

ShopNook: E-Commerce Warenkorbanwendung mit Spring
Boot

ShopNook: Development of an e-commerce shopping cart application
with Spring Boot

Imad-Eddine Abdessami, Mohammed Salih Mezraoui

Bachelor-Projektarbeit

Betreuer: Prof. Dr. Andreas Lux

Ort, DD.MM.YYYY

Kurzfassung

In der Kurzfassung soll in kurzer und prägnanter Weise der wesentliche Inhalt der Arbeit beschrieben werden. Dazu zählen vor allem eine kurze Aufgabenbeschreibung, der Lösungsansatz sowie die wesentlichen Ergebnisse der Arbeit. Ein häufiger Fehler für die Kurzfassung ist, dass lediglich die Aufgabenbeschreibung (d.h. das Problem) in Kurzform vorgelegt wird. Die Kurzfassung soll aber die gesamte Arbeit widerspiegeln. Deshalb sind vor allem die erzielten Ergebnisse darzustellen. Die Kurzfassung soll etwa eine halbe bis ganze DIN-A4-Seite umfassen.

Hinweis: Schreiben Sie die Kurzfassung am Ende der Arbeit, denn eventuell ist Ihnen beim Schreiben erst vollends klar geworden, was das Wesentliche der Arbeit ist bzw. welche Schwerpunkte Sie bei der Arbeit gesetzt haben. Andernfalls laufen Sie Gefahr, dass die Kurzfassung nicht zum Rest der Arbeit passt.

Inhaltsverzeichnis

1	Einleitung und Problemstellung	1
1.1	Überblick	1
1.2	Globale Anforderungen	1
1.2.1	Funktionale Anforderungen	1
1.2.2	Nicht-funktionale Anforderungen	2
1.2.3	Technische Anforderungen	2
2	Methodologie und Systementwurf	3
2.1	Entwurf und Konzeption	3
2.1.1	UML	3
2.1.2	Klassendiagramm	4
2.1.3	Use-Case Diagramme	4
2.2	Front-End Technologien	4
2.2.1	HTML/CSS	4
2.2.2	Typescript	4
2.2.3	Angular	5
2.3	Back-End Technologien	6
2.3.1	Java	6
2.3.2	REST-API	6
2.3.3	HTTPS und SSL/TLS	7
2.3.4	Spring Boot	9
2.3.5	Stripe API	11
2.4	Datenbankstruktur	11
2.4.1	Übersicht über relationale Datenbanken und Auswahl von MySQL	11
2.4.2	Datenbankschemaentwurf mit Spring Data JPA	12
2.4.3	Datenpersistenz und Transaktionen	12
2.4.4	MySQL-Workbench und SQL	13
2.4.5	Datenbankverbindung und -konfiguration in Spring Boot	13
2.5	Authentifizierungs- und Autorisierungsprotokolle	13
2.5.1	Okta	13
2.5.2	JWT	14
2.5.3	OAuth2	14

2.5.4 OpenID Connect	14
2.6 Entwicklungsumgebung und Versionskontrolle	14
2.6.1 Entwicklungsumgebung	15
2.6.2 Versionskontrolle	15
3 Implementierung	17
3.1 Startseite	17
3.2 Online-Shopping	17
3.3 Bezahlprozess	18
4 Ergebnisse und Analyse	19
5 Zusammenfassung und Ausblick	20
Literaturverzeichnis	21
Glossar	23
Selbstständigkeitserklärung	24

Abbildungsverzeichnis

2.1	Beispielhafte Dateistruktur einer Angular-Anwendung mit verschiedenen Komponenten	5
-----	--	---

Tabellenverzeichnis

Einleitung und Problemstellung

Hier werden folgende Aspekte berücksichtigt:

- Relevanz für ein E-Commerce Shop.
- Aktueller Stand im Markt: Welche ähnlichen Anwendungen gibt es und wie unterscheidet sich unsere Anwendung von den bisherigen?
- Problem-/Fragestellung und Zielsetzung für ein zu entwickelndes

1.1 Überblick

ShopNook ist ein internetbasierter Marktplatz, der darauf abzielt, Käufern einen großartigen und angenehmen Einkaufsprozess zu bieten. Mit dieser Anwendung können Käufer ganz einfach durch die verschiedenen verfügbaren Produkte gehen, mehrere davon in ihren Einkaufskörben sammeln und sie sicher bezahlen. Das Design von ShopNook ist attraktiv und auf jeder Bildschirmgröße zugänglich, so dass jeder Nutzer, der die Website besucht, unabhängig von seinen Vorlieben bei den Geräten angesprochen wird. Die Website verfügt außerdem über eingebaute Funktionen wie ein Bestandskontrollsystem, Admin-Rollen wie z. B. einen Editor für Produktdetails und andere sowie Käuferprivilegien.

1.2 Globale Anforderungen

1.2.1 Funktionale Anforderungen

Die App wird über alle notwendigen Funktionen verfügen, um ein reibungsloses Einkaufserlebnis zu gewährleisten. Die Kunden werden die Möglichkeit haben, sich sicher zu registrieren, einzuloggen und einen Produktkatalog zu erkunden. Zu jedem Produkt werden vollständige Details wie Name, Beschreibung, Preis und Bilder angezeigt. Die Kunden können schnell Artikel in ihren Einkaufskorb legen, den Inhalt ändern und zur Zahlung übergehen. Sichere Kreditkartenzahlungen werden während des Kaufvorgangs über die Stripe-API abgewickelt. Administratoren können die Waren überwachen und die Bestellungen im Auge behalten, um sicherzustellen, dass das Online-Geschäft gut funktioniert.

1.2.2 Nicht-funktionale Anforderungen

Die App wird effizient mit gleichzeitigen Nutzern umgehen und die Ladezeiten der Seite sind minimal. HTTPS-Verschlüsselung und JWT-basierte Authentifizierung stellen die Sicherheit in den Vordergrund. Die Einheitlichkeit der Geräte wird durch eine reaktionsschnelle und einfach zu bedienende Schnittstelle gewährleistet.

1.2.3 Technische Anforderungen

Die vollwertige E-Commerce-App wird mit npm für JavaScript-Abhängigkeiten und Maven für die Java Abhängigkeiten und Build-Prozesse entwickelt. Im Frontend wird Angular verwendet, um eine dynamische und reaktionsschnelle Schnittstelle für die Benutzer bereitzustellen, während im Backend das Spring Boot-Framework verwendet wird, um RESTful APIs zu erstellen. MySQL wird die Datenbank sein, die Benutzer-, Produkt- und Bestelldaten speichert. Git und GitHub werden für die Versionskontrolle verwendet, um Änderungen zu verwalten und die Teamarbeit zu erleichtern.

Methodologie und Systementwurf

Hier werden über folgende Punkte diskutiert:

- Die Entwicklungskonzeption, die wir während der Implementation der Anwendung benutzt haben, sowie die Tools, Technologien und Methodologien.
- Überblick über Spring Boot und seine wichtigste Funktionalitäten, die auch in dem Projekt angewendet sein werden.
- Detaillierte Erklärung der Struktur und Design der Anwendung (Bsp: Analyse-/Entwurfsdiagramm)
- Datenbanken, UI-Design und unterschiedliche Komponenten des Systems.
- Wie Spring Boot die Entwicklung und Implementation der verschiedenen Module vereinfacht.

2.1 Entwurf und Konzeption

In der Softwareentwicklung spielen Entwurf und Konzeption eine entscheidende Rolle. Diese Phase des Entwicklungsprozesses befasst sich mit der Strukturierung und Planung von Systemen, bevor die eigentliche Implementierung beginnt.

Ziel ist es, ein klares und verständliches Modell zu erstellen, das die Anforderungen und Funktionen eines Systems abbildet. In diesem Kapitel werden UML und einige Diagrammtypen vorgestellt.

2.1.1 UML

Die Unified Modeling Language (UML) ist ein wesentliches Werkzeug im Bereich Entwurf. UML ist eine standardisierte Modellierungssprache, die eine Vielzahl von Diagrammen bietet, um unterschiedliche Aspekte eines Systems darzustellen. Diese Diagramme helfen dabei, komplexe Systeme zu visualisieren, zu dokumentieren und zu kommunizieren [Bel23a].

2.1.2 Klassendiagramm

2.1.3 Use-Case Diagramme

2.2 Front-End Technologien

Dieses Kapitel befasst sich mit Front-End-Technologien wie HTML, CSS, TypeScript und Angular, die für die Erstellung interaktiver, reaktionsfähiger und visuell ansprechender Benutzeroberflächen in unserer E-Commerce-Anwendung unerlässlich sind.

2.2.1 HTML/CSS

HTML¹ und CSS² sind die grundlegenden Technologien zur Erstellung und Gestaltung von Webseiten. HTML liefert die Struktur und den Inhalt einer Webseite, während CSS für die visuelle Darstellung, Layout, Farben und Schriftarten, verwendet wird. Sie ermöglichen es optisch ansprechende und gut strukturierte Webseiten zu erstellen [HTM24].

2.2.2 Typescript

TypeScript³ ist eine stark typisierte Programmiersprache, die auf JavaScript aufbaut und statische Typdefinitionen hinzufügt. Sie soll die Entwicklung umfangreicher Anwendungen überschaubarer machen, indem sie es den Entwicklern ermöglicht, Fehler schon früh im Entwicklungsprozess zu erkennen, wodurch Fehler reduziert und die Codequalität verbessert werden. [Shu22].

Die wichtigsten Vorteile von TypeScript sind:

- **Statische Typisierung:** Die statische Typisierung ermöglicht es Entwicklern, Variablentypen explizit zu definieren, was zu einer besseren Tooling-Unterstützung führt, z. B. bei der Code-Vervollständigung und beim Refactoring. Es hilft auch bei der Identifizierung von typbezogenen Fehlern während der Kompilierungszeit und nicht zur Laufzeit.
- **Wartbarkeit:** Durch die Hinzufügung von Typdefinitionen wird der Code selbstdokumentierender und leichter verständlich, was in großen Codebasen, in denen mehrere Entwickler zusammenarbeiten, entscheidend ist.

Durch die Wahl von TypeScript für das ShopNook-Projekt wurde es sichergestellt, dass das Frontend der Anwendung robust, wartbar und skalierbar ist und die hohen Anforderungen an eine professionelle E-Commerce-Plattform erfüllt.

¹ HyperText Markup Language

² Cascading Style Sheets

³ <https://www.typescriptlang.org>

2.2.3 Angular

Angular⁴ ist ein Open-Source-Framework für Webanwendungen, das von Google entwickelt und gepflegt wird. Es wird für die Erstellung dynamischer, einseitiger Anwendungen (SPAs)⁵ mit TypeScript und HTML verwendet. Das Framework bietet eine robuste Plattform für die Entwicklung komplexer Anwendungen, indem es einen umfassenden Satz von Tools und Funktionen wie Datenbindung, Dependency Injection und eine modulare Architektur bietet [Ang24a].

Eine der Hauptstärken von Angular ist seine komponentenbasierte Struktur, die es Entwicklern ermöglicht, wiederverwendbare UI-Komponenten zu erstellen, die die Wartbarkeit und Skalierbarkeit verbessern. Darüber hinaus bietet Angular leistungsstarke Funktionen wie reaktive Programmierung mit RxJS⁶, Zustandsverwaltung und ein reichhaltiges Ökosystem von Bibliotheken, was es zu einer idealen Wahl für Anwendungen auf Unternehmensebene macht.

2.2.3.1 Komponentenbasierte Architektur

Die komponentenbasierte Architektur von Angular gliedert die Anwendung in kleine, in sich geschlossene Einheiten, die als Komponenten bezeichnet werden. Jede Komponente kapselt einen bestimmten Teil der Benutzeroberfläche (UI) und die damit verbundene Logik [Ang24b].

Komponenten sind die wichtigsten Bausteine für Angular-Anwendungen. Wie es in der Abbildung 2.1 bezeichnet wurde besteht jede Komponente aus:

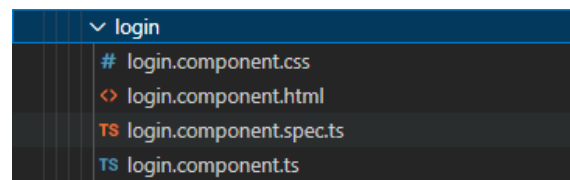


Abbildung 2.1: Beispielhafte Dateistruktur einer Angular-Anwendung mit verschiedenen Komponenten

- einer Komponentendatei `<component-name>.component.ts`

⁴ <https://angular.io>

⁵ Single Page Application

⁶ <https://rxjs.dev>

- einer Vorlagedatei `<component-name>.component.html`
- einer CSS-Datei `<component-name>.component.css`
- Einer Datei mit Prüfvorschriften `<component-name>.component.spec.ts`

Dieser modulare Ansatz bringt mit sich mehrere Vorteile wie Wiederverwendbarkeit und Wartbarkeit.

2.2.3.2 Single Page Application (SPA)

Angular eignet sich besonders gut für die Erstellung von Single Page Applications (SPAs). In einer SPA lädt die gesamte Anwendung eine einzige HTML-Seite und aktualisiert den Inhalt dynamisch, wenn der Benutzer mit der Anwendung interagiert, ohne dass eine komplette Seite neu geladen werden muss [Ang24c].

Dieser Ansatz bietet mehrere Vorteile:

- **Verbesserte Benutzerfreundlichkeit:** SPAs bieten eine reibungslosere und schnellere Benutzererfahrung, da nur die notwendigen Teile der Seite aktualisiert werden, anstatt die gesamte Seite neu zu laden.
- **Geringere Serverlast:** Sie entlasten den Server, da weniger Ganzseitenanfragen gestellt werden, was zu einer effizienteren Nutzung der Serverressourcen führt.

Durch die Nutzung der komponentenbasierten Architektur und der SPA-Funktionen von Angular kann die Anwendung ShopNook eine nahtlose und reaktionsschnelle Benutzererfahrung bieten, die für die Kundenbindung und -zufriedenheit entscheidend ist.

2.3 Back-End Technologien

In diesem Kapitel werden Back-End-Technologien untersucht, wobei der Schwerpunkt auf Spring Boot liegt, um robuste, skalierbare und sichere serverseitige Logik und APIs für unsere E-Commerce-Anwendung zu erstellen.

2.3.1 Java

Java ist eine weit verbreitete Programmiersprache, die für ihre Plattformunabhängigkeit, Stabilität und umfassende Bibliotheken bekannt ist. Aufgrund ihrer Vielseitigkeit und Leistung wird Java häufig für die Entwicklung von Back-End-Anwendungen verwendet [Jav24]. In der E-Commerce-Anwendung (ShopNook) wird Java genutzt, um eine robuste und skalierbare serverseitige Logik zu gewährleisten.

2.3.2 REST-API

REST⁷ ist ein Architekturstil für die Entwicklung vernetzter Anwendungen. Er basiert auf einem zustandslosen, Client-Server- und cachefähigen Kommunikati-

⁷ Representational State Transfer

onsprotokoll, und in fast allen Fällen wird das HTTP-Protokoll verwendet. REST-APIs sind so konzipiert, dass sie einfach, leichtgewichtig und skalierbar sind, was sie zu einer beliebten Wahl für Webdienste macht [RES24].

2.3.2.1 Einführung in REST

Angelehnt an [RES24] bieten REST-APIs eine Möglichkeit, über HTTP auf die Funktionalität und Daten einer Anwendung zuzugreifen. Sie folgen den Prinzipien von REST, die auf Ressourcen und deren Repräsentationen basieren. Jede Ressource wird durch eine eindeutige URI identifiziert und kann durch standardisierte HTTP-Methoden manipuliert werden:

- GET: Abrufen von Ressourcen
- POST: Erstellen neuer Ressourcen
- PUT: Aktualisieren bestehender Ressourcen
- DELETE: Löschen von Ressourcen

REST-APIs sind also aufgrund ihrer Architektur und Funktionsweise weit verbreitet und bieten eine Reihe von Vorteilen:

- **Skalierbarkeit:** Durch das stateless Design können REST-APIs leicht skaliert werden. Jeder HTTP-Request enthält alle notwendigen Informationen, um ihn zu verarbeiten, ohne dass der Server den vorherigen Zustand kennen muss.
- **Flexibilität:** REST-APIs sind flexibel und können mit verschiedenen Datenformaten arbeiten. JSON ist das gebräuchlichste Format, da es leichtgewichtig und gut lesbar ist.
- **Interoperabilität:**⁸ REST-APIs nutzen standardisierte HTTP-Methoden, was ihre Interoperabilität mit verschiedenen Clients und Plattformen gewährleistet.
- **Leichte Integration:** REST-APIs lassen sich leicht in bestehende Systeme integrieren, da sie auf bekannten Webstandards basieren.

Um die Sicherheit von REST-APIs in der ShopNook-Plattform weiter zu gewährleisten, spielt die Implementierung von HTTPS in Kombination mit SSL/TLS eine entscheidende Rolle, da diese Technologien eine sichere und verschlüsselte Kommunikation zwischen dem Client und dem Server ermöglichen.

2.3.3 HTTPS und SSL/TLS

HTTPS ist die sichere Version von HTTP, dem Protokoll, über das die Daten zwischen dem Browser des Kunden und der Website, mit der er verbunden ist, gesendet werden. Das „S“ am Ende von HTTPS steht für „Secure“, was bedeutet, dass die gesamte Kommunikation zwischen dem Kunden und dem Server verschlüsselt ist [HTT24].

SSL/TLS sind allerdings Verschlüsselungsprotokolle, die eine sichere Kommunikation über ein Computernetz ermöglichen. SSL war das ursprüngliche Protokoll,

⁸ Interoperabilität ist die Fähigkeit verschiedener Systeme oder Software, zusammenzuarbeiten und Informationen nahtlos auszutauschen[wik].

aber es wurde zugunsten von TLS, das sicherer und effizienter ist, veraltet [Bel23b]. Diese Protokolle bieten mehrere wichtige Sicherheitsfunktionen, die im Folgenden näher erläutert werden:

- **Verschlüsselung der Daten:** SSL und TLS verschlüsseln die zwischen dem Client und dem Server übertragenen Daten und stellt sicher, dass die Daten, selbst wenn sie abgefangen werden, nicht von Unbefugten gelesen werden können.
- **Server-Authentifizierung:** Diese Protokolle überprüfen auch die Identität des Servers und stellen sicher, dass die Clients mit einem legitimen Server und nicht mit einem Betrüger kommunizieren.
- **Datenintegrität:** Sie bieten auch Datenintegrität, indem es sicherstellt, dass die Daten während der Übertragung nicht manipuliert wurden.

In der Anwendung wurde eine HTTPS Konfiguration (siehe 26) erstellt, um eine sichere Kommunikation zwischen Clients und dem Server zu gewährleisten. Dazu wurde der Server so eingestellt, dass er auf Port 8443 auf HTTPS-Datenverkehr wartet. Der Konfigurationsprozess beinhaltet die Aktivierung der SSL-Unterstützung, die für die Verschlüsselung der über das Netzwerk ausgetauschten Daten unerlässlich ist.

Wir haben eine Keystore-Datei im PKCS12-Format (**shopnook-keystore.p12**) verwendet, in der die für die Verschlüsselung erforderlichen SSL/TLS-Zertifikate sicher gespeichert sind. Der Keystore ist durch ein Passwort geschützt (**server.ssl.keystore-password=secret**), so dass der Zugriff auf die kryptografischen Schlüssel nur autorisierten Prozessen vorbehalten ist.

Innerhalb des Schlüsselspeichers wird das Zertifikat durch den Alias **shopnook** identifiziert, auf den in der Konfiguration verwiesen wird, um die SSL-Vorgänge des Servers mit dem richtigen Zertifikat zu verknüpfen. Diese Einrichtung stellt sicher, dass alle zwischen dem Client und dem Server übertragenen Daten verschlüsselt werden, was einen robusten Schutz gegen Abhör- und Man-in-the-Middle-Angriffe bietet.

Darüber hinaus ermöglicht die Konfiguration eine einfache Anpassung an unterschiedliche Umgebungen. So kann beispielsweise der Port der Anwendung je nach Einsatzumgebung geändert werden, indem die Eigenschaft **server.port** angepasst wird. Für die QA-Demo-Umgebung ist der Port auf **9898** eingestellt, der durch Umschalten der Kommentarzeilen aktiviert werden kann.

Durch die sorgfältige Konfiguration dieser SSL-Einstellungen stellen wir sicher, dass ShopNook den Industriestandards für Sicherheit entspricht.

```
1      #####
2      #
3      # HTTPS configuration
4      #
5      #####
6      #Define the web server's listening port for HTTPS traffic
7      server.port=8443
8
9      #QA Demo Port
10     #server.port=9898
11
12     #Activate SSL support to secure the application with HTTPS
13     server.ssl.enabled=true
14
15     #Specify the key alias used within the keystore for SSL
16     server.ssl.key-alias=shopnook
17
18     #Keystore path
19     server.ssl.key-store=classpath:shopnook-keystore.p12
20
21     #Password to unlock the keystore and access the SSL keys
22     server.ssl.key-store-password=secret
23
24     #format of the keystore file
25     server.ssl.key-store-type=PKCS12
```

Listing 2.1: Implementierung von HTTPS und SSL Konfiguration

Durch die Implementierung von HTTPS mit SSL/TLS hält sich ShopNook an die Industriestandards für Datensicherheit, um seine Nutzer zu schützen und das Vertrauen zu erhalten. Dies ist ein entscheidender Aspekt des Backends der Anwendung, insbesondere für die Wahrung der Vertraulichkeit und Integrität sensibler Daten bei Transaktionen.

2.3.4 Spring Boot

Spring Boot ist ein Framework, das auf dem Spring Framework aufbaut und speziell entwickelt wurde, um schnelle, effiziente und skalierbare Anwendungen zu erstellen. Es bietet eine Vielzahl von Features, die den Entwicklungsprozess beschleunigen und vereinfachen, insbesondere für Java-basierte Webanwendungen und Microservices.

2.3.4.1 Warum wurde Spring Boot ausgewählt ?

Spring Boot wurde aufgrund der breiten Unterstützung in der Entwicklergemeinschaft ausgewählt. Hier sind einige der Hauptgründe:

- **Produktivität:** Das Framework ermöglicht es auf das Schreiben von Geschäftslogik zu konzentrieren, anstatt sich um die Konfiguration von Technologien zu kümmern.
- **Microservices:** Es eignet sich hervorragend für die Entwicklung von Microservices-Architekturen, indem es Server wie Tomcat bietet, sodass die Anwendungen ohne externen Server laufen können.
- **Integration:** Es lässt sich nahtlos in andere Spring-Projekte und eine Vielzahl von Datenbanken integrieren.

Das Framework bietet auch viele Funktionalitäten, die es von anderen abheben, es hat viele weitere Vorteile, die hier genannt werden:

- **Auto-Konfiguration:** Die Autokonfigurationsfunktion von Spring Boot konfiguriert Ihre Anwendung automatisch anhand der Abhängigkeiten, die Sie dem Projekt hinzugefügt haben. Dadurch wird die Notwendigkeit einer manuellen Konfiguration minimiert und die Entwicklung beschleunigt.
- **Eigenständige Anwendungen:** Spring Boot-Anwendungen können als eigenständige Java-Anwendungen verpackt werden, was die Bereitstellung einfacher und konsistenter macht.
- **Produktionstaugliche Funktionen:** Das Framework umfasst zahlreiche produktionsreife Funktionen wie Zustandsprüfungen, Metriken und externalisierte Konfiguration.

2.3.4.2 Wie funktioniert Spring Boot ?

1. **Initial Setup:** Mit Spring Initializr kann man schnell ein neues Spring Boot-Projekt mit allen erforderlichen Abhängigkeiten und Konfigurationen initialisieren.
2. **Main Application Class:** Jede Spring Boot-Anwendung hat eine Hauptklasse, die mit `@SpringBootApplication` annotiert ist. Diese Annotation ist eine Kombination aus `@Configuration`, `@EnableAutoConfiguration` und `@ComponentScan`.

```
1 @SpringBootApplication
2 public class SpringBootEcommerceApplication {
3     public static void main(String[] args) {
4         SpringApplication.run(SpringBootEcommerceApplication.class, args);
5     }
6 }
```

Listing 2.2: Main-Application-Class-Implementierung in Java

3. **Application Properties:** Spring Boot ermöglicht eine einfache Konfiguration durch application.properties-Datei. Dadurch wird die Konfiguration externalisiert, was die Verwaltung verschiedener Umgebungen erleichtert.

```
1 spring.datasource.driver-class-name=com.mysql.cj.jdbc.Driver
2 spring.datasource.url=jdbc:mysql://localhost:3306/full-stack-ecommerce?
3 useSSL=false&useUnicode=yes&characterEncoding=UTF-8&allowPublicKeyRetrieval=
4 true&serverTimezone=UTC
5 spring.datasource.username=username
6 spring.datasource.password=password
7 spring.jpa.properties.hibernate.dialect=org.hibernate.dialect.MySQL8Dialect
8 spring.data.rest.base-path=/api
```

Listing 2.3: Implementierung von Application.properties Datei

2.3.4.3 Spring Security

Spring Security ist ein robustes und anpassungsfähiges Framework, das für die Authentifizierung und Zugriffskontrolle entwickelt wurde und sich zum Standard für die Absicherung von mit Spring erstellten Anwendungen entwickelt hat.

Spring Security ist ein Framework, das sowohl die Authentifizierung als auch die Autorisierung von Java-Anwendungen übernimmt. Seine Stärke liegt in der Flexibilität, die es erlaubt, es leicht zu erweitern, um spezifische Anforderungen zu erfüllen.

Das Framework bietet eine Reihe von Funktionen, darunter umfassende Unterstützung für Authentifizierung und Autorisierung, Schutz vor verschiedenen Angriffen wie Session Fixation, Clickjacking und Cross-Site Request Forgery, Integration mit der Servlet API und optionale Kompatibilität mit Spring Web MVC [Sprd].

Zum Schutz der Endpunkte für Kundenbestellungen wurde Spring Security mit OAuth2-Authentifizierung implementiert, wobei JWT zur Gewährleistung eines sicheren Zugriffs verwendet wird. Die Einrichtung umfasste die Konfiguration von CORS zur Verwaltung von Herkunftsübergreifenden Anfragen und die Anpassung von Sicherheitseinstellungen wie die Deaktivierung des CSRF-Schutzes und die Handhabung der Inhaltsaushandlung. Dieser Ansatz gewährleistet robuste Sicherheit, während er verschiedene Inhaltstypen unterstützt und die gemeinsame Nutzung von Ressourcen über verschiedene Ursprünge hinweg effektiv handhabt.

2.3.5 Stripe API

2.4 Datenbankstruktur

In diesem Abschnitt wird die Datenbankstruktur der Webanwendung untersucht, um ein umfassendes Verständnis für die Organisation, den Zugriff und die Verwaltung der Daten zu vermitteln. Der Schwerpunkt liegt auf dem relationalen Datenbankmodell und den spezifischen Technologien und Frameworks, die zur Handhabung der Datenpersistenz und der Transaktionen verwendet werden. Dabei wird MySQL als das gewählte Datenbanksystem zusammen mit Spring Data JPA für eine nahtlose Dateninteraktion untersucht. In den folgenden Unterabschnitten werden diese Aspekte im Detail behandelt, wobei relationale Datenbanken, die Auswahl von MySQL, Datenpersistenz und Transaktionsmanagement sowie die Integration von MySQL mit Spring Boot behandelt werden.

2.4.1 Übersicht über relationale Datenbanken und Auswahl von MySQL

Die Daten in einer relationalen Datenbank sind in Tabellen mit Spalten und Zeilen organisiert, und auch die Primär- und Fremdschlüssel werden verwendet, um die Beziehungen zwischen den Tabellen herzustellen. Dieser Ansatz ist ideal für

E-Commerce-Anwendungen, da er komplexe Abfragen und aussagekräftige Daten verarbeiten kann. Produktlieferungen, Auftragstransaktionen und Kundendaten werden alle ordnungsgemäß verwaltet. Die Möglichkeit, Tabellen zu verknüpfen, erleichtert umfassende Analysen, einschließlich der Nachverfolgung von Kaufdatensätzen und der Bestandskontrolle, während die Einhaltung von ACID-Eigenschaften eine zuverlässige Transaktionsverarbeitung gewährleistet, die für die Auftragsabwicklung und das Zahlungsmanagement entscheidend ist. Relationale Datenbanken wie MySQL bieten die Robustheit und Konsistenz, die für einen sicheren und produktiven Online-Shopping-Betrieb erforderlich sind [IBM].

2.4.2 Datenbankschemaentwurf mit Spring Data JPA

Ziel dieses Abschnitts ist es, zu erörtern, wie Spring Data JPA den Entwurf und die Verwaltung von Datenbankschemata vereinfacht. Es wird gezeigt, wie Spring Data JPA es Entwicklern ermöglicht, Entitäten und Beziehungen innerhalb eines Datenbankschemas abzubilden und zu verwalten, und wie es die Komplexität des Datenzugriffs durch seine Repository-Schicht abstrahiert.

Spring Data JPA vereinfacht den Entwurf von Datenbankschemata, indem es Entwicklern ermöglicht, Java-Klassen mithilfe von Annotationen wie `@Entity`, `@Id` und `@OneToMany` auf Datenbanktabellen abzubilden. Diese Annotationen übernehmen automatisch die Schemaerstellung und -verwaltung und stellen sicher, dass die Datenbankstruktur mit dem Domänenmodell der Anwendung übereinstimmt [Sprc, Bae].

Die Repository-Schicht in Spring Data JPA abstrahiert die Komplexität des Datenzugriffs und bietet integrierte CRUD-Operationen über Schnittstellen wie `JpaRepository`. Dies macht manuelle SQL-Abfragen überflüssig und rationalisiert die Datenbankinteraktionen, so dass sich die Entwickler auf die Geschäftslogik konzentrieren können [Sprb, Spra].

2.4.3 Datenpersistenz und Transaktionen

In diesem Abschnitt wird erläutert, wie Spring Boot und Hibernate die Datenpersistenz handhaben. Der Schwerpunkt liegt dabei auf CRUD-Operationen, der Rolle des `EntityManager` und der Interaktion des Hibernate ORM mit MySQL.

CRUD-Operationen werden mit Spring Boot und Hibernate verwaltet. Der `EntityManager` ist in diesem Prozess von zentraler Bedeutung und ermöglicht das Erstellen, Abrufen, Aktualisieren und Löschen von Entitäten. Er verwaltet auch den Lebenszyklus von Entitäten innerhalb von Transaktionen und stellt sicher, dass Änderungen bei Bedarf ordnungsgemäß übertragen oder zurückgenommen werden [Bae24].

Hibernate ORM wird verwendet, um Java-Objekte auf Datenbanktabellen abzubilden, was die Interaktion mit der MySQL-Datenbank vereinfacht. Dieses ORM-Framework macht manuelles SQL überflüssig und bietet einen objektorientierten Ansatz für Datenbankoperationen [Hib].

2.4.4 MySQL-Workbench und SQL

In diesem Abschnitt wird die MySQL Workbench als Werkzeug für den Entwurf und die Verwaltung von Datenbanken und SQL als Sprache für die Erstellung von Abfragen und die Verwaltung der Datenbank vorgestellt.

MySQL Workbench wurde zur Visualisierung des Datenbankschemas eingesetzt und ermöglichte eine intuitive Gestaltung und Verwaltung der Datenbankstrukturen. Sie erleichterte die Erstellung und Änderung von Tabellen, Beziehungen und Indizes. Darüber hinaus wurde SQL verwendet, um Abfragen für Tests und die Datenbankverwaltung auszuführen, einschließlich Aufgaben wie Datenmanipulation und Schemaaktualisierungen [myS].

2.4.5 Datenbankverbindung und -konfiguration in Spring Boot

In diesem Abschnitt wird erläutert, wie die Datenbank innerhalb der Spring Boot-Anwendung verbunden und konfiguriert wird.

Die Datenbankverbindung wird in der Datei `application.properties` konfiguriert. Zu den wichtigsten Eigenschaften gehören die JDBC-URL, der Name der Treiberklasse und die Anmeldeinformationen, wie in Listing 2.2 dargestellt.

2.5 Authentifizierungs- und Autorisierungsprotokolle

In der modernen digitalen Landschaft ist die Gewährleistung eines sicheren Zugriffs auf Ressourcen von entscheidender Bedeutung. In diesem Abschnitt werden die wichtigsten Protokolle und Standards zur Verwaltung der Benutzerauthentifizierung und -autorisierung untersucht, darunter JWT, OAuth2 und OpenID Connect.

2.5.1 Okta

Okta verbindet Benutzer mit jeder Anwendung über alle Geräte hinweg. Es ist ein Cloud-basierter Identitätsmanagement-Service, der mit verschiedenen lokalen Systemen kompatibel ist. Okta bietet der IT-Abteilung die Möglichkeit, den Zugriff auf Anwendungen und Geräte über eine sichere, zuverlässige und gut geprüfte Cloud-Plattform zu verwalten, mit einer tiefen Integration in lokale Systeme und Verzeichnisse.

Okta bietet Funktionen wie Provisioning, Single Sign-On (SSO), Active Directory (AD) und LDAP-Integration, zentrales Nutzer-Deprovisioning, Multi-Faktor-Authentifizierung (MFA), mobiles Identitätsmanagement und anpassbare Sicherheitsrichtlinien. Diese Funktionen werden durch das Okta Integration Network (OIN) vereinheitlicht, das umfangreiche Integrationsoptionen bietet und SSO für alle Anwendungen ermöglicht, die Ihre Benutzer benötigen[OTb].

2.5.2 JWT

JWT ist ein offener Standard (RFC 7519) für die sichere Übertragung von Informationen in Form eines JSON-Objekts. Diese Informationen sind aufgrund der digitalen Unterzeichnung überprüfbar und vertrauenswürdig. JWTs können mit einem geheimen Schlüssel mit HMAC oder mit einem öffentlichen/privaten Schlüsselpaar mit RSA oder ECDSA signiert werden. Hier sind einige Situationen, in denen JSON-Web-Token von Vorteil sind:

- **Autorisierung:** JWTs werden in der Regel zur Authentifizierung verwendet. Nach der Anmeldung enthält jede Anfrage das JWT, das den Zugriff auf autorisierte Routen, Dienste und Ressourcen ermöglicht.
- **Informationsaustausch:** Mit JWTs werden Informationen sicher zwischen Parteien übertragen. Signierte JWTs bestätigen die Identität des Absenders und stellen sicher, dass der Inhalt unverändert bleibt, da die Signatur sowohl aus der Kopfzeile als auch aus der Nutzlast abgeleitet wird[JT].

2.5.3 OAuth2

OAuth 2.0, kurz für „Open Authorization“, ist ein Standard, der es einer Website oder Anwendung ermöglicht, im Namen eines Benutzers auf Ressourcen anderer Webanwendungen zuzugreifen. Er löste 2012 OAuth 1.0 ab und hat sich seitdem zum Industriestandard für die Online-Autorisierung entwickelt. OAuth 2.0 erleichtert den autorisierten Zugriff und schränkt gleichzeitig die Aktionen ein, die eine Client-Anwendung für den Benutzer auf Ressourcen durchführen kann, ohne die Anmeldedaten des Benutzers preiszugeben[OTa].

2.5.4 OpenID Connect

OpenID Connect ist ein Authentifizierungsprotokoll, das auf dem OAuth 2.0 Framework (IETF RFC 6749 und 6750) aufbaut. Es rationalisiert die Überprüfung der Benutzeridentität, indem es die von einem Autorisierungsserver durchgeführte Authentifizierung nutzt und Benutzerprofilinformationen in einer RESTful und interoperablen Weise bereitstellt.

OpenID Connect fördert ein Internet-Identitäts-Ökosystem durch einfache Integration, Sicherheits- und Datenschutzfunktionen, breite Client- und Gerätehilfe und die Möglichkeit für jede Einrichtung, als OpenID Provider (OP) zu agieren[OTc].

2.6 Entwicklungsumgebung und Versionskontrolle

In diesem Abschnitt werden die integrierten Entwicklungsumgebungen (IDEs) und Versionskontrollsysteme beschrieben, die im Rahmen des Projekts eingesetzt wurden. Er bietet einen Überblick über die für die Entwicklung ausgewählten IDEs und die Versionskontrollwerkzeuge, die zur effektiven Verwaltung von Codeänderungen eingesetzt wurden.

2.6.1 Entwicklungsumgebung

Dieser Unterabschnitt beschreibt die im Projekt verwendeten Entwicklungsumgebungen, wobei der Schwerpunkt auf IntelliJ IDEA und Visual Studio Code (VS Code) liegt. Er hebt die Funktionen und Vorteile der einzelnen IDEs bei der Unterstützung des Entwicklungsprozesses und der Steigerung der Produktivität hervor.

2.6.1.1 IntelliJ IDEA

IntelliJ IDEA ist bekannt für seinen leistungsstarken Code-Editor, der sich durch eine umfassende Anfangsindizierung beim Verstehen und Verwalten von Code auszeichnet. Diese Funktion ermöglicht es ihm, Fehler in Echtzeit zu erkennen, kontextbezogene Vorschläge zur Code-Vervollständigung anzubieten und sicheres Code-Refactoring durchzuführen, neben anderen Funktionen. Es ist mit einer umfangreichen Suite integrierter Entwicklerwerkzeuge ausgestattet und bietet robuste Unterstützung für verschiedene Spring-Frameworks sowohl in Java als auch in Kotlin. Dazu gehören Spring MVC, Spring Boot, Spring Integration, Spring Security und Spring Cloud. Zu den bemerkenswerten Vorteilen gehören intelligente Codierungshilfe, sofortige Navigation innerhalb des Spring-Codes, integrierte Entwicklungswerkzeuge und erweiterte Visualisierungsfunktionen [Jet].

2.6.1.2 Visual Studio Code

Visual Studio Code ist ein vielseitiger und effizienter Quellcode-Editor, der mit Windows, macOS und Linux kompatibel ist. Er bietet native Unterstützung für JavaScript, TypeScript und Node.js und verfügt über eine breite Palette von Erweiterungen für weitere Sprachen und Plattformen [Tead].

Da die Front-End-Entwicklung Angular, ein auf TypeScript basierendes Framework, nutzt, wurde Visual Studio Code als Entwicklungsumgebung gewählt. Die starke native Unterstützung für TypeScript erleichtert die effiziente und optimierte Projektentwicklung und macht zusätzliche Erweiterungen überflüssig. [Teac].

2.6.2 Versionskontrolle

In diesem Unterabschnitt werden die im Projekt eingesetzten Versionskontrollsysteme beschrieben, wobei der Schwerpunkt auf Git und GitHub liegt. Es wird erläutert, wie diese Tools die Codeverwaltung, die Zusammenarbeit und die Verfolgung von Änderungen während des gesamten Entwicklungsprozesses erleichtern haben.

2.6.2.1 Git

Git ist ein kostenloses und quelloffenes, verteiltes Versionskontrollsystem, das entwickelt wurde, um Projekte jeder Größe schnell und effizient zu verwalten. Es hat einen minimalen Platzbedarf und liefert eine außergewöhnlich schnelle Leistung.

Git übertrifft herkömmliche SCM-Tools wie Subversion, CVS, Perforce und ClearCase mit Funktionen wie kostengünstiger lokaler Verzweigung, benutzerfreundlichen Staging-Bereichen und flexiblen Arbeitsabläufen.

Eines der herausragenden Merkmale von Git ist sein Verzweigungsmodell, das es von fast allen anderen SCM-Tools unterscheidet. Git ermöglicht und fördert die Erstellung mehrerer lokaler Zweige, von denen jeder unabhängig funktionieren kann. Das Erstellen, Zusammenführen und Löschen von Zweigen geht schnell, nahtlos vonstatten und dauert oft nur Sekunden [Teaa].

2.6.2.2 GitHub

GitHub ist eine cloudbasierte Plattform zum Speichern, Freigeben und gemeinsamen Bearbeiten von Code. Die von Git unterstützten Kollaborationsfunktionen von GitHub ermöglichen es uns:

- Projekte zu präsentieren oder zu verbreiten.
- Verfolgen und Verwalten von Codeänderungen im Laufe der Zeit.
- Andere einladen, den Code zu überprüfen und Verbesserungen vorzuschlagen.
- Zusammenarbeit an Projekten ohne das Risiko, dass unbeabsichtigte Änderungen die Arbeit der anderen beeinträchtigen, bis die Änderungen integriert werden können. [Teab].

Implementierung

Hier wird das Implementationsprozess vorgestellt, zusätzlich werden die während der Implementation eingetretenen Probleme in die Diskussion eingebracht.

Die Frage: wie wurden diese Probleme behandelt?

Außerdem werden wir eine tiefe Darstellung und Beschreibung der Hauptfunktionalitäten der Anwendung (z.B : Warenkorb, Check Out Prozess, Produkt Listing...) geben.

3.1 Startseite

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua . At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

3.2 Online-Shopping

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua . At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

3.3 Bezahlprozess

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua . At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Ergebnisse und Analyse

Eine Darstellung und Analyse der Ergebnisse, sowie ein Vergleich von unserer entwickelten Anwendung mit schon im Markt existierenden E-Commerce Anwendungen.

Endlich werden wir die Strengths, Weaknesses, Opportunities und Threats (SWOT-Analyse) der entwickelten Anwendung ins Licht stellen und darüber diskutieren.

Zusammenfassung und Ausblick

Hier werden wir die Schwierigkeiten und Herausforderungen benennen, die wir bei der Konzeptentwicklung und auch bei der Umsetzung sehen. Welche Punkte sind offen geblieben? Was gilt es noch herauszufinden?

Literaturverzeichnis

- Ang24a. *Angular - Landing Page*. <https://angular.io>, 2024. Abgerufen am 02.06.2024.
- Ang24b. *Angular components overview*. <https://v17.angular.io/guide/component-overview>, 2024. Abgerufen am 18.08.2024.
- Ang24c. *Routing in single-page applications*. <https://angular.dev/guide/routing/router-tutorial>, 2024. Abgerufen am 18.08.2024.
- Bae. BAELDUNG: *JPA Entities*. <https://www.baeldung.com/jpa-entities/>. Abgerufen am 14.08.2024.
- Bae24. BAELDUNG: *EntityManager*. <https://www.baeldung.com/hibernate-entitymanager/>, 2024. Abgerufen am 14.08.2024.
- Bel23a. BELL, DONALD: *An introduction to the Unified Modeling Language*. <https://developer.ibm.com/articles/an-introduction-to-uml/>, 2023. Abgerufen am 26.07.2024.
- Bel23b. BELL, DONALD: *What is SSL/TLS: An In-Depth Guide*. <https://www.ssl.com/article/what-is-ssl-tls-an-in-depth-guide/>, 2023. Abgerufen am 19.08.2024.
- Hib. HIBERNATE: *Hibernate*. <https://hibernate.org/orm/what-is-an-orm/>. Abgerufen am 14.08.2024.
- HTM24. *HTML For Beginners*. <https://html.com>, 2024. Abgerufen am 02.06.2024.
- HTT24. *An overview of HTTP*. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview>, 2024. Abgerufen am 19.08.2024.
- IBM. IBM: *What is a relational database?* <https://www.ibm.com/topics/relational-databases/>. Abgerufen am 14.08.2024.
- Jav24. *What is Java technology and why do I need it?* https://www.java.com/en/download/help/whatis_java.html, 2024. Abgerufen am 19.08.2024.
- Jet. JETBRAINS: *The IDE for Spring developers*. <https://www.jetbrains.com/idea/spring/>. Abgerufen am 14.08.2024.
- JT. JWT-TEAM: *Introduction to JSON Web Tokens*. <https://jwt.io/introduction>. Abgerufen am 19. August 2024.
- myS. MYSQL: *MySQL Workbench Manual*. <https://dev.mysql.com/doc/workbench/en/wb-intro.html>. Abgerufen am 14.08.2024.

- OTa. OAUTH2-TEAM: *What is OAuth 2.0?* <https://auth0.com/intro-to-iam/what-is-oauth-2>. Abgerufen am 19. August 2024.
- OTb. OKTA-TEAM: *What is Okta and what does Okta do?* https://support.okta.com/help/s/article/what-is-okta?language=en_US. Abgerufen am 19. August 2024.
- OTc. OPENID-TEAM: *How OpenId Connect Works*. <https://openid.net/developers/how-connect-works/>. Abgerufen am 19. August 2024.
- RES24. *What is REST?* <https://www.codecademy.com/article/what-is-rest>, 2024. Abgerufen am 18.08.2024.
- Shu22. SHUBEL, MEREDITH: *Typescript*. <https://thenewstack.io/what-is-typescript/>, 2022. Abgerufen am 18.08.2024.
- Spra. SPRING: *JPA Query Methods*. <https://docs.spring.io/spring-data/jpa/reference/jpa/query-methods.html/>. Abgerufen am 14.08.2024.
- Sprb. SPRING: *JPA Repositories*. <https://docs.spring.io/spring-data/jpa/docs/1.6.0.RELEASE/reference/html/jpa.repositories.html/>. Abgerufen am 14.08.2024.
- Sprc. SPRING: *Spring Data JPA*. <https://www.ibm.com/topics/relational-databases/>. Abgerufen am 14.08.2024.
- Sprd. SPRING: *Spring Security*. <https://spring.io/projects/spring-security>. Abgerufen am 14. August 2024.
- Teaa. TEAM, GIT: *Git About*. <https://git-scm.com/about>. Abgerufen am 14. August 2024.
- Teab. TEAM, GITHUB: *GitHub About*. <https://docs.github.com/en/get-started/start-your-journey/about-github-and-git#about-github>. Abgerufen am 14. August 2024.
- Teac. TEAM, VISUAL STUDIO: *Using Angular in Visual Studio Code*. <https://code.visualstudio.com/docs/nodejs/angular-tutorial>. Abgerufen am 14. August 2024.
- Tead. TEAM, VISUAL STUDIO: *Visual Studio Code Overview*. <https://code.visualstudio.com/docs>. Abgerufen am 14. August 2024.
- wik. *Wikipedia: Interoperability*. <https://en.wikipedia.org/wiki/Interoperability>. Abgerufen am 27.07.2024.

A

Glossar

DisASter	Distributed Algorithms Simulation Terrain, eine Plattform zur Implementierung verteilter Algorithmen
DSM	Distributed Shared Memory
SQL	Structured Query Language
API	Application Programming Interface
JPA	Java Persistence API
MVC	Model-View-Controller
OAuth2	Open Authorization 2
JWT	JSON Web Token
CORS	Cross-Origin Resource Sharing
CSRF	Cross-Site Request Forgery
ACID	Atomicity, Consistency, Isolation, Durability
CRUD	Create, Read, Update, Delete
ORM	Object-Relational Mapping
JDBC-URL	Java Database Connectivity Uniform Resource Locator
IDE	Integrated Development Environment
SCM	Source Code Management
CVS	Concurrent Versions System
HTTPS	Hypertext Transfer Protocol Secure
UML	Unified Modeling Language
HTML	Hypertext Markup Language
CSS	Cascading Style Sheets
SPA	Single-Page Application
UI	User Interface
RxJs	Reactive Extensions for JavaScript
HTTP	Hypertext Transfer Protocol
URI	Uniform Resource Identifier
JSON	JavaScript Object Notation
REST API	Representational State Transfer

B

Selbstständigkeitserklärung

- ☐ Diese Arbeit wurde als Gruppenarbeit angefertigt. Meinen Anteil habe ich selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet.

Namen der Mitverfasser:

Meine eigene Leistung ist:

Datum

Unterschrift der Kandidatin/des Kandidaten

Datum

Unterschrift der Kandidatin/des Kandidaten