Vorschau: die OWASP Top 10 für API Security 2019

AIRLOCK®
SECURE ACCESS HUB

Airlock und die OWASP Top 10 für API Security 2019 (Entwurf Juli 2019) Die zehn kritischsten API Security Risiken

Die folgende Tabelle zeigt die zehn grössten API Security Risiken, wie sie von OWASP in ihrem Entwurf "OWASP Top 10 2019" von Juli 2019 dargestellt werden. Die Tabelle erklärt wie Airlock API jedes dieser Risiken adressiert, um APIs zu schützen und welche Features dafür relevant sind.

Vulnerability	Beschreibung durch OWASP	Wie Airlock API Gateway schützt	Relevante Airlock Features
A1 – Missing Object Level Access Control	APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface Level Access Control issue. Object level authorization checks should be taken in mind in every function that accesses a data source using an input from the user.	Airlock bietet umfangreiche Access Management Funktionen für APIs. Damit können API Zugriffe generell mittels solider Authentisierung und Autorisierung geschützt werden. Laut OWASP ist der Kern dieser Schwachstelle darin begründet, dass die Server Komponente den Status des Clients nicht verfolgt und sich daher auf Parameter wie Objekt-IDs verlässt, welche vom Client geschickt werden. Anhand dieser Objekt-IDs wird dann entschieden worauf zugegriffen wird. Airlock bietet mit dem patentierten DyVE (Dynamic Value Endorsement) Feature ein Gegenmittel dafür an. Mittels DyVE können Objekt-IDs (und andere Werte) über mehrere zusammenhängende Client Request verfolgt werden. Clients dürfen dann nur diejenigen IDs verwenden, die in der gleichen Interaktion bereits vom API angeboten, d.h. in einer Antwort ausgeliefert, wurden. Mit diesem Ansatz können Angreifer keine gestohlenen oder selbsterstellten Objekt IDs verwenden, um unautorisierten Zugriff zu erhalten.	– API Access Management – Authentisierung und Autorisierung von Benutzern und API Clients – Dynamic Value Endorsement (DyVE)

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

Über die OWASP Top 10
OWASP hat gerade mit einem Projekt für eine neue Top10 Liste für API Security begonnen, um das Bewusstsein für dieses neue Thema zu stärken. Die gelisteten Top 10 stellen einen breiten Konsens darüber dar, was die derzeit wichtigsten API-Sicherheitsthemen sind. Weitere Informationen zu den OWASP Top 10 finden Sie unter https://www.owasp.org/index.php/OWASP_API_Security_Project

Vorschau: die OWASP Top 10 für API Security 2019

AIRLOCK®
SECURE ACCESS HUB

Vulnerability	Beschreibung durch OWASP	Wie Airlock API Gateway schützt	Relevante Airlock Features
A2 – Broken Authentication	Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising system's ability to identify the client/user, compromises API overall security.	Airlock bietet zentrales Access Management für APIs mit Support für alle relevanten Standards wie OAuth 2 und OpenID Connect. Die Authentisierung von Benutzern und API Clients ist nicht auf API Keys beschränkt. Eine Vielzahl integrierter Authentisierungsmittel erlauben die einfache Umsetzung von starker Authentisierung (MFA) auch auf API Zugriffen. API Keys können in der Gültigkeit eingeschränkt werden auf autorisierte API Endpoints und Unterpfade, in Verbindung mit der verwendeten HTTP Methode. Des Weiteren ist Airlock kompatibel mit PSD2-Standards für Access Management, wie z.B. NextGenPSD2 oder STET. Roadmap 2020: Der Airlock API Gateway bietet integriertes API Key Management mit Usage Plans und deren Durchsetzung.	– Policy Enforcement für Authentisierung und Autorisierung – Riskiko-basierte oder adaptive Authentisierung – Integration von diversen Authentisierungsmitteln – Sicheres Session Management – OAuth 2 Support – OpenID Connect Support – API Key Durchsetzung – API Key Management
A3 – Excessive Data Exposure	Looking forward to generic implementations developers tend to expose all object properties without considering their individual sensitivity, relying on clients to perform the data filtering before showing it to the user. Without controlling client's state, servers receive more and more filters which can be abused to gain access to sensitive data.	In seiner Funktion als Reverse-Proxy kann Airlock Antworten von APIs umschreiben bevor sie an den Client geschickt werden. Insbesondere können damit sensitive Teile entfernt werden, die nicht exponiert werden sollen. Airlock kann API Spezifikationen (z.B. OpenAPI) prüfen und durchsetzen. Daher können Angreifer nicht länger mit illegalen Filter-Optionen herumspielen, welche die Endpoints «überlisten» und dazu bringen könnten, sensitive Informationen auszuliefern. Auch Fehlerseiten neigen dazu, sensitive Informationen zu enthalten und nach aussen zu transportieren. Mit Airlock können diese Seiten durch sichere Standard-Fehlerseiten ersetzt werden.	– Reverse-Proxy Architektur – Umschreiben von Inhalten – Ersetzen von Fehlerseiten – Durchsetzung von OpenAPI Spezifikationen

Vorschau: die OWASP Top 10 für API Security 2019

AIRLOCK®
SECURE ACCESS HUB

Vulnerability	Beschreibung durch OWASP	Wie Airlock API Gateway schützt	Relevante Airlock Features
A4 – Lack of Resources & Rate Limiting	Quite often APIs do not impose any restrictions on the size or number of resources that can be requested by the client/user. Not only this can impact the API server performance, leading to Denial of Service (DoS), but also leaves the door open to authentication flaws such as brute force.	Airlock hat Rate-Limiting Funktionen und erlaubt das Setzen von diversen Limiten auf Requests und JSON Objekten. Dazu gehören beispielsweise die maximale Verschachtelungstiefe, maximale Namenlängen, die Anzahl Elemente pro Ebene und natürlich die totale Grösse von Requests. Gegen Angriffe auf Authentisierungsmittel verfügt Airlock zudem über massgeschneiderte Detektions- und Präventionsmethoden. Roadmap 2020: Der Airlock API Gateway bietet flexible Usage Plans auf API Key level.	– Rate Limiting – Prüfen von Limiten und Thresholds – DOS Schutz – Detektion von Bruteforcing auf Authentisierungsmitteln
A5 – Missing Function/Resources Level Access Control	Complex access control policies with different hierarchies, groups and roles and a not so clear separation between administrative and regular functions tend to lead to authorization flaws. Exploiting these issues, attackers gain access to other users resources and/or administrative functions.	Airlock bietet umfangreiche Access Management und Kontrollfunktionen. Der Zugriff auf neue APIs ist standardmässig abgeschaltet und muss erst autorisiert werden. Die Autorisierung von authentisierten Requests ist feingranular möglich und berücksichtigt Endpoints, Unterpfade (z.B. /admin) wie auch die HTTP Methode (GET, POST, DELETE, etc.). Zusätzlich kann die Zugriffshistorie des Clients und ein Risiko Score in Zugriffsentscheide miteinbezogen werden, um Risiko-basierte bzw. adaptive Authentisierung umzusetzen.	– API Access Management – Einbezug von HTTP Methoden und Unterpfaden in die Autorisierung – Risiko-basierte oder adaptive Authentisierung – Historie von erfolgreichen Authentisierungen als Baseline dafür was «normal» ist

Vorschau: die OWASP Top 10 für API Security 2019

AIRLOCK®
SECURE ACCESS HUB

Vulnerabilities	Beschreibung durch OWASP	Wie Airlock API Gateway schützt	Relevante Airlock Features
A6 – Mass Assignment	Binding client provided data (e.g. JSON) to data models without proper properties filtering based on a whitelist usually lead to Mass Assignment. Either guessing objects properties, exploring other API endpoints or reading the documentation, providing additional object properties in request payloads, allow attackers to modify object properties they are not supposed to.	Airlock validiert API Call gegen eine formale Spezifikation, wie z.B. OpenAPI. Zugriff auf nicht-publizierte Endpoints, «kreative» Objektsyntax und Attributwerte werden bereits auf dem Gateway unterbunden. Darüber hinaus unterstützt Policy Learning bei der Erstellung von sicheren Regeln, falls die Spezifikation nicht eng genug ist. Wenn beispielsweise die Spezifikation das Format «String» verlangt, ermöglicht dies nach wie vor Injection Angriffe auf diesem Attribut (siehe A8). Policy Learning analysiert effektiv abgesetzte Calls und kann z.B. empfehlen ein Attribut auf UUIDs einzuschränken, weil alle beobachteten Werte diesem Format entsprechen. Damit können Injection Angriffe verhindert werden. Zusätzlich werden alle Attribute mit den eingebauten Blacklist Rules und Angriffssignaturen abgeglichen. Mittels DyVE (Dynamic Value Endorsement) können Objekt-IDs und andere Werte innerhalb einer Client Interaktion (z.B. alle Request mit demselben Access Token) dynamisch erlaubt werden. Ein Beispiel: Nachdem der Benutzer erfolgreich authentifiziert wurde, darf das «user_name» Attribut in nachfolgenden Calls nicht mehr geändert werden, sondern muss dem vom API in der Antwort gelieferten Wert entsprechen.	– Support für OpenAPI Spezifikationen – Policy Learning – Angriffs-Signaturen und Blacklist Regeln – DyVE (Dynamic Value Endorsement)

Vorschau: die OWASP Top 10 für API Security 2019

AIRLOCK®
SECURE ACCESS HUB

Vulnerabilities	Beschreibung durch OWASP	Wie Airlock API Gateway schützt	Relevante Airlock Features
A7 – Security Misconfiguration	Security misconfiguration is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive Cross-Origin resource sharing (CORS) and verbose error messages containing sensitive information.	Airlock enthält Standardregeln die regelmässig aktualisiert werden. Die Mapping-orientierte Konfiguration ermöglicht es dem Administrator, selektiv nur den Zugriff auf bekannte Endpoints freizuschalten. Standardfilter verhindern Zugriff auf typische administrative Bereiche einer Applikation die von extern nicht erreichbar sein sollten. 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 Konfiguration und warnen vor üblichen Fehlkonfigurationen (Log Only Modus, unpassende Zertifikate, etc.) 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. Wenn formale Spezifikationen für APIs vorhanden sind (z.B. OpenAPI), kann Airlock automatisch die eingehenden Requests überprüfen und nicht-konforme Anfragen blockieren. Eine umfangreiche und somit fehleranfällige Konfiguration der API Security Policy wird damit auf ein überschaubares Mass reduziert. Zudem liefert Airlock immer aktuelle TLS Konfigurationen, die zentral durchgesetzt werden. HTTP Security Headers werden standardmässig gesetzt und können angepasst werden.	– Sichere Standardeinstellungen – Eingebaute Filter – TLS Terminierung und sichere TLS Konfiguration – Regelmässig aktualisiertes System, Hotfixes für dringende Patches – Unterstützung für Integratoren durch Policy Learning – Standard CORS Regeln – Umschreiben von Inhalten und Headern – Ersetzen von Fehlerseiten – Konfigurations-Validierung – Support für OpenAPI Spezifikationen

Vorschau: die OWASP Top 10 für API Security 2019

AIRLOCK®
SECURE ACCESS HUB

Vulnerabilities	Beschreibung durch OWASP	Wie Airlock API Gateway schützt	Relevante Airlock Features
A8 – Injection	Injection flaws, such as SQL, NoSQL, Command 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 data without proper authorization.	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. Globale Threat Intelligence Feeds, die in Echtzeit aktualisiert werden, werden eingesetzt um Clients zu blockieren, die nachweislich solche und ähnliche Angriffe ausgeführt haben. Falls formale API Spezifikationen wie OpenAPI zur Verfügung stehen, kann Airlock automatisch die Konformität der Calls überprüfen und verhindert damit Injection Angriffe auf typisierte Objektattribute. DyVE (Dynamic Value Endorsement) kontrolliert zudem Objekt-IDs in API Interaktionen und erschwert die Injection von selbsterzeugten IDs. Angriffe über Header-Felder oder Cookies werden durch Filter und/oder den Cookie Store verhindert. Airlock 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 erzwungenen Protokollbruch verhindert.	– Blacklist Filters – Support für OpenAPI Spezifikationen – Dynamic Value Endorsement (DyVE) – Policy Learning – Cookie Store – HTTP/S Protokollbruch – Security Domain Separierung – Address-Layout-Randomization (ASLR) – No-Execute (NX) – Stack-protection (SSP) und Stack Clash Protection
A9 – Improper Assets Management	APIs tend to expose more endpoints than traditional web applications, what makes proper and updated documentation highly important. Proper hosts and deployed API versions inventory also play an important role to mitigate issues such as deprecated API versions and exposed debug endpoints.	Airlock liest formale API Definitionen wie z.B. OpenAPI Spezifikationen. Der Zugriff wird nur auf effektiv veröffentlichte Endpoints und Versionen freigeschaltet, die in der Spezifikation enthalten sind. Zusätzlich wird sicheres Access Management auf den öffentlichen Endpoints durchgesetzt. Andere Endpoints und Hosts bleiben intern und sind dank der Reverse-Proxy Architektur von Airlock von aussen nicht erreichbar. OpenAPI Spezifikationen sind auf Airlock abgelegt und können öffentlich als stets aktuelle API Dokumentation für Client Entwickler verfügbar gemacht werden.	– Support für OpenAPI Spezifikationen – Selektive Publikation von API Endpoints – Access Management für öffentliche API Endpoints – Reverse-Proxy Architektur – Zentraler Zugriff auf aktuelle API Dokumentation

Vorschau: die OWASP Top 10 für API Security 2019

AIRLOCK®
SECURE ACCESS HUB

Vulnerabilities	Beschreibung durch OWASP	Wie Airlock API Gateway schützt	Relevante Airlock Features
A10 – Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.	Airlock ist spezialisiert auf die Detektion und Prävention von Angriffen auf APIs. Jeder Zugriff und jeder sicherheitsrelevante Vorfall wird in einer Datenbank persistiert. Detektierte Angriffe sind im mitgelieferten Reporting System auf diversen Standard Dashboards sichtbar. Eine dynamische Abfragesprache erlaubt zudem spezifische Detailanfragen an die Datenbank und die entsprechende Aktualisierung der Dashboards. Bei Angriffen werden Events generiert und bei Bedarf können verantwortliche Personen benachrichtigt werden. Angriffsinformationen können zur Event-Korrelation und Incident Analyse an ein SIEM System weitergeleitet werden. Mit den unterstützen Formaten CEF und JSON lassen sich die gängigen SIEM Systeme problemlos anbinden. Virtuelle Patches auf dem zentralen Gateway sorgen beim nächsten Incident dafür, dass offene Schwachstellen gegen aussen schnell und zentral geschlossen werden können. Dies verschafft die notwendige Zeit um alle Back-end Systeme abzusichern.	– Detektion, Logging und Blockierung von Angriffen – Event Generierung für Notifikation und schnelle Incidence Response – Echtzeit Dashboards mit grafischer Visualisierung – Einfacher Drill-down von Grafiken auf die ursächlichen Logzeilen – SIEM Integration (CEF und JSON Logformat) – Airlock App für Splunk

International führende Sicherheitslösung
Airlock schützt Webapplikationen und Webservices vor Angriffen und sorgt für nachhaltige, zentral kontrollierte Sicherheit. 550 Kunden in 11 Ländern schützen tausende Applikationen und mehr als 20 Millionen Identitäten mit Airlock.

Ergon Informatik AG steht für exzellente IT-Spezialisten mit ausgeprägtem Fokus auf den Kundennutzen. Das Unternehmen ist führend in der Realisierung von massgeschneiderten Anwendungen und ein etablierter Hersteller von Softwareprodukten.

Ergon Informatik AG
Merkurstrasse 43
CH-8032 Zürich

Telefon: +41 44 268 89 00
www.ergon.ch

ergon