Introduction

Welcome to the OWASP Guide 2.0!

The Guide has been re-written from the ground up, dealing with all forms of web application security issues, from old hoary chestnuts like SQL injection, through modern concerns such as phishing, credit card handling, session fixation, cross-site request forgeries, and compliance and privacy issues.

In Guide 2.0, you will find details on securing most forms of web applications and services, with practical guidance using J2EE, ASP.NET, and PHP samples. We now use the highly successful OWASP Top 10 style, but with more depth, and references to take you further.

Security is not a black and white field; it is many shades of grey. In the past, many organizations wished to buy a simple silver security bullet – “do it this way or follow this check list to the letter, and you’ll be safe.” The black and white mindset is invariably wrong, costly, and ineffective.

The Guide strongly recommends the use of threat risk modeling as a way to reduce development costs and time, and eliminate wasted resources. Instead, with careful selection of controls via threat risk modeling, only those controls that demonstrably reduce the risk are implemented. These controls are usually cheap, effective, and simple to implement.

In some countries, risk-based development is not an optional extra, but legally mandated. For example, a core control required by Sarbanes Oxley is to prove that adequate controls are in place for financial systems, and that senior management believes the controls are effective. The Guide provides keys into COBIT (the most commonly used control framework for SOX) to assist organizations produce applications that meet SOX requirements.

As with any long-lived project, there is a need to keep the material fresh and relevant. Therefore, some of the material from the older Guides has been migrated to OWASP’s portal or outright replaced with new advice.

Thanks to the many authors and editors for their hard work in bringing this guide to where it is today. If you have any comments or suggestions on the Guide, please e-mail the Guide mail list (see our web site for details) or contact me directly.

Andrew van der Stock, [vanderaj@owasp.org](mailto:vanderaj@owasp.org)  
Melbourne, Australia  
July 24, 2005