



# DENIM GROUP



## APPLICATION SECURITY JUMPSTART

### ... For the Information Security Auditor

If you are an information systems auditor and find yourself in charge of an effort to audit custom web applications, you likely are experiencing the uncomfortable feeling that you have inherited a huge risk, have little time to learn the technical details of web applications, and are presented with a dizzying array of potential issues to handle.

In addition, you are more than likely not a developer, so there is a significant amount of time you are going to have to invest in understanding the operations of your internal development team. And, like most other potential risk areas, you are in a race with time to put in place a program that mitigates corporate risk

This document is designed to provide you resources and first steps that will help you learn fundamentals of web application security in a rapid manner. It provides a list of resources to visit that will enable you to lower your learning curve and understand where to focus your initial energies. The resources include:

- **Visit the Web Application Security Project (OWASP) Website**

The first place to visit is a vendor-neutral clearing house for all issues relating to securing custom applications. The OWASP's "Ten Most Critical Web Application Security Vulnerabilities" has become the de facto standard list of top application threats and should serve as a starting point for analyzing internally-developed applications. Perhaps more importantly, though, OWASP's assessment guide provides a template for conducting an application security review. More information can be found at their website:

[www.owasp.org](http://www.owasp.org)

- **Review the ISC2 resources**

Although you may be a CISA, you, you might consider looking at the Common Bodies of Knowledge (CBK) addressing the topic of application security. This topic, officially titled "Application Development Security" is another reference point from which to begin building your application security program. The many CISSP tutorials and study guides provide an outline of the major topic areas and should provide you a gist of the application security areas to address. More information can be found on the ISC2 website at [www.isc2.org](http://www.isc2.org).

- **Subscribe to an Application Security Mailing List**

Two e-mail lists that have technical and business issues associated with application security are hosted by the OWASP and Securityfocus.com. You can subscribe to the OWASP mail list by signing up at:

<http://www.owasp.org/documentation/guide>

In addition, you can subscribe to the Securityfocus.com Secure Programming mailing lists at:

<http://www.securityfocus.com/archive>

- **Read a book!**

In addition to the large amount of online resources that exist, you might want to consider reading the following:

***"Secure Coding: Principles and Practices"*** – A great overview from O'Reilly and Associates for the security generalist.

***"Hacking Web Applications" Exposed"*** - From the venerable "Hacking Exposed" series of books from Joel Scambray and Stuart McClure. This book provides hands on instruction on how to begin the assessment process for securing corporate custom applications.

***"Building Secure Software"*** – by John Viega and Gary McGraw. Another great book that provides secure application development methodology for corporations.

- **Establish Rapport with Your Development Manager**

As simple as this might sound, a good first step is to meet with the person responsible for building applications within your organization. If you outsource some or all of this process, then find the project manager responsible within your IT organization who manages the software production projects. There will likely be significant education that you might have to provide, but your organization will be better served if the application development manager is on board with the concept of securing custom applications.

- **Begin to understand the development requirements process**

Followed closely after your meeting with the application development manager, you should carve out time to better understand the software development process within your organization. The key point here is to understand where application security assessments might be injected into the production process. In the long-term, in order to effectively produce applications without vulnerabilities you will have to add security as a business unit requirement that the development team includes.

- **Begin the process to inventory internally-developed applications**

Before you begin engaging vendors or acquire tools, a simple inventory of what applications have been built internally is another great starting point. As part of this process, consider ranking the applications according to criticality so you can prioritize which applications to perform security assessments against first.

Finally, if you have any questions or would like to know more about how your organization can benefit from a comprehensive strategy to secure your custom software, contact Denim Group at (210) 572-4400 or at [info@denimgroup.com](mailto:info@denimgroup.com).