



## Airlock and the OWASP Top Ten Web Application Security Risks

The following table lists the ten most critical Web Application security risks, as identified by OWASP in their 2010 edition of “OWASP Top Ten”. It then explains for each of those risks how Airlock addresses them to protect Web Applications from these kinds of attacks.

Vulnerability	Description <sup>1</sup>	How Airlock prevents an exploit	Relevant Airlock features
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.	Requests containing SQL content are detected by a combination of blacklisting and dynamic whitelisting. URL Encryption and Smart Form Protection prevent any tampering of URL parameters and read-only form field values sent by the application. Other input containing SQL injection is blocked by the built-in SQL blacklist rules.	Built-in blacklist filters URL encryption Smart Form Protection
A2 – Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data 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.	Requests containing XSS content are detected by a combination of blacklisting and dynamic whitelisting. URL Encryption and Smart Form Protection prevent any tampering of URL parameters and read-only form field values sent by the application. Other input containing XSS is blocked by the built-in XSS blacklist rules.	Built-in blacklist filters URL Encryption Smart Form Protection

### About OWASP

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to conceive, develop, acquire, operate and maintain applications that can be trusted. All of the OWASP tools, documents, forums and chapters are free and open to anyone interested in improving application security.

*For more information on OWASP, visit their homepage at [www.owasp.org](http://www.owasp.org)*

### About OWASP Top Ten

The OWASP Top Ten is published roughly every 3 years and provides a powerful tool for raising awareness regarding Web Application security. The ten issues listed below represent a broad consensus on what the most critical Web Application security topics are at this time.

*For more information on the OWASP Top Ten, visit [www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)*

<sup>1</sup> Taken from the OWASP web site. Ergon’s comments in *italic*

Vulnerability	Description	How Airlock prevents an exploit	Relevant Airlock features
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.	As the HTTP protocol is stateless by nature, sessions are normally bound to a session ID contained in a cookie or in a URL parameter which is passed with each call. Any session ID manipulation is prevented by encrypting all URLs or the session cookie. By default, Airlock replaces all application cookies with its own session tracking (based on the SSL session or a secure Airlock cookie).	Cookie Store Cookie Encryption URL Encryption Airlock Session Handling
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 can be protected using URL encryption and Smart Form Protection. Airlock will block requests if an URL or a form parameter was manipulated on the client side.	URL Encryption Smart Form Protection
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. <i>This attack is sometimes also called "session riding" or "one-click attack"</i>	A CSRF attack can be blocked by encrypting all URLs with a session-based key. Such a URL is therefore only valid for one user (and only during his or her session). The URL is useless for an attacker without the corresponding session cookie. As form action URLs are also encrypted, this technique protects both GET and POST requests. Note that URLs that are encrypted with a session-based key cannot be bookmarked or indexed by search engines. For most applications however, this restriction is irrelevant because the potentially vulnerable URLs may only be accessed after a personal login.	Session-based URL Encryption

Vulnerability	Description	How Airlock prevents an exploit	Relevant Airlock features
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.	Airlock contains default rules, which are regularly updated. When creating a new mapping, all rules will be activated, without any admin interaction. The regularly distributed Airlock updates affect all safety relevant components. Airlock customers are notified when a new update comes out.	Update Mechanism Default rules
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.	Sensitive data can get additional protection by Airlock if it is contained in the URL, in a hidden or option form field or in a cookie, since Airlock can encrypt all of these.	URL Encryption SMART Form Protection Cookie Store Cookie Encryption
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.	An URL that is encrypted with a session-based key is only valid for one user during his or her session. As the key is created randomly for each session, it is not predictable.  This technique also enforces proper usage of the application, i.e. it protects the application's flow. A page can therefore not be accessed before the application has presented the user with a link to it.	Session-based URL Encryption

Vulnerability	Description	How Airlock prevents an exploit	Relevant Airlock features
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.	Ergon actively monitors the SSL layer technology, and provides rapid fixes for newly discovered vulnerabilities. Airlock is acting as Reverse Proxy between the application and the browser; it can encrypt the connection using SSL. If necessary, application responses can be re-written to contain HTTPS URLs only, even if the back-end uses HTTP for performance reasons. Additionally, Airlock forbids weak or export SSL ciphers by default, and alerts in the case of expired SSL certificates.	SSL Termination Response Rewriting for HTML and other content types
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.	Airlock verifies redirects sent by its protected applications. Such redirects can be limited to certain destinations, to local destinations only or completely blocked. The Airlock Authentication Service also supports fixation or validation of user forwards to applications.	Authentication Service Redirects Filtering

### Leading international security solution

Airlock protects Web applications and Web services against attacks and provides sustainable, centrally monitored security. 200 customers in 8 countries already protect over 5000 applications with Airlock.

Ergon Informatik AG delivers specialist IT excellence with a clear focus on customer advantage. The company leads the field in the implementation of customised applications and is an established producer of software products.

Airlock is a registered trademark of Ergon Informatik AG.



Ergon Informatik AG  
Kleinstrasse 15  
CH-8008 Zürich

Telefon +41 44 268 89 00  
Telefax +41 44 261 27 50  
[www.ergon.ch](http://www.ergon.ch)