Abschlussprojekt - Secure Software Engineering

Beschreibung

Als Abschlussprojekt sollen Sie eine eigene Software nach den in diesem Dokument beschriebenen Vorgaben sicher entwickeln. Hierbei wird unter dem Punkt "Umfang" einzeln erläutert, welche Funktion Sie wie implementieren sollen. Die einzelnen Punkte orientieren sich an dem Inhalt der Vorlesungen.

Die Anwendung soll eine klassische Client-Server Webanwendung sein. Welche Frameworks Sie für das Frontend und das Backend verwenden ist Ihnen freigestellt. Hierbei ist allerdings zu beachten, dass alle Teile der Anwendung local ausgeführt werden müssen und keine externen Hosting-Tools (wie z.B. Firebase) verwendet werden dürfen. Für die Umsetzung von bestimmten Funktionen dürfen Sie auch externe Bibliotheken verwenden. Wichtig hierbei ist, dass Sie die Funktionsweise dieser verstehen und mögliche Sicherheitsrisiken kennen. Beides sollte bei der Verwendung von externen Bibliotheken ausführlich dokumentiert werden.

Die Entwicklung soll mithilfe des Versionsverwaltungssystem `git` unter der Verwendung von gitlab (THM) oder github durchgeführt werden. Benutzen Sie hierbei den Feature-Branch Workflow. Wir empfehlen Ihnen die Verwendung von GitHub, da hier die Einrichtung der CI/CD ein wenig angenehmer ist.

Umfang

Anmeldung

In Ihrer Anwendung soll ein Nutzer sich mit einem Nutzernamen und einem Passwort anmelden können. Schlägt eine Anmeldung fehl, sollte der Benutzer sinnvoll darüber informiert werden. Die Anmeldung soll vor möglichen Angriffen abgesichert werden.

Checkliste

- ☐ Anmeldung mit Nutzername und Passwort möglich
- ☐ Sinnvolle Fehlermeldungen für den Benutzer anzeigen
- ☐ Eingabeformular vor möglichen Angriffen schützen
- ☐ Schnittstelle für die Anmeldung vor möglichen Angriffen schützen

Registrierung

Es soll möglich sein, sich bei der Anwendung als Benutzer zu registrieren. Hierbei sollte die Stärke des Passwortes überprüft werden. Die Passwörter sollen sicher in der Datenbank gespeichert werden. Bei einer fehlerhaften Registrierung sollte dem Nutzer eine sinnvolle Fehlermeldung angezeigt werden.

Checkliste

- ☐ Registrierung als Benutzer möglich
- ☐ Passwortstärke überprüfen
- ☐ Eingabeformular vor möglichen Angriffen schützen
- ☐ Schnittstelle für die Registrierung vor möglichen Angriffen schützen

Autorisierung

Ein Benutzer sollte für alle weitere HTTP-Anfragen autorisiert sein. Hierbei können Sie die Methode der Autorisierung frei wählen.

Checkliste

- ☐ Ein angemeldeter Nutzer wird autorisiert
- ☐ Die Autorisierung wird sicher gespeichert

Funktionen der Anwendung

Notiz

In der Anwendung soll es möglich sein, in einem Eingabefeld Notizen zu erstellen. Die Eingabe akzeptiert Markdown, um den Text zu formatieren. Hierbei sollen auch alle gängigen HTML-Tags unterstützt werden. Die geschriebenen Texte werden in einer Liste aller Notizen angezeigt. Eine Notiz kann als öffentlich oder privat markiert werden. Ist sie öffentlich so kann jeder Benutzer der Anwendung den Inhalt der Notiz in seiner Liste sehen. Ist eine Notiz privat taucht diese nur in der Liste des Erstellers auf.

Jede Notiz hat einen bestimmten Link, über welche sie erreicht werden kann, auch für Nutzer bei denen die Notiz nicht in ihrer Liste auftaucht. So ist es möglich, mit Nutzern die Notiz zu teilen über das weitergeben des Links. Dies gilt sowohl für private, als auch für öffentliche Notizen.

Link-Struktur `https://my-app.de/documents/{document_id}`

Checkliste

- ☐ Es ist möglich, Notizen mittels Markdown zu erstellen
- ☐ Nutzern mit Wissen über die Link-Struktur ist es nicht möglich, an private Notizen anderer zu gelangen.
- ☐ Der formatierte Markdown-Text ist sicher vor Angreifern

Social-Plugins (Gruppengröße: 3)

Es soll möglich sein, einer Notiz einen Youtube-Link anzuhängen, sodass das angegebene Video in einem IFrame abgespielt werden kann.

Checkliste

- ☐ YouTube-Videos können Notizen angehangen werden

Suche

Es soll möglich sein, über ein Suchfeld nach Notizen zu suchen. Hierbei sollte der Suchbegriff über den Ergebnissen angezeigt werden. Ebenso sollte der Inhalt der Suche als query-Paramter in der URL angezeigt werden.

Beispiel `https://my-app.de/search?q=suchbegriff%20in%20der%20url`

Checkliste

- ☐ Es ist möglich nach öffentlichen Notizen zu suchen (Gruppengröße 3)
- ☐ Es ist möglich nach eigenen Notizen zu suchen (Gruppengröße < 3)
- ☐ Der Eingegebene Suchbegriff wird über den Ergebnissen angezeigt
- ☐ Der Suchegriff steht als query-Parameter in der URL
- ☐ Eingabe des Suchfelds vor möglichen Angriffen schützen

CI/CD

Richten Sie Ihre CI/CD so ein, dass Ihre verwendeten dependiencies automatisch geupdatet werden. Des Weiteren sollten Sie Ihr Projekt so einrichten, dass Sie vor Vulnerabilities in Ihren Dependecies gewarnt werden. Richten Sie mindestens einen automatischen Test für das Frontend sowie das Backend ein.

Checkliste

- ☐ Verwendete Dependecies werden automatisch geupdatet
- ☐ Vor Sicherheitslücken in verwendeten Dependencies wird gewarnt
- ☐ Automatischer Test für das Frontend
- ☐ Automatischer Test für das Backend

Zusatzaufgaben

Die Zusatzaufgaben bringen Bonuspunkte. Gibt es in der Umsetzung, der Dokumentation oder der Präsentation Fehler, so können diese durch die Zusatzaufgaben ausgeglichen werden, um trotz der Fehler eine bessere Note zu bekommen. **WICHTIG: Zusatzaufgaben sind nicht notwendig, um die volle Punktzahl zu erreichen.**

OAuth / OpenIDConnect

Neben einer lokalen Anmeldung ist es ebenfalls möglich, sich mittels OAuth über dritte Dienste (wie z.B. GitHub) oder über OpenIDConnect bei einer lokalen zentralen Benutzer Verwaltung (hier kann z.B. keycloak verwendet werden) anzumelden.

Passwort vergessen

Ein Benutzer hat die Möglichkeit bei der Anmeldung auf ein `Passwort vergessen` Feld zu klicken, um daraufhin an eine angegebene E-Mail einen Link für das Zurücksetzen zu senden.

Dokumentation

Die Dokumentation des Projekts sollte einer gewissen Struktur folgen.

Beschreibung:

- Inhalt der Anwendung
- Gruppenmitglieder
- Verwendete Technologien (z.B. React, ...)

Infrastruktur

- CI/CD
- Verwendete IDE
- Struktur des Entwicklungsprozesses
    - z.B. Nutzung von GitHub mit Issues und Kanban-Board etc.

Funktionen

- Umsetzung jeder einzelnen Funktion
- mögliche Schwachstellen sowie deren Vorbeugung
- Datenschutz (werden sensible Daten gespeichert etc.)

In welchem Format Sie die Dokumentation erstellen ist Ihnen freigestellt. Diese muss nur in Ihrem GitHub Repository enthalten sein. Gerne können Sie auch einen `static site generator` wie `docusaurus` oder `mkdocs` verwenden und z.B. bei `Github-Pages` hosten. Hierbei reicht es aus wenn der Link zu der Dokumentation im Repository hinterlegt ist.

Präsentation

Datum: 07.07.2023 + 14.07.2023

Rahmen: Präsentationen zu den Modulzeiten.

Umfang: 10-15 Minuten pro. Person

Eine Powerpoint/Latex-Beamer Präsentation Ihres Projektes.

Inhalt: In der Präsentation sollen Sie die Anwendung mit denen von Ihnen umgesetzten Funktionen präsentieren. Hierbei sollen Sie auf die Umsetzung dieser eingehen, die möglichen Sicheheitsrisiken beschreiben und Ihr Schutz vor diesen erläutern.

Nach dem Vorstellen der Anwendung mittels der Powerpoint/Latex-Beamer Präsentation sollten Sie zum Schluss noch eine Live-Demo präsentieren.

Format:

- Schriftgröße auf den Folien: mind. 16 (durschnittlich 18-20)
- Nutzen Sie Grafiken

Abgabe

Deadline: 07.07.2023, 14:00 Uhr

Um Ihr Projekt erfolgreich abzugeben, müssen Sie die Dozenten (Benutzernamen) bis zum Abgabetermin zu dem Repository hinzufügen und den Link zu diesem bei Moodle abgeben. Desweiteren sollte die Präsentation als PDF-Datei im Repository enthalten sein. Wichtig ist, dass sich das Programm starten lässt. Hier empfiehlt sich die Verwendung von Docker, da es so zu keinen Kompatibilitätsproblemen durch verschiedene Systeme kommen kann. Commits die nach dem Abgabedatum gemacht werden, werden bei der Bewertung nicht berücksichtigt.

Checkliste

- ☐ Präsentation als PDF-Datei zum Repository hinzufügen
- ☐ Dozenten zum Repo hinzufügen (Benutzernamen)
- ☐ Abgabe in Moodle

Bewertung

Die Abgabe und Präsentation gehen zu jeweils 50% in die Endnote ein. Bei der Abgabe bekommt eine Gruppe eine gemeinsame Note, bei der Präsentation hingegen werden individual Noten für die einzelnen Vortragenden vergeben.

Anhang

Benutzernamen

(THM) Gitlab

Berechtigung: **Developer**

- msph97
- tplk70

Github

Berechtigung: **Write**

- mxsph
- TimonPllkrn