

Sicherheitsrichtlinien

Dennis Grabowski, Julius Zint, Philip Matesanz, Torben Voltmer

Masterprojekt „Entwicklung und Analyse einer sicheren
Web-Anwendung“
Wintersemester 18/19

9. Dezember 2018



Inhaltsverzeichnis

1	Annahmen	3
2	Akteure	4
3	Eintrittspunkte	4
4	Assets	5
5	Aktionen	5
6	Richtlinien	7
7	Literatur	10

1 Annahmen

- Netzwerkverbindungen sind abhörsicher und von außen nicht beeinflussbar.
- Betriebssystem, Hardware, Datenbank sowie verwendete Bibliotheken enthalten keine sicherheitsrelevanten Fehler.
- Hashing-Algorithmus „bcrypt“ macht es einem Angreifer wirtschaftlich unmöglich, evtl. erbeutete Password-Hashes durch Brute-Force oder Rainbow Tables in Klartext zu verwandeln.
- Lösen eines Captcha ist für einen Angreifer wirtschaftlich undurchführbar.
- Die von Google-Servern eingebundenen reCAPTCHA JavaScript-Dateien werden niemals zur Code-Injection verwendet / Google's reCAPTCHA Server sind grundsätzlich vertrauenswürdig.
- Bibliotheksfunktion `java.security.SecureRandom` [1] erstellt Zufallszahlen, die kryptografisch sicher sind.
- Einstellung `ALLOW_LITERALS=NONE` der Datenbank „h2“ verhindert SQL Injections.
- „JSON Web Token“-Format ist kryptografisch sicher zur Speicherung von Session- sowie Cookie-Daten.
- Die von JWT verwendete Signatur (HMAC-SHA256) verhindert, dass eine Manipulation von JWT-Cookies erfolgen kann.
- Applikation kann nur über die definierten Eintrittspunkte verwendet werden.
- Benutzer des HsH-Helpers verraten nicht ihr Passwort an andere.
- Initialer Benutzer „admin“ ist vertrauenswürdig.
- Autogenerierte IDs der Datenbank „h2“ sind aufsteigend und positiv. Sie werden nicht wiederverwendet, sofern eine ID wieder frei wird.
- Angreifer verfügen nur über einen begrenzten Pool an IP-Adressen, die „Anschaffung“ großer Mengen von IP-Adressen für einen Login-Brute-Force ist unwirtschaftlich.
- Zertifikate sind grundsätzlich vertrauenswürdig. Certificate Authorities stellen keine Zertifikate für missbräuchliche Zwecke aus.
- Die Quelle der kryptografisch-sicheren Zufallszahlen versiegt nicht (`/dev/random` (Linux), Cryptography API: Next Generation (Windows) [2]).
- Der gewählte Datentyp `Long` der Identifikatoren in der „h2-Datenbank“ ist für den Benutzungskontext des HsH-Helpers ausreichend lang.
- Nutzer des HsH-Helpers verwenden moderne, aktuelle Browser, die spezifische sicherheitsrelevante HTTP-Header unterstützen (Browser nach 2013 für CSP).

- Alle Browser respektieren den HTTP-Header `Content-Type: application/octet-stream`.
- Unserer In-Memory-Datenbank geht niemals der Speicher aus, zumindest in Rahmen dieses Projekts.
- Nutzer unserer Applikation greifen nur innerhalb einer Sandbox auf eine Datei zu.

2 Akteure

- Administratoren (A)
- Gruppenbesitzer (GO)
- Gruppenmitglied (GM)
- Dateibesitzer (DO)
- Authentisierter Benutzer mit Schreiberechtigung auf eine Datei (DW)
- Authentisierter Benutzer mit Leseberechtigung auf eine Datei (DR)
- Authentisierter Benutzer (U+)
- Unauthentisierter Benutzer (U-)
- E-Mail Server (EM)
- Google reCAPTCHA Server (GR)

Sofern nicht explizit anders geschildert, haben alle Akteure über dem „Authentisierten Benutzer“ die selben Basisrechte wie diese Privilegienstufe.

3 Eintrittspunkte

- Netzwerkschnittstellen
 - **EP1:** HTTP (Port 80) [U-, U+]
 - **EP2:** SMTP (Port 587) [U-]
- **EP3:** Eingebettetes Google reCAPTCHA JavaScript [U-, GR]

Sofern nicht explizit anders geschildert, geschieht ein Zugriff auf ein Asset oder das Durchführen einer Aktion über EP1.

4 Assets

- Benutzeranmeldeinformationen
 - **AS1:** Passworthash [-]
 - **AS2:** Session [U+, GM, GO, A]
- **AS3:** Gruppen [U+, GM, GO, A]
- **AS4:** Nutzerkonto [A]
- Dateien
 - **AS5:** Dateiname [DR, DW, DO]
 - **AS6:** Dateiinhalt [DR, DW, DO]
 - **AS7:** Kommentar [DR, DW, DO]
 - **AS8:** Zugriffsberechtigungen [DO]
- Netzdienste
 - **AS9:** Netzdienstanmelde-URL [A]
 - **AS10:** Zugangsdaten eines Nutzers für einen externen Netzdienst [U+]
 - **AS11:** Generierter Schlüssel zum Ver-/Entschlüsseln seiner Zugangsdaten für einen externen Netzdienst [-]
- **AS12:** Geheimnis für die Zwei-Faktor-Authentisierung [-]

5 Aktionen

- **AK1:** Einloggen [U-, GR] (Zusätzlich EP3)
- **AK2:** Ausloggen [U+]
- **AK3:** Nutzerkonto erstellen [A]
- **AK4:** Nutzerkonto löschen [A]
- **AK5:** Passwort-Reset anfordern [U-, EM, GR] (Zusätzlich EP2 & EP3)
- **AK6:** Passwort im Rahmen des Passwort-Reset neu vergeben [U+]

- **AK7:** Aktive Sessions anzeigen lassen [U+]
- **AK8:** Aktive Sessions zerstören [U+]
- **AK9:** Gruppe erstellen [U+]
- **AK10:** Gruppe löschen [GO, A]
- **AK11:** Nutzer zu einer Gruppe hinzufügen [GO, A]
- **AK12:** Nutzer aus einer Gruppe entfernen [GO, A]
- **AK13:** Gruppen anzeigen lassen [GM, GO, A]
- **AK14:** Mitglieder einer Gruppe sehen [GM, GO, A]
- **AK15:** Eine Datei hochladen [U+]
- **AK16:** Eine Datei löschen [DO]
- **AK17:** Eine Datei runterladen [DR, DO]
- **AK18:** Dateiinhalte und/oder -kommentar verändern [DW, DO]
- **AK19:** Dateien sowie Dateidetails anzeigen lassen [U+]
- **AK20:** Nutzerberechtigungen einer Datei verwalten [DO]
- **AK21:** Gruppenberechtigungen einer Datei verwalten [DO]
- **AK22:** Nutzer kann Speicherplatzverbrauch sowie -limit anzeigen lassen [U+]
- **AK23:** Speicherplatzlimit eines Nutzers anpassen [A]
- **AK24:** Session-Timeout einstellen [U+]
- **AK25:** Passwort ändern [U+]
- **AK26:** Nach Dateien suchen [U+, DR, DW, DO]
- **AK27:** Neuen Netzdienst hinzufügen [A]
- **AK28:** Bestehenden Netzdienst löschen [A]
- **AK29:** Parameter eines bestehenden Netzdienstes anpassen [A]
- **AK30:** Zugangsdaten für einen Netzdienst hinzufügen [U+]
- **AK31:** Hinterlegte Zugangsdaten für einen Netzdienst löschen [U+]
- **AK32:** Bei Netzdienst mit hinterlegten Zugangsdaten anmelden (Single Sign-On) [U+]
- **AK33:** Zwei-Faktor-Authentisierung für ein Nutzerkonto aktivieren [U+]
- **AK34:** Zwei-Faktor-Authentisierung für ein Nutzerkonto deaktivieren [U+, A]
- **AK35:** Letzte, erfolgreiche Logins anzeigen lassen [U+]

6 Richtlinien

Aktion	A	GO	GM	DO	DW	DR	U+	U-
AK1	✗	✗	✗	✗	✗	✗	✗	✓
AK2	✓	✓	✓	✓	✓	✓	✓	✗
AK3	✓	✗	✗	✗	✗	✗	✗	✗
AK4	✓	✗	✗	✗	✗	✗	✗	✗
AK5	✗	✗	✗	✗	✗	✗	✗	✓
AK6	✓	✓	✓	✓	✓	✓	✓	✗
AK7	✓	✓	✓	✓	✓	✓	✓	✗
AK8	✓	✓	✓	✓	✓	✓	✓	✗
AK9	✓	✓	✓	✓	✓	✓	✓	✗
AK10	✓	✓	✗	✗	✗	✗	✗	✗
AK11	✓	✓	✗	✗	✗	✗	✗	✗
AK12	✓	✓	✗	✗	✗	✗	✗	✗
AK13	✓	✓	✓	✗	✗	✗	✗	✗
AK14	✓	✓	✓	✗	✗	✗	✗	✗
AK15	✓	✓	✓	✓	✓	✓	✓	✗
AK16	✗	✗	✗	✓	✗	✗	✗	✗
AK17	✗	✗	✗	✓	✗	✓	✗	✗
AK18	✗	✗	✗	✓	✓	✗	✗	✗
AK19	✓	✓	✓	✓	✓	✓	✓	✗
AK20	✗	✗	✗	✓	✗	✗	✗	✗
AK21	✗	✗	✗	✓	✗	✗	✗	✗
AK22	✓	✓	✓	✓	✓	✓	✓	✗
AK23	✓	✗	✗	✗	✗	✗	✗	✗
AK24	✓	✓	✓	✓	✓	✓	✓	✗
AK25	✓	✓	✓	✓	✓	✓	✓	✗
AK26	✗	✗	✗	✓	✓	✓	✗	✗
AK27	✓	✗	✗	✗	✗	✗	✗	✗
AK28	✓	✗	✗	✗	✗	✗	✗	✗
AK29	✓	✗	✗	✗	✗	✗	✗	✗
AK30	✓	✓	✓	✓	✓	✓	✓	✗
AK31	✓	✓	✓	✓	✓	✓	✓	✗
AK32	✓	✓	✓	✓	✓	✓	✓	✗
AK33	✓	✓	✓	✓	✓	✓	✓	✗
AK34	✓	✓	✓	✓	✓	✓	✓	✗
AK35	✓	✓	✓	✓	✓	✓	✓	✗

- Nutzer [U+] können nur mit dem System interagieren, wenn sie authentisiert sind (AK2-4, sowie AK6-21).
- Ein Nutzer [U-] kann sich nur einloggen, wenn er ein eigenes Passwort vergeben hat.
- Ein Nutzer [U-] kann sein Passwort nur dann zurücksetzen, wenn er ein Authentifizierungsmerkmal angibt, dass er über einen vertrauenswürdigen Zweit-Kanal erhalten hat.
- Nutzer [GM, GO, A] können nur Gruppen sehen, dessen Mitglied sie sind (AK14).
- Ausschließlich Administratoren [A] können alle Gruppen sehen (AK14).
- Nutzer [GO] dürfen nur Mitglieder zu einer Gruppe hinzufügen, wenn sie der Besitzer dieser Gruppe sind (AK11).
- Ausschließlich Administratoren [A] können Mitglieder zu allen Gruppen hinzufügen (AK11).
- Nutzer [GO] dürfen nur Mitglieder aus einer Gruppe entfernen, wenn sie der Besitzer dieser Gruppe sind (AK12).
- Ausschließlich Administratoren [A] können Mitglieder (aber nicht den Besitzer) aus allen Gruppen entfernen (AK12).
- Kein Nutzer [U+] ist in der Lage, eine Gruppe zu erstellen (AK9), wenn der gewünschte Gruppenname (AS3) bereits von einer anderen Gruppe verwendet wird. Gruppennamen sind somit eindeutig.
- Kein Nutzer, auch nicht Administrator, [-] kann die Sessions anderer Nutzer betrachten oder zerstören (AK7-8).
- Passwörter eines Nutzer können von keinem Nutzer [-] ausgelesen werden.
- Ein Administrator [A] hat nur schreibenden Zugriff auf ein Nutzerkonto durch das Löschen des Nutzerkontos (AK4) oder durch Anpassen des Speicherplatzlimits eines Nutzers (AK23). Ihm ist nicht möglich, andere Informationen aus dem Nutzerkonto zu lesen oder zu ändern.
- Der initiale Benutzer „admin“ kann nicht gelöscht werden.
- Ein Nutzer [U+] darf nur dann gelöscht werden, wenn er weder Besitzer der Gruppe Alle oder Administratoren ist.
- Ein Nutzer [U-] muss ein Captcha lösen, wenn auf dem korrespondierenden Account 5 fehlgeschlagene Logins in einem Zeitraum von 5 Stunden erfolgt sind (AK1).
- Ein Nutzer [U-] muss ein Captcha lösen, wenn von seiner IP 15 fehlgeschlagene Logins in einem Zeitraum von 5 Stunden erfolgt sind (AK1).

- Ein Nutzer [U-] darf sich nicht mehr einloggen, wenn von seiner IP 30 fehlgeschlagene Logins in einem Zeitraum von 5 Stunden erfolgt sind (AK1).
- Die E-Mail eines Nutzerkontos ist einzigartig, so dass die Erstellung zweier Nutzerkonten mit der selben E-Mail-Adresse nicht möglich ist (AK3).
- Ein Nutzer [U-] muss zusätzlich ein Captcha lösen, um sein Passwort zurücksetzen lassen zu können (AK5).
- Ein Nutzer [U+] darf nur eine Datei hochladen (AK15), solange dessen Dateiname (AS5), -inhalt (AS6) und der Kommentar (AS7) zusammen nicht sein Speicherplatzlimit überschreiten.
- Ein Nutzer [DO] darf nur eine Datei löschen (AK16), wenn er dessen Besitzer ist.
- Ein Nutzer [DR] darf beim lesenden Zugriff auf eine Datei (AK17) keine Informationen verändern.
- Ein Nutzer [DW, DO] darf beim Verändern des Dateiinhalts oder des Kommentars (AK18) niemals den Dateinamen anpassen.
- Ein Nutzer [U+] darf sich nur Dateien anzeigen lassen (AK19), zu welchen er mindestens zum Lesen oder Schreiben berechtigt ist.
- Ein Nutzer [DO] darf die Nutzer- und Gruppenberechtigungen einer Datei jederzeit anpassen (AK20, 21); dies bedeutet löschen, hinzufügen, verändern.
- Ein Nutzer [U+] darf sich nur zu seinem **eigenem** Speicherplatzlimit informieren (AK22) und hat keinen Zugriff auf die Speicherplatzlimit anderer Nutzerkonten.
- Ein Nutzer [U+] darf nur seinen **eigenen** Session-Timeout (AK24) einstellen.
- Ein Nutzer [U+] darf nur sein **eigenes** Passwort (AK25) ändern.
- Nur der Dateibesitzer [DO] darf lediglich beim Upload der Datei schreibend auf den entsprechenden Dateinamen (AS5) zugreifen, alle anderen [DR, DW] nur lesend.
- Ein Nutzer [U+] hat nur Zugriff (AK29, AK30) auf seine **eigenen** Zugangsdaten (AS10) für einen Netzdienst.
- Wenn ein Nutzer [U+] die Zwei-Faktor-Authentisierung aktiviert hat (AK32), muss er den zweiten Faktor bei jedem Login (AK1) mit angeben.
- Ein Nutzer [U+] darf die Zwei-Faktor-Authentisierung nur für seinen **eigenen** Account aktivieren (AK33) und deaktivieren (AK34).
- Kein Nutzer [-], auch kein Administrator oder jemand mit Zugriff auf die Datenbank/Anwendung kann gespeicherten Netzdienst-Zugangsdaten (AS10) im Klartext auslesen.
- Ein Nutzer [U+] kann nur die ihm zugehörigen Netzdienst-Zugangsdaten (AS10) löschen (AK31) und im Klartext auslesen (AK32).

- Ein Nutzer [U+] kann nur die bei seinem Account erfolgten Logins (AK35) betrachten.
- Wenn ein Nutzer [U+] nach Dateien sucht (AK26), so kann er nur Dateien finden, für welche er mindestens zum Lesen oder Schreiben berechtigt ist.
- Ein Administrator [A] darf zusätzlich sehen, ob ein Nutzerkonto die Zwei-Faktor-Authentisierung verwendet, damit er, für den Fall, dass der Nutzer seinen zweiten Faktor (AS12) verloren hat, die Zwei-Faktor-Authentisierung für dieses Nutzerkonto deaktivieren (AK34) kann.

7 Literatur

- [1] Oracle and/or its affiliates. *SecureRandom - Java Platform, Standard Edition 8 API Specification*. URL: <https://docs.oracle.com/javase/8/docs/api/java/security/SecureRandom.html> (besucht am 11.04.2018).
- [2] *Cryptography API: Next Generation*. URL: <https://docs.microsoft.com/en-us/windows/desktop/SecCNG/about-cng> (besucht am 07.11.2018).