software development lifecycle (SDLC). Each time a new module is introduced or a current code is changed, a competent code review should be performed. A comprehensive second review can be invaluable in catching functionality issues, security vulnerabilities, as well as attack vectors to be used in the future.

9. Implement targeted vulnerability assessments -- Third party vulnerability assessments are one of the few ways to thoroughly test your application. Performing a targeted assessment while the application is in development will find attack vectors before they are introduced into production code. Additionally, application assessment vendors can help with remediation support and validation if needed.

10. Implement appropriate safeguards -- Researching and implementing application safeguards ahead of production releases can save time and money. Application Firewalls, Application Logging, Server Logging and Intrusion Prevention Devices are all useful safeguards to consider but each device is limited in use. Application Firewalls, for example, are great for point to point security, however if used for applications which have multiple security zones (ssl vs non-ssl), the margin for error increases. Consider all of the available safeguards, their limitations and price structures; then implement the appropriate safeguards ensuring they are configured and hardened according to the manufacturer's recommendations.

Overall, application security requires planning, dedication, and the conscious effort to make sure that you know exactly what you are doing. Some formal effort can go a long way towards building stronger applications; thereby helping you better protect your data as well as that of your customers. Remember, if you follow the suggestions presented, the vast majority of application attack vectors can be stopped before the application is ever placed into production.



About the Author

Glenn Roberts is a senior security consultant for Solutionary, Inc. Glenn, a Certified Information Systems Security Professional (CISSP), is a subject matter experts for application security.

Glenn joined Solutionary in 2007 as a technical security consultant. He has developed Solutionary's wireless, application, and social engineering testing methodologies. Glenn is an active member in the Open Web Application Security Project and is in charge of assessing international financial applications for Solutionary's Fortune 500 clientele.

Glenn has over eight years of experience in information technology, with five years dedicated to information security. His experience includes security reviews, mitigation, strategy, architecture, planning, design, and implementation. He has consulted clients on a broad range of information security projects including security assessments, incident response and full scale implementation of security architectures.

Prior to joining Solutionary, Glenn worked as a senior security consultant for Unisys Corporation, an IT manager for Kaiser Permanente Medical Group and a senior network administrator for Kaiser Foundation Health Plan.

About Solutionary

Solutionary is an information security company that delivers a wide range of managed security solutions and professional services to reduce risk, increase security and ensure compliance for medium-to-large businesses.

The company's services are based on next generation security intelligence and offer true security and compliance management. Solutionary provides customers with advanced service delivery, patented technology, thought leadership, years of innovative groundwork and proprietary certifications that exceed industry standards, enabling the company to have one of the highest client retention rates in the industry.

Solutionary is positioned by Gartner as a "visionary" in the MSSP Magic Quadrant, and Forrester as a "strong performer" in the MSSP Wave. The company maintains 24/7, fully redundant security operations centers (SOCs) in Pittsburgh and Omaha where it is headquartered.

