



OWASP Top Ten Vulnerabilities – Watchfire Compliance

Top Vulnerabilities in Web Applications From Open Web Application Security Project's (OWASP)* Top Ten List		Detected by AppScan?
Unvalidated Input	Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.	Yes
Broken Access Control	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.	Yes
Broken Authentication and Session Management	Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.	Yes
Cross-Site Scripting (XSS) Flaws	The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.	Yes
Buffer Overflows	Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers and web application server components.	Yes
Injection Flaws	Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.	Yes
Improper Error Handling	Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service and cause security mechanisms to fail, or crash the server.	Yes
Insecure Storage	Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.	**

Denial of Service	Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.	Yes
Insecure Configuration Management	Having a strong server configuration standard is critical to a secure web application. These servers have many configuration options that affect security and are not secure out of the box.	Yes

* The OWASP Top Ten is a list of vulnerabilities that require immediate remediation. Existing code should be checked for these vulnerabilities, as these flaws are being actively targeted by attackers. Development projects should address these vulnerabilities in their requirements documents and design, and build and test their applications to ensure that they have not been introduced. Project managers should include time and budget for application security activities including developer training, application security policy development, security mechanism design and development, penetration testing and security code review.

** AppScan checks for defects in some but not all cryptographic functions. Contact Watchfire with questions about specific encryption methods.