HOCHSCHULE
HANNOVER
UNIVERSITY OF
APPLIED SCIENCES
AND ARTS
–
Fakultät IV
Wirtschaft und
Informatik

Sicherheitsrichtlinien

Dennis Grabowski, Julius Zint, Philip Matesanz, Torben Voltmer

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

11. November 2018

Inhaltsverzeichnis

1 Annahmen 3

2 Akteure 4

3 Eintrittspunkte 4

4 Assets 4

5 Aktionen 5

6 Richtlinien 5

7 Literatur 7

Abkürzungsverzeichnis 8

Glossar 9

1 Annahmen

- Netzwerkverbindungen sind abhörsicher und von außen nicht beeinflussbar.
- Betriebssystem, Hardware 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 Plaintext zu verwandeln.
- Lösen eines Recaptchas ist für einen Angreifer wirtschaftlich undurchführbar.
- Die von Google-Servern eingebundenen Recaptcha Java-Script 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 (JWT)“-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-Helfers 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-Addressen, 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-Helfers ausreichend lang.

2 Akteure

- Administratoren (A)
- Gruppenbesitzer (GO)
- Gruppenmitglied (GM)
- Authentisierter Benutzer (U+)
- Unauthentisierter Benutzer (U-)
- E-Mail Server (EM)
- Google reCAPTCHA Server (GR)

3 Eintrittspunkte

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

Sofern nicht 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]

5 Aktionen

- **AK1:** Einloggen [U-, GR] (Zusätzlich EP3)
- **AK2:** Ausloggen [U+, GM, GO, A]
- **AK3:** Nutzerkonto erstellen [A]
- **AK4:** Nutzerkonto löschen [A]
- **AK5:** Passwort zurücksetzen lassen [U-, EM, GR] (Zusätzlich EP2 & EP3)
- **AK6:** Passwort nach Zurücksetzung anpassen [U+, GM, GO, A]
- **AK7:** Aktive Sessions anzeigen lassen [U+, GM, GO, A]
- **AK8:** Aktive Sessions zerstören [U+, GM, GO, A]
- **AK9:** Gruppe erstellen [U+, GM, GO, A]
- **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 [U+, GM, GO, A]
- **AK14:** Mitglieder einer Gruppe sehen [GM, GO, A]

6 Richtlinien

- Nutzer [U+, GM, GO, A] können nur mit dem System interagieren, wenn sie authentisiert sind (AK2-14).

Aktion	Administrator	Gruppenbesitzer	Gruppenmitglied	Nutzer
AK1	✗	✗	✗	✗
AK2	✓	✓	✓	✓
AK3	✓	✗	✗	✗
AK4	✓	✗	✗	✗
AK5	✗	✗	✗	✗
AK6	✓	✓	✓	✓
AK7	✓	✓	✓	✓
AK8	✓	✓	✓	✓
AK9	✓	✓	✓	✓
AK10	✓	✓	✗	✗
AK11	✓	✓	✗	✗
AK12	✓	✓	✗	✗
AK13	✓	✓	✓	✓
AK14	✓	✓	✓	✗

- Nutzer [U+, 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, 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 (AK4). Ihm ist nicht möglich, andere Informationen aus dem Nutzerkonto zu lesen oder zu ändern.
- Ein Nutzer [-] muss nur ein reCAPTCHA lösen, wenn er sich mehrmals hintereinander fehlerhaft eingeloggt hat (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 reCAPTCHA lösen, um sein Passwort zurücksetzen lassen zu können (AK5).

- Ein Nutzer [U+, GM, GO, A] darf nur dann gelöscht werden, wenn er weder Owner der Gruppe Alle oder Administratoren ist.

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).

[3] M. Jones, J. Bradley und N. Sakimura. *JSON Web Token (JWT)*. RFC 7519. http://www.rfc-editor.org/rfc/rfc7519.txt. RFC Editor, Mai 2015. URL: http://www.rfc-editor.org/rfc/rfc7519.txt.

Abkürzungsverzeichnis

DFD Datenflussdiagramm *Glossareintrag:* Datenflussdiagramm

JWT JSON Web Token 3, *Glossareintrag:* JSON Web Token

UUID Universally Unique Identifier *Glossareintrag:* Universally Unique Identifier

Glossar

JSON Web Token Ein auf JSON basiertes Access-Token, standardisiert in RFC7519 [3]. Ermöglicht den Austausch von verifizierbaren Daten. 3