AIRLOCK by ergon

Airlock und die OWASP TOP 10 - 2017

Version 2.1 | 24.11.2017

Ergon Informatik AG
smart people – smart software

Merkurstrasse 43
CH – 8032 Zürich

T +41 44 268 89 00
F +41 44 261 27 50

www.airlock.com
twitter.com/ErgonAirlock

AIRLOCK by ergon

OWASP Top 10

A1 – Injection 3
A2 – Broken Authentication 5
A3 – Sensitive Data Exposure 6
A4 – XML External Entities (XXE) 7
A5 – Broken Access Control 8
A6 – Security Misconfiguration 9
A7 – Cross-Site Scripting (XSS) 10
A8 – Insecure Deserialization 11
A9 – Using Components with Known Vulnerabilities 12
A10 – Insufficient Logging & Monitoring 13

Airlock und die OWASP Top 10 2017 - Die 10 grössten Sicherheitsschwachstellen von Webanwendungen

Die folgende Übersicht zeigt auf, wie Airlock Webanwendungen vor Sicherheitsrisiken schützt und welche Funktionalitäten von Airlock 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“ (2017) definiert worden sind.

Über die 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*

Die OWASP Top 10

Die 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

A1 – Injection

Beschreibung

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.

Wie Airlock schützt

Anfragen, die Injections wie SQL, XSS, HTML LDAP 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.

Funktionalitäten von Airlock

- Whitelist Parameter Learning
- Eingebaute Blacklist-Filter
- URL-Verschlüsselung
- Smart Form Protection
- Dynamic Value Endorsement (DyVE)
- Cookie Store
- CAPI-Schnittstelle
- Protokollbruch
- Add-on-Module
- Trennung der Security Domains
- Prinzip der minimalen Rechte
- Address-Layout-Randomization (ASLR)
- No-Execute (NX)
- Stack-protection (SSP)

A2 – Broken Authentication

Beschreibung

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.

Wie Airlock schützt

Airlock IAM hat sich seit vielen Jahren in hochsicheren Umgebungen als zentraler und spezialisierter Authentisierungs- und Autorisierungsserver bewährt. Airlock WAF ermöglicht vorgelagerte Authentisierung mit Airlock IAM und stellt sicher, dass nur korrekt authentisierte Benutzer Zugriff auf die Applikation und ihre Ressourcen erhalten. Dies umfasst auch WebSockets und SSL VPN Verbindungen. Airlock IAM unterstützt dazu diverse Authentisierungsverfahren. Mittels risikobasierter Authentisierung werden starke Authentisierungsverfahren nur ausgelöst, wenn Airlock ein erhöhtes Sicherheitsrisiko erkennt.

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 WAF Session Cookie). Durch die Verwendung von Airlock Client Fingerprinting können Aktivitäten die auf ein Session Hijacking hindeuten geahnt werden (z.B. Beenden der verdächtigen Session).

Funktionalitäten von Airlock

- Vorgelagerte Authentisierung mit Airlock IAM
- Risikobasierte Authentisierung
- Cookie Store
- Cookie-Verschlüsselung
- URL-Verschlüsselung
- Sicheres Session Management
- Airlock Client Fingerprinting
- SSL VPN

A3 – Sensitive Data Exposure

Beschreibung

Viele Webanwendungen und APIs schützen sensitive Daten wie Transaktionen, Gesundheitsdaten, oder persönliche Daten (PII) 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.

Wie Airlock schützt

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.

Funktionalitäten von Airlock

- URL-Verschlüsselung
- Cookie Store
- Cookie-Verschlüsselung
- Response Rewriting
- SSL/TLS-Terminierung
- Sichere SSL/TLS Konfiguration
- Vorgelagerte Authentisierung

A4 – XML External Entities (XXE)

Beschreibung

Diverse ältere oder schlecht konfigurierte XML Prozessoren evaluieren externe Entity-Referenzen in XML Dokumenten. Externen Entitites können missbraucht werden um beispielsweise auf interne Dateien oder Shares zuzugreifen und internes Port scanning, Remote Code Execution oder Denial of Service Attacken durchzuführen.

Wie schützt Airlock

Mit den Airlock XML Filter und SOAP Filter Add-ons kann ein Schutzlayer vor SOAP Webservices oder Webservices mit XML data streams gezogen werden. Diese Filter schützen gegen XEE und XXE Angriffe, auch bekannt als DTD Angriffe oder XML bombs.

Der Airlock XML Filter validiert XML data streams gegenüber den entsprechenden XML Schemas und der Airlock SOAP Filter validiert SOAP Messages gegenüber WSDL Dateien.

Anders als SOAP Webservices, benutzen RESTful Webservices meist das JSON Format für Datentransfer. Der integrierte JSON Parser von Airlock WAF ermöglicht es, für herkömmliche Webapplikationen und REST APIs eine einheitliche Sicherheitspolicy zu definieren.

Funktionalitäten von Airlock

- Airlock SOAP Filter Add-on
- Airlock XML Filter Add-on

A5 – Broken Access Control

Beschreibung

Zugriffsbeschränkungen für authentisierte Benutzer werden nicht richtig durchgesetzt. Angreifer nutzen dies aus um Zugriff auf Funktionen oder Daten zu erhalten, für welche sie nicht autorisiert sind, wie z.B. Benutzeraccounts, Benutzerdaten, geschützte Dateien, Business-Objekte oder Zugriffsrechte.

Wie Airlock schützt

Durch die vorgelagerte Autorisierung in Airlock WAF kann kein unautorisierter Request von aussen auf geschützte Applikationen gelangen. Airlock WAF wird als Policy Enforcement Point eingesetzt und prüft, ob ein Benutzer das Recht hat auf ein gewisses API bzw. eine Ressource zuzugreifen. Object Keys und IDs, welche die Applikation exponiert können mittels Whitelist Learning, URL Encryption, Smart Form Protection, oder Dynamic Value Endorsement (DyVE) vor Manipulation geschützt werden.

Funktionalitäten von Airlock

- Vorgelagerte Authentisierung und Autorisierung
- Zentraler Policy Enforment Point
- Whitelist Learning
- URL-Verschlüsselung
- Smart Form Protection
- Dynamic Value Endorsement (DyVE)

A6 – Security Misconfiguration

Beschreibung

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.

Wie Airlock schützt

Airlock WAF enthält Standardregeln die regelmässig aktualisiert werden. Die mapping-orientierte Konfiguration ermöglicht es dem Administrator, selektiv nur den Zugriff auf bekannte Applikationen freizuschalten. Standardfilter verhindern Zugriff auf typische administrative Bereiche einer Applikation die von extern nicht erreichbar sein sollten. URL Encryption bietet einen umfassenden Schutz gegen forceful browsing.

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“ Attribute in Cookies werden erkannt und korrigiert.

Validatoren prüfen die Airlock WAF 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.

Funktionalitäten von Airlock

- Sichere Standardkonfiguration
- Standardfilter
- Policy Learning
- URL-Encryption
- Mapping-orientierte Konfiguration
- Content Rewriting
- Error Page Replacement
- Header Rewriting
- Konfigurationsvalidierung

A7 – Cross-Site Scripting (XSS)

Beschreibung

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.

Wie Airlock schützt

Anfragen, die XSS enthalten, werden durch eine Kombination von Blacklist-Filtern und dynamischen Whitelist-Filtern blockiert. URL-Verschlüsselung, Smart Form Protection, Cookie Store, Cookie-Verschlüsselung und Dynamic Value Endorsement verhindern die Modifikation von Cookies, 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 Session Cookie vor Zugriffen aus JavaScript-Code.

Funktionalitäten von Airlock

- Eingebaute Blacklist-Filter
- Cookie Store
- Cookie-Verschlüsselung
- URL-Verschlüsselung
- Smart Form Protection
- Dynamic Value Endorsement (DyVE)
- Sicheres Airlock WAF Session Management
- Header Rewriting

A8 – Insecure Deserialization

Beschreibung

Unsichere Deserialisierung führt oft zu Remote Code Execution. Auch wenn keine Remote Code Execution möglich ist, können diese Schwachstellen z.B. für Replay und Injection Angriffe oder Privilege Escalation missbraucht werden.

Wie Airlock schützt

Parameter, die von einer Applikation interpretiert werden, müssen generell vor Manipulationen auf dem Client geschützt werden. Airlock WAF bietet hierfür diverse Möglichkeiten, z.B. den zentralen Cookie Store, Whitelist Learning, Form Protection oder Cookie Verschlüsselung. Mit dem Cookie Store ist es beispielsweise möglich, Cookies welche den Applikationszustand als serialisiertes Objekt enthalten, gar nicht erst an den Client auszuliefern und damit vor Manipulationen komplett zu schützen.

Da Airlock WAF die grobgranulare Zugriffssteuerung übernimmt, laufen Manipulationsversuche mit dem Ziel mehr Zugriffsrechte zu erreichen prinzipiell ins Leere.

Schutz gegen Plattform-weite Deserialisierungs-Schwachstellen, wie z.B. CVE-2015-4852 für Java, kann durch das Einspielen eines virtuellen Patches erreicht werden.

Funktionalitäten von Airlock

- Voregelagerte Zugriffskontrolle
- Cookie Store
- Cookie Verschlüsselung
- Whiltelist Learning
- HTML Form Protection
- Dynamic Value Endorsement (DyVE)
- Virtual Patching

A9 – Using Components with Known Vulnerabilities

Beschreibung

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.

Wie Airlock schützt

Das Airlock Team veröffentlicht regelmässig sicherheitsrelevante Updates für Airlock WAF und IAM. Das Airlock Security Team informiert über aktuelle Bedrohungen von Webapplikationen und veröffentlicht technische Sicherheitsanalysen inklusive virtuelle patches falls eine Schwachstelle nicht bereits standardmässig verhindert wird.

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 Backend schicken. Address-Layout-Randomization (ASLR), No-Execute (NX), Stack Protection (SSP) sowie die Least Privilege Policy (SELinux) für alle extern erreichbaren Dienste reduzieren auf Airlock WAF den Angriffsvektor.

Funktionalitäten von Airlock

- Hotfixes
- Virtuelle patches
- Protokollbruch
- Security compartments
- Address-Layout-Randomization (ASLR)
- No-Execute (NX)
- Stack-protection (SSP)
- SELinux/Least Privilege

A10 – Insufficient Logging & Monitoring

Beschreibung

Ungenügendes Logging und Monitoring, zusammen mit fehlender Integration von Incident Response, gibt Angreifern Zeit ihre Angriffe auszuweiten, zu persistieren, auf weitere Systeme zu gelangen und schliesslich Daten zu verändern, zu extrahieren, oder zu löschen. Die meisten Studien zeigen, dass Einbrüche erst nach 200 Tagen entdeckt werden. Wenn sie entdeckt werden, dann meist durch externe Hinweise und nicht durch interne Prozesse oder Monitoring.

Wie Airlock schützt

Airlock WAF als Web Application Firewall kümmert sich zentral und spezialisiert um die Detektion und Verhinderung von Angriffen aller Art. Detektierte Angriffe lassen sich im Onboard Reporting oder einem externen SIEM System weiter analysieren. Virtuelle Patches lassen sich zentral und vorgelagert für sämtliche geschützten Applikationen zeitnah einspielen.

Funktionalitäten von Airlock

- Detektion von aktiven Angriffen
- Logging von Angriffen
- Blockierung von Angriffen
- Event Generierung für Notifizierung und schnelle Incident Response
- Graphische Dashboards, in Real-time aktualisiert
- Logeinträge sind mit Dashboards verknüpft für schnelle Ursachenanalyse
- SIEM Integration (CEF Logformat, Airlock App für Splunk)