AIRLOCK by ergon

Airlock WAF und die OWASP Top 10 2013
Die 10 grössten Sicherheitsschwachstellen von Webanwendungen

Die folgende Übersicht zeigt auf, wie Airlock WAF Webanwendungen vor Sicherheitsrisiken schützt und welche Funktionalitäten von Airlock WAF dabei zur Anwendung kommen. Die Tabelle folgt den 10 grössten Sicherheitsschwachstellen von Webanwendungen, wie sie von der OWASP in ihrer aktuellen Ausgabe der «OWASP Top 10» (2013) definiert worden sind.

Schwachstelle	Beschreibung	Wie Airlock WAF schützt	Funktionalitäten von Airlock
A1: Injection	Injection-Schwachstellen, wie z.B. SQL-, OS- oder LDAP-Injection treten auf, wenn nicht vertrauenswürdige Daten als Teil eines Kommandos oder einer Abfrage von einem Interpreter verarbeitet werden. Ein Angreifer kann Eingabedaten dann so manipulieren, dass er nicht vorgesehene Kommandos ausführen oder unautorisiert auf Daten zugreifen kann.	Anfragen, die Injections wie SQL, XSS, HTML oder Operating System-Befehle enthalten, werden durch eine Kombination von Blacklist-Filtern und dynamischen Whitelist-Filtern detektiert und blockiert. URL-Verschlüsselung, Smart Form Protection und Dynamic Value Endorsement verhindern die Modifikation von URL-Parametern und versteckten Formularfeldern. Angriffe über Header-Felder oder Cookies werden durch Filter und/oder den Cookie Store verhindert. Airlock WAF selbst ist gegen Overflow und OS Injection-Attacken durch eine strikte Trennung der Security Domains, ASLR, No-Execute, starken Stack Schutz sowie SELinux, welches das Prinzip der minimalen Rechte umsetzt, geschützt. Die ICAP-Schnittstelle ermöglicht Inhaltsfilterung mittels Airlock WAF Add-on-Modulen wie SOAP/XML/AMF-Filtern oder Virenscannern von Drittanbietern. Andere Arten von Injection-Angriffen oder Protokollverletzungen werden durch den von Airlock WAF erzwungenen Protokollbruch verhindert.	– Eingebaute Blacklist-Filter – URL-Verschlüsselung – Smart Form Protection – Dynamic Value Endorsement (DyVE) – Header Whitelisting – Cookie Store – ICAP-Schnittstelle – Protokollbruch – Add-on-Module – Trennung der Security Domains – Prinzip der minimalen Rechte – ASLR, NX und SSP

Über OWASP
Das Open Web Application Security Project (OWASP) ist eine offene Community mit dem Ziel, Organisationen und Unternehmen bei der Verbesserung der Sicherheit von Webanwendungen zu unterstützen. Im Vordergrund stehen dabei Werkzeuge, Methoden und Konzepte für eine sichere Entwicklung sowie der Schutz von Webanwendungen. Für weitere Informationen zur OWASP: www.owasp.org

OWASP Top 10
OWASP Top 10 werden ca. alle drei Jahre publiziert und stellen einen Überblick über die derzeit 10 grössten Schwachstellen und Sicherheitsrisiken für Webanwendungen dar. Für weitere Informationen zu den OWASP Top 10: www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Schwachstelle	Beschreibung	Wie Airlock WAF schützt	Funktionalitäten von Airlock
A2: Fehler in Authentifizierung und Session-Management	Anwendungsfunktionen, die die Authentifizierung und das Session-Management umsetzen, werden oft nicht korrekt implementiert. Dies erlaubt es Angreifern, Passwörter oder Session-Identifikatoren zu kompromittieren oder die Schwachstelle so auszunutzen, dass sie die Identität anderer Benutzer annehmen können.	Das HTTP-Protokoll selbst ist zustandslos. Deshalb werden Sessions normalerweise an die Session-ID gebunden, welche in einem Cookie oder URL-Parameter den Anfragen mitgegeben wird. Die Manipulation dieser Session-ID wird durch Verschlüsselung der URL und der Session Cookies verhindert. Airlock WAF ersetzt standardmässig alle Applikations-Cookies durch sein eigenes Session Management (basierend auf der SSL Session-ID oder einem sicheren Airlock Session Cookie). Die Verwendung von Airlock Client Fingerprinting kann dazu genutzt werden, Aktivitäten, die auf ein Session Hijacking hindeuten, zu ahnden (z.B. Beenden der verdächtigen Session). Vorgelagerte Authentisierung stellt sicher, dass nur korrekt authentisierte Benutzer Zugriff auf die Applikationsserver erhalten. Dies umfasst auch WebSockets und SSL VPN Verbindungen. Es ist eine gute Idee, die Benutzerverwaltung an spezialisierte IAM-Komponenten zu delegieren. Airlock WAF kümmert sich zentral um Idle Timouts, Session Lifetimes und Logout Propagation.	– Vorgelagerte Authentisierung – Cookie Store – Cookie-Verschlüsselung – URL-Verschlüsselung – Sicheres Airlock Session Management – Airlock Client Fingerprinting – Vorgelagerte Authentisierung für WebSockets – SSL VPN
A3: Cross-Site Scripting (XSS)	XSS-Schwachstellen treten auf, wenn eine Anwendung nicht vertrauenswürdige Daten entgegennimmt und ohne entsprechende Validierung und Kodierung an einen Webbrowser sendet. XSS erlaubt es einem Angreifer, Scriptcodes im Browser eines Opfers auszuführen und somit Benutzersitzungen zu übernehmen, Seiteninhalte zu verändern oder den Benutzer auf bösartige Seiten umzuleiten.	Anfragen, die XSS enthalten, werden durch eine Kombination von Blacklist-Filtern und dynamischen Whitelist-Filtern blockiert. URL-Verschlüsselung, Smart Form Protection und Dynamic Value Endorsement verhindern die Modifikation von URL-Parametern und versteckten Formularfeldern. Sicherheitsrelevante Header wie X-XSS-Protection werden standardmässig hinzugefügt. Die Herkunft von Inhalten kann durch den Einsatz von Content-Security-Policy-Headern überprüft werden. Durch Setzen des HttpOnly-Flags schützt das Airlock WAF das Session Cookie vor Zugriffen aus Javascript-Code.	– Eingebaute Blacklist-Filter – Cookie Store – Cookie-Verschlüsselung – URL-Verschlüsselung – Smart Form Protection – Dynamic Value Endorsement – Sicheres Airlock Session Management – Header Rewriting
A4: Unsichere direkte Objektreferenzen	Unsichere direkte Objektreferenzen treten auf, wenn Entwickler Referenzen zu internen Implementierungsobjekten, wie Dateien, Ordner oder Datenbankschlüssel von aussen zugänglich machen. Ohne Zugriffskontrolle oder anderen Schutz können Angreifer diese Referenzen manipulieren, um unautorisiert Zugriff auf Daten zu erlangen.	Direkte Objektreferenzen können durch URL-Verschlüsselung, Smart Form Protection und Dynamic Value Endorsement geschützt werden. Airlock WAF blockiert Anfragen, falls diese manipulierte URL oder Formularfelder enthalten.	– URL-Verschlüsselung – Smart Form Protection – Dynamic Value Endorsement

Schwachstelle	Beschreibung	Wie Airlock WAF schützt	Funktionalitäten von Airlock
A5: Sicherheitsrelevante Fehlkonfiguration	Sicherheit erfordert die Festlegung und Umsetzung einer sicheren Konfiguration für Anwendungen, Framework, Applikations-, Web- und Datenbankserver sowie deren Plattformen. Alle entsprechenden Einstellungen müssen definiert, umgesetzt und gewartet werden, da sie meist nicht mit sicheren Grundeinstellungen ausgeliefert werden. Dies umfasst auch die regelmässige Aktualisierung aller Software, inkl. der verwendeten Bibliotheken und Komponenten.	Airlock WAF enthält Standardregeln, die regelmässig aktualisiert werden. Die mapping-orientierte Konfiguration ermöglicht es dem Administrator, selektiv nur den Zugriff auf bekannte Applikationen freizuschalten. Fehlermeldungen können umgeschrieben oder ersetzt werden, damit heikle Informationen (z.B. Stack Traces) nicht nach aussen weitergegeben werden. Typische Fehler wie zu freizügige CORS Header oder fehlende „secure“ Attibute in Cookies werden erkannt und korrigiert. Validatoren prüfen die Airlock Konfiguration und warnen vor üblichen Fehlkonfigurationen (Log Only Modus, unpassende Zertifikate, ...) Das Policy Learning generiert automatisch sinnvolle und ausgewogene Konfigurationsvorschläge, um entdeckte Probleme einfach zu beheben. Dies hilft dem Administrator bei der Einhaltung der best Practices und verhindert auch in Stresssituationen eine Überreaktion.	– Standardkonfiguration – Mapping-orientierte Konfiguration – Content Rewriting – Error Page Replacement – Header Rewriting – Konfigurationsvalidierung – Policy Learning
A6: Verlust der Vertraulichkeit sensitiver Daten	Viele Webanwendungen schützen sensitive Daten wie Kreditkarten- oder Authentisierungsinformationen ungenügend. Angreifer entwenden oder verändern solch ungenügend geschützte Daten, um Kreditkartenbetrug, Identitätsbetrug oder andere Straftaten zu begehen. Sensitive Daten müssen deshalb speziell geschützt werden, z.B. mittels Verschlüsselung von gespeicherten und übermittelten Daten oder über spezielle Vorkehrungen bei der Interaktion mit einem Browser.	Falls sensitive Daten in der URL oder einem Cookie enthalten sind, kann Airlock WAF diese durch Verschlüsselung schützen. Standardmässig enthält Airlock WAF Rewrite-Regeln, die es erlauben, sensitive Daten (wie z.B. Kreditkarteninformationen) aus Antworten herauszufiltern. Die korrekte Konfiguration von SSL/TLS ist nicht trivial. Ergon überwacht aktiv die Entwicklungen rund um SSL/TLS und stellt umgehend allfällige Sicherheitsupdates für Code oder Konfiguration zur Verfügung. Airlock WAF kann in seiner Funktion als Reverse Proxy die Verbindung zum Browser mit TLS verschlüsseln. Fall notwendig, können Antworten von Applikationen so umgeschrieben werden, dass sie nur HTTPS-URLs enthalten, selbst wenn die Applikation aus Performancegründen HTTP verwendet. Der Strict-Transport-Security Header (HSTS) wird standardmässig gesetzt. Public-Key-Pinning (HPKP) kann als Response Action konfiguriert werden. Zusätzlich verbietet Airlock WAF standardmässig den Einsatz von schwachen SSL/TLS-Verschlüsselungen. OCSP Stapling vereinfacht die Validierung von Zertifikaten. Passwort-Hashes sind sensitive Daten und gehören deshalb nicht in die Applikationsdatenbank. Vorgelagerte Authentisierung löst dies durch die Delegation an einen spezialisierten Authentisierungsservice.	– URL-Verschlüsselung – Cookie Store – Cookie-Verschlüsselung – Response Rewriting – SSL-Terminierung – Vorgelagerte Authentisierung
A7: Missing Function Level Access Control	Die meisten Webapplikationen überprüfen die Zugriffsrechte auf Applikationsfunktionen, bevor diese im GUI angezeigt werden. Trotzdem müssen die Zugriffsrechte auf Serverseite nochmals geprüft werden. Geschieht dies nicht, können Angreifer gefälschte Anfragen erstellen, mittels derer sie Zugriff auf unautorisierte Funktionen erhalten.	Eine verschlüsselte URL mit einem sessionbasierten Schlüssel ist nur für eine einzige Benutzersession gültig. Der Schlüssel ist zufällig und kann nicht vorhergesehen werden. Damit wird der Workflow der Applikation geschützt, da der Benutzer nur Aktionen auslösen kann, die von der Applikation vorgesehen waren. Seiten, die dem Benutzer nicht von der Applikation präsentiert wurden, können nicht aufgerufen werden. Mittels vorgelagerter Authentisierung lassen sich feingranulare Zugriffsrechte für Applikationspfade definieren.	– Sessionbasierte URL-Verschlüsselung – Vorgelagerte Authentisierung

Schwachstelle	Beschreibung	Wie Airlock WAF schützt	Funktionalitäten von Airlock
A8: Cross-Site Request Forgery (CSRF)	Ein CSRF-Angriff bringt den Browser eines angemeldeten Benutzers dazu, einen manipulierten HTTP-Request an die verwundbare Anwendung zu senden. Session Cookies und andere Authentifizierungsinformationen werden dabei automatisch vom Browser mitgesendet. Dies erlaubt es dem Angreifer, Aktionen innerhalb der betroffenen Anwendungen im Namen und Kontext des angegriffenen Benutzers auszuführen.	CSRF Token schützen sowohl standard HTML Webseiten wie auch JavaScript / REST Applikationen. URL Verschlüsselung mit Session-basiertem Schlüssel kann ebenfalls CSRF-Angriffe verhindern. Die verschlüsselten URLs sind nur für eine bestimmte Benutzersession gültig. Der X-XSS Header wird per Default gesetzt. CSP Header (Content-Security-Policy) können einfach mittels standard Response Actions hinzugefügt werden. Das „same-site“ Cookie Attribut kann auch hinzugefügt werden.	– CSRF Token – Sessionbasierte URL-Verschlüsselung – Header Rewrites – Cookie Rewriter
A9: Benutzen von Komponenten mit bekannten Schwachstellen	Softwarekomponenten wie Bibliotheken oder Frameworks laufen oft mit vielen Rechten. Sobald eine verwundbare Komponente ausgenützt wird, kann es deshalb zu ernsthaftem Datenverlust oder zur Übernahme eines Servers kommen. Applikationen, die verwundbare Komponenten enthalten, können andere Schutzmechanismen unterwandern und ermöglichen eine Vielzahl von Angriffen.	Das Airlock Team veröffentlicht regelmässig sicherheitsrelevante Updates und informiert Kunden, sobald Updates verfügbar sind. Airlock WAF schützt sich selbst durch eine sichere Architektur gegen 0-Day-Attacken. Privilege Separation (SELinux) erzwingt die korrekte Abarbeitung von Anfragedaten. Der Web Listener darf z.B. nicht auf das Session-Management zugreifen oder Anfragen an das Back-End schicken. Address-Layout-Randomization, No-Execute und Stack Protection reduzieren auf Airlock WAF den Angriffsvektor.	– Protokollbruch – Security compartments – ASLR, NX und SSP – Update Mechanismus
A10: Ungeprüfte Um- und Weiterleitungen	Viele Anwendungen leiten Benutzer auf andere Seiten oder Anwendungen um oder weiter. Dabei werden für die Bestimmung des Ziels oft nicht vertrauenswürdige Daten verwendet. Ohne eine entsprechende Prüfung können Angreifer ihre Opfer auf Pishing-Seiten oder auf Seiten mit Schadcode um- oder weiterleiten.	Airlock WAF verifiziert ausgehende Weiterleitungen. Location Parameters werden überprüft, z.B. bezüglich einer gültigen URL-Verschlüsselung. Airlock IAM ermöglicht es, Weiterleitungen zu fixieren oder zu validieren.	– Airlock Login/IAM – Filterung von Weiterleitungen – URL-Verschlüsselung

Über Ergon Informatik AG und Airlock Suite

Die 1984 gegründete Ergon Informatik AG ist führend in der Herstellung von individuellen Softwarelösungen und Softwareprodukten. Die Basis für unseren Erfolg: 250 hoch qualifizierte IT-Spezialisten, die dank herausragendem Know-how neue Technologietrends antizipieren und mit innovativen Lösungen Wettbewerbsvorteile sicherstellen. Ergon realisiert hauptsächlich Grossprojekte im B2B-Bereich.

Die Airlock Suite kombiniert die Themen Filterung und Authentisierung in einer abgestimmten Gesamtlösung, die punkto Usability und Services Massstäbe setzt. Das Security-Produkt Airlock ist seit dem Jahr 2002 am Markt und heute bei über 350 Kunden weltweit im Einsatz.

Ergon Informatik AG
Merkurstrasse 43
CH–8032 Zürich

+41 44 268 89 00
www.airlock.com
twitter.com/ErgonAirlock