Web und API: Angemeldet heißt nicht berechtigt

PRUEFEN. BELEGEN. NACHHALTEN.

Prüfliste für Entwickler und autorisierte Tester. Ausschließlich eigene beziehungsweise ausdrücklich freigegebene Testsysteme und getrennte Testkonten verwenden.

Pruefbereich / Team:

Datum:

- [ ] **01 / Rollen, Mandanten, Aktionen und geschützte Objekte in einer Berechtigungsmatrix erfassen; Standardentscheidung bei fehlender Freigabe ablehnen.**

  Nachweis: Versionierte Matrix mit nachvollziehbaren Erlaubnis- und Verbotsfällen.

- [ ] **02 / Jeden serverseitigen Zugriff auf das konkrete Objekt und die Aktion autorisieren; übermittelte Objekt-IDs nicht als Berechtigungsnachweis behandeln.**

  Nachweis: Negative Direktaufrufe zwischen zwei Konten desselben und unterschiedlicher Mandanten.

- [ ] **03 / Administrative Funktionen separat prüfen; versteckte Menüs oder clientseitige Rollenanzeigen sind keine Zugriffssperre.**

  Nachweis: API-Tests mit nicht privilegiertem Konto für administrative Endpunkte und Methoden.

- [ ] **04 / Erlaubte Eingabe- und Ausgabefelder ausdrücklich festlegen; sensible Eigenschaften weder beliebig überschreiben noch unberechtigt ausliefern lassen.**

  Nachweis: Tests zusätzlicher Felder und geprüfte Antworten für unterschiedliche Rollen.

- [ ] **05 / Falls JWTs genutzt werden: erlaubte Algorithmen und vertrauenswürdige Schlüssel festlegen; erwarteten Aussteller, Empfänger und zeitliche Gültigkeit prüfen.**

  Nachweis: Ablehnung manipulierten, abgelaufenen sowie für andere Empfänger ausgestellten Tokens.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 12

- [ ] **06 / Berechtigungen auch bei Downloads, Suchergebnissen, Exporten und verschachtelten Ressourcen durchsetzen.**

  Nachweis: Abgedeckte alternative Zugriffspfade statt ausschließlich getesteter Detailseite.

- [ ] **07 / Bei automatisch mitgesendeten Browser-Zugangsdaten zustandsändernde Aktionen angemessen gegen CSRF schützen; CORS nicht als Autorisierung verwenden.**

  Nachweis: Gezielte Herkunfts-/CSRF-Tests und dokumentierte CORS-Konfiguration.

- [ ] **08 / Grenzfälle, entzogene Rechte und technische Fehler prüfen; bei fehlgeschlagener Prüfung sicher abbrechen und sensible Details nicht offenlegen.**

  Nachweis: Regressionstests für Rollenwechsel, fehlende Zuordnung und Fehlerpfade.

- [ ] **09 / Fehlgeschlagene und besonders relevante Zugriffe nachvollziehbar protokollieren, ohne Geheimnisse zu speichern; Aufwand und Datenmengen begrenzen.**

  Nachweis: Auffindbare Testereignisse, Datenminimierung und getestete Ressourcenlimits.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

Mit zwei freigegebenen Testkonten Zugriffe auf eigene und fremde Testobjekte vergleichen; die negative Gegenprobe muss serverseitig scheitern.

GRENZEN UND VORAUSSETZUNGEN

Unvorhersehbare IDs helfen gegen Erraten, ersetzen aber keine Autorisierung. Authentifizierung, Objektzugriff, Funktionsrechte und Feldfreigaben sind getrennte Prüfungen. Token- und Session-Verhalten hängt vom gewählten Profil ab; nicht jede Anwendung benötigt JWTs. Erfolgreiche Einzeltests beweisen keine vollständige Sicherheit aller API-Pfade.

PRIMAERQUELLEN / STAND 09.11.2026

OWASP: Authorization Cheat Sheet
cheatsheetseries.owasp.org

OWASP API Security: Broken Object Level Authorization
api-security.owasp.org

OWASP: REST Security Cheat Sheet
cheatsheetseries.owasp.org

OWASP: API Security Top 10
devguide.owasp.org