

# Mapping the Application Security Terrain

## Choosing an Appropriate Application Security Assessment Process



© Copyright 2007 Pixoi Ltd. All Rights Reserved.

**Carl Schwarcz**

**Director of Application Security**

Carl.Schwarcz@AsTechConsulting.com

---

AsTech Consulting, Inc.  
601 Montgomery, Suite 688  
San Francisco, CA 94111

Telephone: 415.291.9911

Toll Free: 888.777.5995

Facsimile: 415.291.9922

[www.atechconsulting.com](http://www.atechconsulting.com)

## Summary

Network perimeter security has become more and more effective as products and services have matured. Internet applications are now the target of choice for criminals to obtain restricted information and unwarranted access to companies' protected assets. The number and type of protection measures for these applications is growing. The selection of an appropriate application security risk management solution should take into account the business's diverse requirements and factors. There is no single solution that will fit every company's needs.

Those responsible for the security of their environments need to understand what risks are present in their applications, as each vulnerability has an associated criticality that is based on various factors. Armed with this knowledge, an appropriate risk management strategy can be developed with prioritized action to reduce these threats.

AsTech Consulting has over 7 years of experience assessing internet applications using manual and automated methods for both 'white box' and 'black box' assessments. We have developed a range of service levels utilizing these methods to match our customers' business needs and security requirements.

## What is the required level of application security assessment?

As enterprise application security requirements are considered, it is useful to put them in the same context as various other software attributes that we usually deal with:

- Functionality
- Usability
- Performance
- Reliability
- Security**

For each attribute, more is inherently desirable for the application and the business. If the application is easier to use, faster, more reliable and more secure the application is better and the business offering should be more competitive.

However, we can't deal with the characteristics of our applications in isolation; we consider them in the context of business requirements and real world business factors including feasibility, funding, return on investment, and opportunity cost.

While better is always desirable, we can't evaluate what is better without understanding the status quo. We need to answer the "better than what?" question. This requires sufficient analysis/assessment to identify a comparative baseline.

- A company's web-facing newsletter sign-up page is found to have a cross-site scripting vulnerability. Addressing this risk may require \$20,000 in development costs. Is this the best use of funds for this company?

In theoretical terms we want absolute safety. In practical terms we want a "reasonable or better" level of security. The definition of "reasonable" is only meaningful within the context of a specific application and business. The definition may be based upon government (e.g. DOD levels of classification), industry group requirements (Payment Card Industry), and business domain requirements (the video game in contrast to the aircraft supplier).

The very act of measuring security, performance, or reliability has an associated variable cost based upon the precision and thoroughness of the analysis, the skills of the analysts, etc.

An application security assessment process is the method of identifying application security vulnerabilities so that the business can make informed risk management decisions that include the evaluation of the financial and opportunity costs associated with mitigating the identified security risks. The thoroughness, depth, and cost of an application security assessment process should reasonably vary with business requirements.

### What types of security risks might be considered?

A useful starting reference point is the vulnerability taxonomy maintained by OWASP, the Open Web Application Security Project<sup>1</sup>. There, one can find hundreds of articles defining common application security flaws. OWASP also maintains a TOP 10 list of the most critical web application vulnerabilities. While the Top 10 list is a very useful document to increase security awareness, like most lists of this sort, it is neither intended to be comprehensive nor a sufficient definition of application security. AsTech maintains a more wide-ranging catalog of vulnerability classes which we have developed over the past 10 years.

<sup>1</sup> <http://www.owasp.org>



**If Microsoft's Flight Simulator crashes occasionally, Microsoft's business risk could be considered negligible. If the software driving Boeing's avionics system were to crash similarly, it could be catastrophic.**

## What Application security assessment methodologies are available?

There are a number of approaches to assessing application security involving varying combinations of automated and manual analysis from an external (black box) and internal (white box) perspective.

### External Web Application Scanning

Application scanning involves interacting with a running application (essentially using and attacking the application) as a black box to identify points of vulnerability.

While the best of breed commercial automated scanning tools can produce some valuable results, they still can't yet approach the quality and breadth of results that can be identified by a highly skilled ethical hacker.

The strength of application scanning is that because the application is actually attacked, the resulting proof of vulnerability is usually quite concrete and compelling. For example, the results of a successful SQL injection attack might include data or metadata accessed without authorization. If you can see another user's account data or display the structure of the database, it is hard to argue with existence of the vulnerability.

The weakness of application scanning is that it identifies only a limited range of vulnerabilities and requires a highly skilled practitioner. Since the application user interface is the attack vector, the approach is ill-suited to examining business component, back-end, or external service vulnerabilities. For example, if sensitive data such as social security numbers are not being encrypted, or third-party services operate without proper protection, or critical security events such as failed logins are not being adequately logged, these vulnerabilities are likely to go undetected.

### Automated Static Analysis

Static analysis involves the review of the application code for vulnerabilities. For most tools, this usually refers to the source code but less frequently refers to the binary code. This would be considered a 'white box' assessment, as nothing is hidden from the analyst. The application code is a much larger and richer analysis target than the user interface addressed by external, or 'black box' application scanning, and therefore a broader range of vulnerabilities can be identified.

The best of breed static analysis tools utilize sophisticated compiler technologies such as data flow analysis, control flow analysis, and pattern recognition to identify security vulnerabilities. The results of automated analysis generally include a high degree of false positives, requiring a highly skilled security engineer to analyze the results with the source code in hand to distinguish between the truly and the falsely reported vulnerabilities.

Static analyzers are best at identifying vulnerabilities that can be represented as identifiable patterns. Examples of these risks include:

- a missing entry in an xml configuration file
- the use of a dangerous function, including unvalidated user input data in web page output (cross-site scripting vulnerability)
- including unvalidated input data in the construction of a database query (SQL injection)

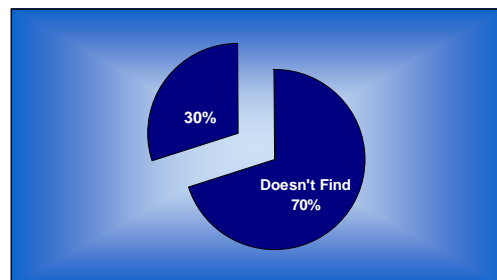
Most static analysis tools can also identify a range of poor programming practices such as the use of uninitialized variables or the lack of error handling.

The main strength of automated static analysis is that the analyzers reliably identify candidate issues (which could turn out to be false positives) and can do so in the face of highly complex application structure and control flow that might daunt most humans. For the software expense and the skilled labor required, the results can be quite cost effective.

The main limitation of these automated tools is that they currently can only find approximately 30% of the types of security vulnerabilities that should be evaluated in a security assessment to provide a comprehensive view of risks present in an application. With the current state of the technology, automated analyzers are generally not capable of testing algorithms, security policy adherence, and issues that may be derived from the application domain. Examples of these areas include:

- authentication
- authorization
- disclosure of confidential data
- audit logging
- cross-site request forgery (XSRF)
- identifying application 'back-doors'

**The limitation of automated static analysis tools is that they currently can only find approximately 30% of the types of security vulnerabilities that should be evaluated in a security assessment.**



## Manual Static Analysis

Manual static analysis involves a review of the application architecture and source code by highly skilled software security engineers. The resulting analysis is comprehensive and is, overall, the most reliable of the approaches. Thus it has been the method of choice where application security is of paramount concern, such as most financial services.

The strength of manual analysis is the level of depth and thoroughness of the assessment. The full range of security vulnerabilities can most readily be identified with high reliability. Specific attributes of the application domain (credit card numbers, account numbers, classified data, etc.) can be taken into account.

The main drawback of manual analysis is that engineers with the necessary skills and experience - both extensive enterprise application development experience coupled with deep security knowledge - are scarce and in high demand. The time required and the level of effort involved makes this approach more costly than other options.

## Vendor Claims

Predictably, vendors of specific technologies or services tend to tout the strengths of their specific approaches and diminish the value of the alternatives. The vendors of automated static analysis tools promote their cost effectiveness and minimize the importance of potentially material coverage gaps, which as we have shown may be significant. Providers of purely manual assessment services tout comprehensive coverage and minimize the impact of cost and schedule.

Of course, there is no 'one size fits all' approach to application security. A sound risk management strategy will make the most appropriate use of any available technology or process.

## AsTech Consulting's Unique Position – The True Consultancy

AsTech Consulting is in a unique position to develop a balanced, objective understanding of application security evaluation approaches. We have a seven year history of performing application security assessments for major financial institutions and other industries. Furthermore, we employ all of these technologies and provide all the described services.

We have developed security assessment service levels based on utilizing each assessment technology where it is most appropriate and providing the greatest return on investment. We tailor our services to meet our client's business needs and financial parameters.

## Application Assessment Service Level Descriptions

There are many different types of applications in use today, encompassing a myriad of functionalities and business purposes. Therefore, there can be no 'one size fits all' approach to risk management when contemplating application security. An internally utilized client-server application that tracks office equipment purchases will not have the same security requirements as those of a publicly accessible banking application.

We have previously described the relative effectiveness of various assessment methodologies at discovering risks. AsTech Consulting has developed the following levels of service to effectively address a range of "white box" risk discovery options. External or "black box" vulnerability assessments can be included in any of these options for an added level of verification.

### 1. Comprehensive Assessment - Automated analysis with complete manual analysis

To obtain the most comprehensive results and thus minimize risk, this service employs automated source code static analysis tools to identify a preliminary set of vulnerabilities, a full manual analysis of the source code for types of vulnerabilities not reliably found through automated tools. This service is most appropriate for commercial applications that have the highest security requirements such as application involving a high volume or high value financial transactions in that it provides the lowest level of residual risk.

### 2. Perimeter Assessment - Automated analysis with attack surface manual analysis

To provide breadth of analysis while lowering cost, this service employs automated source code static analysis tools to identify a preliminary set of vulnerabilities and a manual analysis of the source code focused on those areas of the source that represent the greatest risk for types of vulnerabilities not reliably found through automated tools. Representative areas of focus include the code representing the attack perimeter of the application such as user interfaces and use of external services as well as authentication, authorization, and data protection. Since the manual review is somewhat limited, there is some amount of residual risk.

### 3. Perimeter Audit - Automated analysis with attack surface manual audit

To further reduce cost but still provide some breadth of analysis, this service employs automated source code static analysis tools to identify a preliminary set of vulnerabilities and a manual audit of the source code focused on those areas of the source that represent the risk for types of vulnerabilities not reliably found through automated tools. The auditing process samples a portion of the code which is taken to contain representative examples within the range of vulnerabilities present in the application. Since the manual review is even more limited, there is a greater level of residual risk.

## 4. Automated Assessment - Automated static source analysis

To minimize expense while obtaining some reliable level of security assessment, automated static analysis of the application is performed and validated. This provides a reasonable assessment for some of the most frequent critical vulnerabilities such as SQL injection and cross-site scripting. However it leaves other key areas that not addressed by automated analysis unassessed. The level of residual risk is therefore higher still and thus may not be appropriate for an application that is business critical.

## Summary of Service Offerings – Cost/Risk Identification

	Level of Risk Identification	Relative Cost	Resulting Residual Risk
<b>Comprehensive Assessment</b>	Highest	Higher	Lowest
<b>Perimeter Assessment</b>	Higher	Moderate	Low
<b>Perimeter Audit</b>	High	Low	Moderate
<b>Automated Assessment</b>	Moderate	Lower	Significant

## Conclusions

Every day, more threats and exploits against Internet applications are being discovered. Many applications contain vulnerabilities that haven't been discovered by those responsible for securing their systems, rendering it impossible to implement effective risk management strategies. There are more than a few options available to security personnel which can identify these vulnerabilities, but the decision of which to use in what business environment may be complicated, since all options have pluses and minuses.

AsTech Consulting has been performing application security assessments for top-tier clients since 2001. Our assessment processes combine the skills of some of the industry's best security engineers with the best of class automated analysis tools. We continually modify our processes to take into account the improvements in automated tools, the changes in threats, and industry standards and best practices. Thus we are ideally positioned to assist our clients in choosing the most appropriate application security process based upon each client's risk management and financial objectives.