RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-01	Abstreiten der Buchung	Mittel	Hoch	Mittel	Reduzieren
Beschreibung					
Ein Fluggast streitet die Buchung eines Fluges ab.					
Anforderungen					
Eine Buchung muss beweisfähig an Fluggast/Benutzer gebunden sein. **OWASP 7.1.4** Verify that each log event includes necessary information that would allow for a detailed investigation of the timeline when an event happens.					
Maßnahmen				**Überprüfung**	**TestID**
Bei jedem Login wird der Benutzer eindeutig identifiziert und ab diesem Punkt wird jede Aktion des Benutzers mit Zeitstempel festgehalten und gespeichert.				Automatisierter Test	T-01

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-02	Abstreiten der Stornierung	Mittel	Hoch	Mittel	Reduzieren
Beschreibung					
Ein Fluggast streitet die Stornierung eines Fluges ab.					
Anforderungen					
Eine Buchung muss beweisfähig an Fluggast/Benutzer gebunden sein. **OWASP 7.1.4** Verify that each log event includes necessary information that would allow for a detailed investigation of the timeline when an event happens.					
Maßnahmen				**Überprüfung**	**TestID**
Bei jedem Login wird der Benutzer eindeutig identifiziert und ab diesem Punkt wird jede Aktion des Benutzers mit Zeitstempel festgehalten und gespeichert.				Automatisierter Test	T-01

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-03	Löschen von Logs	Mittel	Hoch	Mittel	Reduzieren

Beschreibung
Ein Angreifer kann Logs löschen.

Anforderungen
Der Zugriff auf Logs muss gesichert sein. **OWASP 7.3.3** Verify that security logs are protected from unauthorized access and modification.

Maßnahmen	Überprüfung	TestID
Das Backend erlaubt keine Löschvorgänge der Logs in der Datenbank. Die Datenbank selbst ist durch ein Passwort geschützt.	Design / Code Review	-

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-04	Passwortdiebstahl	Hoch	Sehr hoch	Hoch	Reduzieren

Beschreibung

Ein Angreifer kann fremde Passwörter aus der Datenbank auslesen.

Anforderungen

Geklaute Passwörter aus der Datenbank sollten wertlos für Angreifer sein.

OWASP 2.4.1 Verify that passwords are stored in a form that is resistant to offline attacks. Passwords SHALL be salted and hashed using an approved one- way key derivation or password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash.

OWASP 2.4.2 Verify that the salt is at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. For each credential, a unique salt value and the resulting hash SHALL be stored.

Maßnahmen	Überprüfung	TestID
Alle Passwörter werden vor der Speicherung gesalted und gehashed.	Automatisierter Test	T-04

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-05	Flugdaten ausspähen	Hoch	Mittel	Mittel	Reduzieren
Beschreibung					
Ein Angreifer kann Flugdaten von Kunden ausspähen.					
Anforderungen					
Jeder Standard-Benutzer darf nur seine eigenen Buchungsinformationen sehen. **OWASP 13.1.2** Verify that access to administration and management functions is limited to authorized administrators.					
Maßnahmen				**Überprüfung**	**TestID**
Der Admin-Account ist mit Multi-Faktor-Authentifizierung geschützt und kann nur von autorisierten Administratoren verwendet werden.				Manueller Test	T-05

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-06	Diebstahl von Kreditkarteninformationen	Sehr hoch	Sehr hoch	Sehr hoch	Transferieren
Beschreibung					
Ein Angreifer kann Zugang zu Kreditkarteninformationen im Transit oder der nach Speicherung erlangen.					
Anforderungen					
Benutzer müssen ihre Kreditkarteninformationen sicher übertragen können. **OWASP 7.1.1** Verify that the application does not log credentials or payment details. Session tokens should only be stored in logs in an irreversible, hashed form.					
Maßnahmen				**Überprüfung**	**TestID**
Es wird ein externer Zahlungsdienstleister verwendet.				Code Review	-

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-07	Zahlreiche kurzfristige Stornierungen	Mittel	Hoch	Mittel	Reduzieren
Beschreibung					
Eine Gruppe von Angreifern/Accounts bucht Flüge aus und storniert diese kurz vor Abflug.					
Anforderungen					
Stornierungen müssen zeitlich limitiert oder an eine Gebühr gebunden sein.					
Maßnahmen				**Überprüfung**	**TestID**
Eine Erstattung des Ticket-Preis ist nur bei Stornierungen bis 48h vor Abflug möglich.				Code Review	-

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-08	Überladen des Servers mit Anfragen	Niedrig	Hoch	Niedrig	Akzeptieren
Beschreibung					
Der Server erhält zahlreiche Anfragen in kurzer Zeit, sodass der Server neue Anfragen nicht mehr bearbeiten kann (DDoS).					
Anforderungen					
Keine direkte Anforderung, da das Risiko akzeptiert wird (Aufwand zu hoch für den Anwendungsscope). *Falls sich die Eintrittswahrscheinlichkeit erhöht:* Der Server benötigt DDoS-Protection. **OWASP 11.1.4** Verify the application has sufficient anti-automation controls to detect and protect against data exfiltration, excessive business logic requests, excessive file uploads or denial of service attacks.					
Maßnahmen				**Überprüfung**	**TestID**
Falls sich die Eintrittswahrscheinlichkeit erhöht: Für den Server wird Load Balancing und eine IP Blacklist konfiguriert.				-	-

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-09	Speicherüberlastung der Datenbank durch automatisierte Benutzererstellung	Niedrig	Hoch	Niedrig	Akzeptieren

Beschreibung

Ein Angreifer kann durch automatisierte Benutzererstellung den Speicherverbrauch der Datenbank stark vergrößern, was zu Performanceeinbußen und Abstürzen führen kann.

Anforderungen

Keine direkte Anforderung, da das Risiko akzeptiert wird (Aufwand zu hoch für den Anwendungsscope).

Falls sich die Eintrittswahrscheinlichkeit erhöht: Das automatisierte Erstellen von Benutzern muss erschwert werden.

OWASP 11.1.8 Verify the application has configurable alerting when automated attacks or unusual activity is detected.

OWASP 13.2.4 Verify that REST services have anti-automation controls to protect against excessive calls, especially if the API is unauthenticated.

Maßnahmen	Überprüfung	TestID
Falls sich die Eintrittswahrscheinlichkeit erhöht: Zur Benutzererstellung wird ein Captcha-Test verwendet und der Benutzer benötigt einen zweiten Faktor (z.B. Telefonnummer)	-	-

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-10	Clientseitige Manipulation von Rolleninformationen	Sehr hoch	Sehr hoch	Sehr hoch	Reduzieren
Beschreibung					
Ein Angreifer kann durch die Manipulation von Rolleninformationen im Sitzungstoken die Administratorrolle annehmen.					
Anforderungen					
Sitzungstoken müssen vom Server signiert und bei Verwendung verifiziert werden. **OWASP 3.5.3:** Verify that stateless session tokens use digital signatures, encryption, and other countermeasures to protect against tampering, enveloping, replay, null cipher, and key substitution attacks.					
Maßnahmen				**Überprüfung**	**TestID**
Als Sitzungstokens werden signierte JWT-Tokens verwendet und bei einer Anfrage wird diese Signatur überprüft.				Automatisierter Test	T-10

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-11	Übernahme eines Admin-Sitzungstokens durch Stored XSS	Hoch	Sehr hoch	Hoch	Reduzieren
Beschreibung					
Ein Angreifer kann Nutzereingaben für Stored Cross-Site-Scripting verwenden, sodass Sitzungstoken eines Administrators bei Aufruf einer bestimmten Ressource/Liste an den Angreifer übermittelt wird.					
Anforderungen					
Die Applikation muss gegen Cross-Site-Scripting geschützt sein. **OWASP 5.2.7** Verify that the application sanitizes, disables, or sandboxes user-supplied Scalable Vector Graphics (SVG) scriptable content, especially as they relate to XSS resulting from inline scripts, and foreign Object. **OWASP 5.3.3** Verify that context-aware, preferably automated - or at worst, manual - output escaping protects against reflected, stored, and DOM based XSS.					
Maßnahmen				**Überprüfung**	**TestID**
Die Applikation verwendet flächendeckend Eingabevalidierung und Ausgabecodierung.				Penetration Test	T-11

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-12	SQL Injection	Sehr hoch	Sehr hoch	Sehr hoch	Reduzieren

Beschreibung

Ein Angreifer kann über eine Eingabemaske Daten aus der Datenbank auslesen und verändern.

Anforderungen

Die Applikation muss gegen SQL Injections geschützt sein.

OWASP 5.3.4 Verify that data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from database injection attacks.

OWASP 5.3.5 Verify that where parameterized or safer mechanisms are not present, context- specific output encoding is used to protect against injection attacks, such as the use of SQL escaping to protect against SQL injection.

Maßnahmen	Überprüfung	TestID
Die Applikation verwendet flächendeckend Eingabevalidierung.	Penetration Test	T-12

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-13	Ausprobieren von Anmeldeinformationen (Bruteforce)	Sehr hoch	Hoch	Hoch	Reduzieren

Beschreibung

Ein Angreifer kann verschiedene Anmeldeinformationen nacheinander ausprobieren und wird dabei nicht verlangsamt.

Anforderungen

Die Applikation verlangsamt Anmeldeprozess bei zu vielen fehlerhaften Anmeldeversuchen.

OWASP 2.2.1 Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.

Maßnahmen	Überprüfung	TestID
Ein Account wird nach 100 fehlerhaften Anmeldeversuchen vorläufig deaktiviert.	Automatisierter Test	T-13

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-14	Standard Admin-Kennwort	Mittel	Sehr hoch	Mittel	Vermeiden
Beschreibung					
Die Applikation wird mit einem Standard-Administratorkennwort ausgeliefert/bereitgestellt.					
Anforderungen					
Die Applikation darf keine Standard-Administratorkennwörter verwenden. **OWASP 2.5.4** Verify shared or default accounts are not present (e.g. "root", "admin", or "sa").					
Maßnahmen				**Überprüfung**	**TestID**
Administrator Kennwörter müssen gezwungenermaßen geändert werden.				Automatisierter Test	T-14

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-15	Ausnutzung der Wiederherstellung der Anmeldeinformationen	Hoch	Sehr hoch	Hoch	Vermeiden
Beschreibung					
Ein Angreifer nutzt Prozess der Wiederherstellung der Anmeldeinformationen aus.					
Anforderungen					
Es existiert keine Möglichkeit durch eine Wiederherstellungsfunktionalität der Anmeldeinformationen das alte Passwort offen zu legen. **OWASP 2.5.3** Verify password credential recovery does not reveal the current password in any way. **OWASP 2.5.5** Verify that if an authentication factor is changed or replaced, that the user is notified of this event.					
Maßnahmen				**Überprüfung**	**TestID**
Es wird keine Wiederherstellungsfunktionalität der Anmeldeinformationen implementiert				Design / Code Review	-

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-16	Selbsterstellte Krypto-Implementierung	Hoch	Sehr hoch	Hoch	Vermeiden
Beschreibung					
Ein Angreifer kann den selbst erstellten Schlüsselaustausch oder eine selbst erstellte Integritätskontrolle brechen / ausnutzen.					
Anforderungen					
Vertraulichkeit und Integrität der Daten bleibt gewahrt. **OWASP 2.9.3** Verify that approved cryptographic algorithms are used in the generation, seeding, and verification.					
Maßnahmen				**Überprüfung**	**TestID**
Sämtliche Prozesse, die Krypto involvieren, werden ausschließlich mit State-of-the-Art-Krypto umgesetzt.				Code Review	-

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R-17	Datenveränderung bei der Übertragung	Hoch	Sehr hoch	Hoch	Reduzieren
Beschreibung					
Ein Angreifer kann Daten manipulieren, da es keinen Integritätsschutz für Daten im Netzwerk gibt.					
Anforderungen					
Vertraulichkeit und Integrität müssen während der Übertragung geschützt sein. **OWASP 1.9.1** Verify the application encrypts communications between components, particularly when these components are in different containers, systems, sites, or cloud providers.					
Maßnahmen				**Überprüfung**	**TestID**
Kommunikation findet ausschließlich verschlüsselt und signiert statt.				Code Review	-