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

28. November 2018

Inhaltsverzeichnis

1 Annahmen 3

2 Akteure 4

3 Eintrittspunkte 4

4 Assets 5

5 Aktionen 5

6 Richtlinien 7

7 Literatur 9

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 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.
- Nutzer des HsH-Helfers 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 Berechtigung zum Lesen und Schreiben auf eine Datei (DA)
- Authentisierter Benutzer mit Schreibeberechtigung 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+, 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]
- Dateien
  - **AS5:** Dateiname [DR, DW, DA, DO]
  - **AS6:** Dateiinhalt [DR, DA, DO]
  - **AS7:** Kommentar [DR, DW, DA, DO]
  - **AS8:** Zugriffsberechtigungen [DO]

5 Aktionen

- **AK1:** Einloggen [U-, GR] (Zusätzlich EP3)
- **AK2:** Ausloggen [U+]

- **AK3:** Nutzerkonto erstellen [A]
- **AK4:** Nutzerkonto löschen [A]
- **AK5:** Passwort zurücksetzen lassen [U-, EM, GR] (Zusätzlich EP2 & EP3)
- **AK6:** Passwort nach Zurücksetzung anpassen [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, DA, DO]
- **AK18:** Dateiinhalt und/oder -kommentar verändern [DW, DA, DO]
- **AK19:** Dateien anzeigen lassen [U+]
- **AK20:** Nutzerberechtigungen einer Datei verwalten [DO]
- **AK21:** Gruppenberechtigungen einer Datei verwalten [DO]
- **AK22:** Informationen zu dem Speicherplatzlimit eines Nutzers anzeigen lassen [U+]
- **AK23:** Speicherplatzlimit eines Nutzers anpassen [A]
- **AK24:** Nutzer kann Session-Timeout einstellen [U+]
- **AK25:** Nutzer kann Passwort ändern [U+]
- **AK26:** Nutzer kann nach Dateien suchen [DR, DW, DA, DO]

Aktion	A	GO	GM	DO	DA	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	✗	✗	✗	✓	✓	✓	✓	✗	✗

6 Richtlinien

- Nutzer [U+] können nur mit dem System interagieren, wenn sie authentisiert sind (AK2-4, sowie AK6-21).
- 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, 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 Owner der Gruppe Alle oder Administratoren ist.
- Ein Nutzer [U-] 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+] 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, DA, 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 mindestens zum Lesen oder Schreiben berechtigt ist.
- Ein Nutzer [DO] darf die Nutzer- und Gruppenberechtigungen einer Datei jederzeit anpassen (AK20, 21); 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 seinen eigenen Session-Timeout (AK24) einstellen.

- Ein Nutzer [U+] darf sein eigenes Passwort (AK25) einstellen.
- Nur der Dateibesitzer [DO] darf schreibend auf den Dateinamen (AS5) zugreifen, alle anderen [DR, DW, DA] nur lesend.

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).