



OWASP Top 10, 2010— *The Ten Most Critical Web Application Security Risks*

As the leading cloud-based business integration company, Hubspan adheres to the highest levels of security across its products, processes, and services. Hubspan takes a comprehensive, 360 degree approach to security, making sure your data and business processes are protected throughout the integration process.

Hubspan’s commitment to building the most secure cloud integration platform is reflected in addressing the OWASP 2010 Top Ten Security Risks.

The OWASP Top Ten is a list of the ten most dangerous current Web application security flaws, along with effective methods of dealing with those flaws. OWASP (Open Web Application Security Project) is an organization that provides unbiased, practical, and cost-effective security information about computer and Internet applications.

Every few years OWASP updates the Top Ten and has done so in 2010. The OWASP Top Ten was first released in 2003, minor updates were made in 2004 and 2007, and this reflects the 2010 updated Top Ten, see http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project for details.

In the commercial market, the Payment Card Industry (PCI) standard has adopted the OWASP Top Ten, and requires (among other things) that all merchants get a security code review for all their custom code. In addition, a broad range of companies and agencies around the globe are also using the OWASP Top Ten.

Hubspan provides industry leading security features and best practices. Hubspan emphasizes data encryption, access controls, key management security functionality as well as adherence to guidelines published by the CSA, PCI DSS, OWASP, and SAS 70 Type II.

Application Security Risks	Description	Hubspan’s Adherence
A1: Injection	Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.	Hubspan prevents SQL injection by implementing stored procedures containing bind variables, which are strongly tied to web form fields. Hubspan validates all input data prior to being used. Other flaws such as OS and LDAP are also tightly controlled.
A2: Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim’s browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.	UTF-8 encoding was applied to all Java Server Pages (responses) as we well as specifying UTF-8 encoding in the action request, before any processing of fields start. All data displayed to the user is properly HTML-encoded.
A3: Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users’ identities.	Passwords are not directly stored by the application, instead a digest form is stored. Authentication tokens stored within session cookies are persistent in an encrypted form and are transient in order to prevent unauthorized data access.
A4: Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.	Direct object references are encrypted with a token that changes with each web request unique to a user’s session. All references are validated to ensure that the user is authorized to access that resource.

OWASP Top 10, 2010—The Ten Most Critical Web Application Security Risks

Application Security Risks	Description	Hubspan's Adherence
A5: Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.	CSRF attacks are prevented by validating a secure random token and a timestamp that are renewed on every request. Hubspan generates the secure random token and sends it as part of the response in the form of an encrypted cookie. Checks are in place to verify that the tokens match and the request is within the required timeframe before the user is allowed to proceed.
A6: Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application.	Access to application configuration is tightly controlled by defaulting to the strongest security settings wherever appropriate. Processes are in place to ensure security patches are applied to all software used within or by the application.
A7: Insecure Cryptographic Storage	Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.	A strong industry standard for document cryptography is utilized to ensure that all messages are protected throughout all phases of transaction processing both at rest and in transit. Passwords and other credentials are stored in digest form.
A8: Failure to Restrict URL Access	Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway.	The application was designed from the ground up using an Access Control List (ACL) model based upon user roles, thereby preventing unauthorized access to pages and data.
A9: Insufficient Transport Layer Protection	Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly.	All data is transported using SSL or other secure transport protocols. Strong SSL certificates and encryption algorithms are used during SSL session negotiation.
A10: Unvalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.	The application doesn't forward or redirect to external websites, and any internal forwards are validated against an Access Control List.



About Hubspan, Inc.

Hubspan is the leading provider of business integration solutions, helping companies automate business processes and provide strong collaboration among cloud-based internal and external communities. Hubspan's cloud integration platform is cost-effective, scalable and reliable. With its any-to-any connections, Hubspan ensures seamless interoperability across systems, applications, and standards. Thousands of companies worldwide, from small and medium enterprises to Fortune 500 companies, successfully use the Hubspan platform every day to achieve stronger business collaboration. For more information, go to www.hubspan.com.