



The Top Ten List

The following is a short summary of the most significant web application security vulnerabilities. Each of these is described in more detail in the following sections.

| Top Vulnerabilities in Web Applications | | |
|---|--|---|
| A1 | 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. |
| A2 | 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. |
| A3 | 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. |
| A4 | 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. |
| A5 | 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. |
| A6 | 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. |
| A7 | 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, cause security mechanisms to fail, or crash the server. |
| A8 | 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. |
| A9 | 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. |
| A10 | 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. |



Our Application Assessment methodology includes within it the OWASP Top 10 and we develop remediation plans to address each of the OWASP Top Ten most Critical Web Application Vulnerabilities. Integral is also very active in the local OWASP user group.