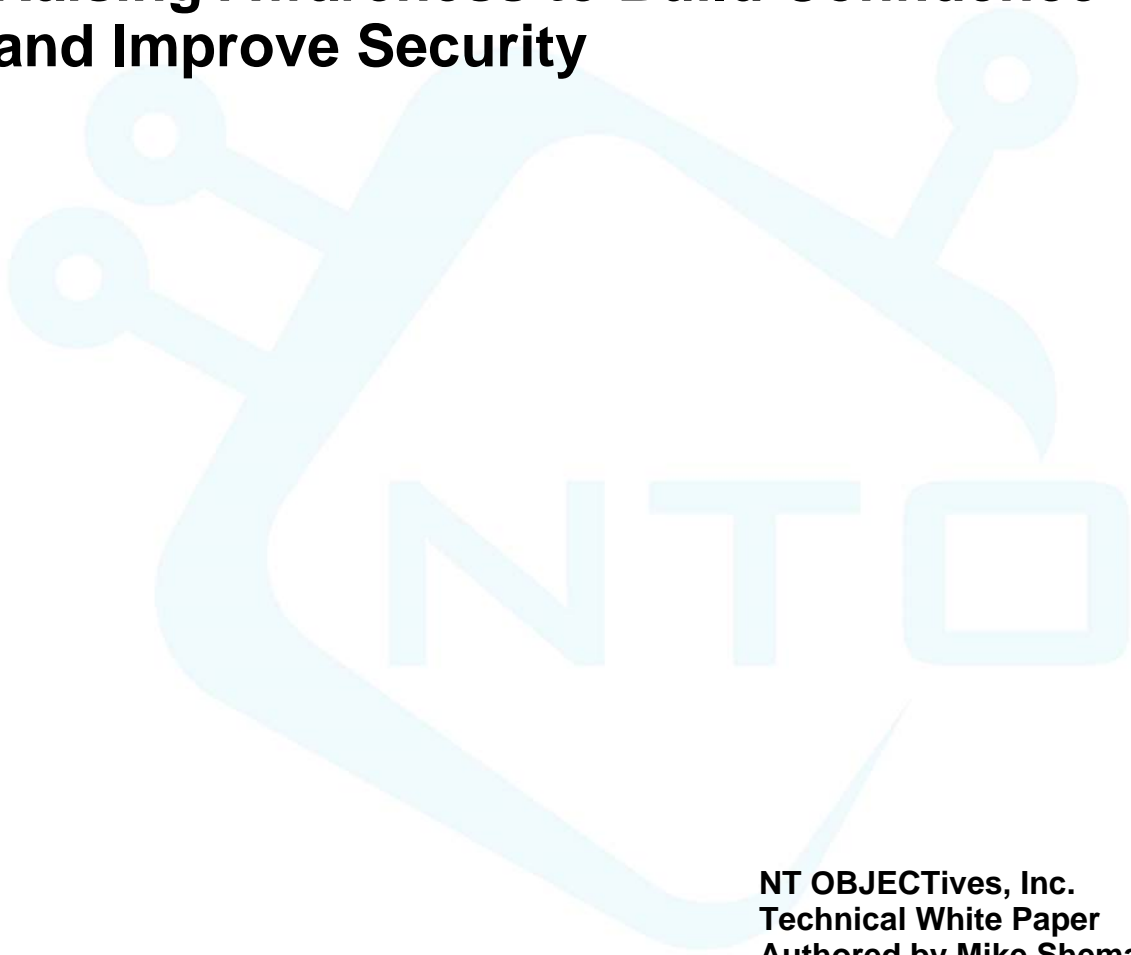


Web Application Exposure to Risk: Raising Awareness to Build Confidence and Improve Security



**NT OBJECTives, Inc.
Technical White Paper
Authored by Mike Shema**

Web Application Exposure to Risk: Raising Awareness to Build Confidence and Improve Security

Web sites face many threats to the confidentiality, integrity, and availability of the data used and the functionality provided by the application. The threats range from malicious users to anonymous attackers, each with varying levels of skill. An insecure web application may expose customers' personal information, financial information, passwords, or lead to fraudulent transactions. For many web applications, the result of identity theft or fraudulent activity impacts has financial and legal impact for the application owner.

Exposure describes the relative probability that a web application *may be vulnerable* due to its **architecture, complexity, data manipulation, and deployment**. These categories are measured from an external perspective as either an anonymous or authenticated user of the application.

The exposure rating is designed to aid decision makers choose where to focus resources when reviewing the security of a web site.

The Relation Between Exposure and the Application

Security personnel and developers can take proactive steps to minimize the impact of a compromise, but must always accept some lower bound that represents the inherent risk of placing a publicly available server on the Internet. The concept of exposure measures this risk and is important for web application owners to understand. It is often easier to quantify the risk associated with a network service, such as remote administration (SSH), file transfer (FTP), or e-mail (SMTP), by considering the firewall rules, updated security patches, and secure configuration techniques applied to the server. Web applications present a more difficult challenge to determine their fundamental exposure to compromise because they provide functionality that most network-level security devices are not designed to protect.

The most commonly known web application attacks are probably *SQL injection*, and *Cross-Site Scripting* (or HTML injection). These attacks use malicious syntax to attack a web application. A successful attack results in unrestricted access to database information or theft of other users' e-mail address or password; these attacks succeed regardless of firewall restrictions or security patches. Other attacks exploit poor session handling, cookies, or passwords and do not rely on syntax errors or payloads that may be targeted by firewalls or intrusion detection systems. Consequently, application owners must place countermeasures within the application in order to successfully defend against these attacks. Whether or not these countermeasures exist, there is always the potential that a web application will be exploited. The most significant factors that impact web site exposure are architecture, complexity, data manipulation and deployment.

- Architecture – The logical and physical architecture of an application affects its security. Multiple services (web, database) must interact securely, must not introduce a single point of failure,

Web Application Exposure to Risk: Raising Awareness to Build Confidence and Improve Security

and must be conducive to the manageability of the application.

- Complexity – As the functionality of an application increases, so does the probability that more bugs exist. Problems can arise from syntax errors when calling functions to logical errors or incorrect assumptions about authorization controls.
- Data Manipulation – The core of the application is its collection and presentation of data. These must be handled properly to meet privacy, financial, and legal regulations or guidelines.
- Deployment – The application and its environment must be secured. A vulnerability in the web server negates security implemented in the application.

A web site's exposure is qualified by mapping common web application attributes to the above categories. These attributes are not inherently insecure, but they represent typical vectors used to attack web applications. The exposure rating highlights where effort should be focused to create countermeasures; it does not imply that certain attributes should be reduced or removed.

- Authentication mechanism – How the application authenticates users, tracks the authentication, and protects access to restricted areas.
- Use of cookies – How the application generates, modifies, and expires cookies. What content the application stores in cookies.
- Use of forms – How many areas exist where the application requests user input.
- Exchange of data with external application – How the application interfaces to services outside the control of the application owners. What information the application sends to third-party services.
- Amount of unique parameters – How many areas exist where the application tracks dynamic information on the client.
- Bad Return Codes – How often the client experiences error-related HTTP response codes from the server (e.g. 404, 500).

It is important to emphasize that the above attributes represent an external view of the application. Regardless of proper input validation routines, an application with a large amount of parameters exposes many points of attack and introduces many chances for error.

Use Exposure To Guide Security of the Application

The exposure rating is an external view of the application and does not consider input validation routines or other internal countermeasures designed to reduce the probability that the site will be successfully compromised. The application owner's goal is not necessarily to reduce the exposure rating by removing application attributes, but to increase the confidence of the countermeasures through secure coding techniques.

Web Application Exposure to Risk: Raising Awareness to Build Confidence and Improve Security

For example, consider a site that has a high exposure rating due to its reliance on a large amount of unique HTML forms (e.g. bulletin board or forum). There is probably a good reason for having so many forms, including editing profiles, viewing posts, replying to posts, creating topics, searching posts, and so on. The application owner should not try to reduce the exposure rating by reducing the total number of unique forms. Although this would have a desirable affect on the exposure rating, it detracts from the usability and power of the application. Instead, the application owner should focus on input validation routines or centralize form manipulation to a single code object. Once that task is complete then resources can be applied to items with a lower exposure or perceived risk.

The exposure rating also helps application owners prioritize multiple web sites. Given a limited amount of resources, an application with a higher exposure rating would receive more attention to secure coding and other countermeasures before lower-rated applications.

Build Confidence in the Security of the Application

Exposure is an external view of the web site, but application owners have access to more information based on internal views of the site. This knowledge builds confidence in the application's resistance to attacks. Confidence is built from several sources, including:

- **Exhaustive Threat Modeling** – A understanding of the methods in which applications are compromised and how those threats can be mitigated. This is often accomplished through training of developers and administrators.
- **Security Audit** – A “black box” security audit of the web application, either performed manually or via automated assessment tools. A good security audit addresses existing threat models and identifies new ones.
- **Secure Coding** – Proactive steps taken to resolve syntax, semantic, and logical errors. This is a broad category that ranges from input validation to separation of code and data.
- **Access and Authorization** – Similar to secure coding, this defines how well the application implements access and granular authorization. The concept of *least privilege* is applied here.
- **Database Schema** – Proactive steps taken to protect the confidentiality and integrity of the database. A good schema and implementation reduces the impact of an application compromise or amount of sensitive data that an attacker can pilfer.

Web Application Exposure to Risk: Raising Awareness to Build Confidence and Improve Security

Exposure cannot be expected to reduce over time because it is correlated with the amount of functionality and size of the application. Consequently, application owners need to increase their confidence in the site's security measures in order to reduce the potential for compromise. Figure 1 demonstrates the relation between the exposure of a web site and the confidence of the application owners in their site's security measures.

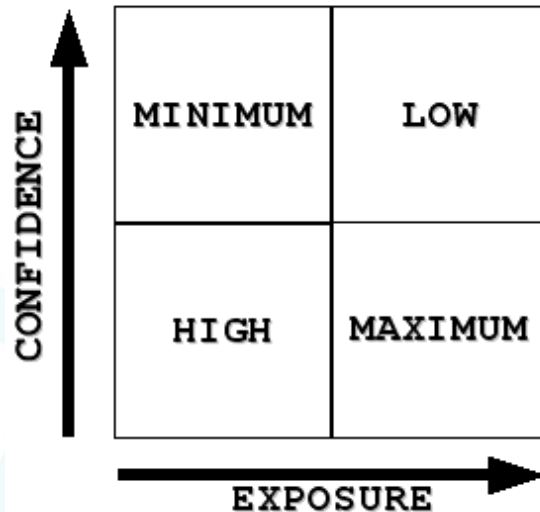


Illustration 1 Potential for compromise based on the relation between exposure and confidence.

Low confidence implies that the application does not have server-side input validation or that a third-party security audit has not been performed. Higher confidence is gained by periodic security reviews, secure coding, and consistent monitoring.

Web Application Exposure to Risk: Raising Awareness to Build Confidence and Improve Security

For additional research, resources and tools, including NTO's freeware exposure assessment tool "ntoinsight", please visit www.ntobjectives.com. **ntoinsight** offers the public a freeware tool to assist in identifying and understanding site security exposure in order to assist in policy development and security mitigation planning.

About NT OBJECTives

NT OBJECTives, based in Orange County, California, brings together an unprecedented collection of this industry's top experts to offer a comprehensive suite of industry leading technology and services to solve the application security concern for today's global business leaders. Through the synergy of the top security software developers and some of the industry's best consultants and researchers, NTO has created the first next-generation, automated technology capable of performing accurate application security audits. Coupled with a comprehensive service offering, including security training services, NTO is uniquely positioned to provide complete application security solutions to today's businesses.

About Mike Shema

Mike Shema is Director of Research & Development at NT Objectives where he focuses on assessment and mitigation strategies for all aspects of web application security.

Prior to joining NT OBJECTives, Mr. Shema worked as a Principal Consultant at Foundstone where he performed network penetration tests, web application security assessments, and wireless network security audits. In this time Mr. Shema led security audits for Fortune 100 companies, financial institutions, and large software development companies. Diverse clients and application platforms have enabled Mike to field-test and expand security methodologies, techniques, and tools across the entire enterprise security industry.

Mr. Shema previously worked at a product development company where he configured and deployed high-capacity Apache web and Oracle database servers for numerous Internet clients; and also worked at Booz Allen Hamilton where he conducted security assessments for government and military networks across the country.

His experience with Web application security has led to several **Bugtraq** advisories, co-authorship of ***Hacking Exposed: Web Applications***, and authoring ***Hack Notes: Web Application Security***. He has also co-authored ***The Anti-Hacker Toolkit***, creating a collection of tools and techniques for security administrators to secure and defend enterprise networks. He has taught at the Black Hat conferences in Las Vegas, Singapore, and Amsterdam, and continues to speak regularly at premier industry conferences and events around the world.

Mr. Shema's other writing credits include technical columns about Web server security for ***Security Focus*** and ***DevX*** and technical editor for ***Incident Response: Investigating Computer Crime***. He holds B.S. degrees in Electrical Engineering and French from Penn State University.