

Projekt Basel Coin

Modul 183



6. Januar 2024

Gruppe: Aimo, aZIN, Giorgio & Ilia

Abbildungsverzeichnis

Tabellenverzeichnis

Quellenverzeichnis

Versionsverzeichnis

|  |  |  |
| --- | --- | --- |
| Version | Datum | Änderung |
| 1  1.1  1.3 | 27.02.2024  27.02.2024  01.03.2024 | Projektdokumentation Erstelldatum  Erste Einträge in die Dokumentation  Letzter Eintrag in die Dokumentation |

Inhalt

[1 Einleitung 3](#_Toc160097120)

[1.1 Was war der Auftrag? 3](#_Toc160097121)

[2 Anwendung 3](#_Toc160097122)

[2.1 Login 3](#_Toc160097123)

[3 Sicherheitsfeatures der Basel Coin 4](#_Toc160097124)

[3.1 Feature 1 4](#_Toc160097125)

[3.2 Feature 2 4](#_Toc160097126)

[3.3 Feature 3 5](#_Toc160097127)

[3.4 Feature 4 6](#_Toc160097128)

# Einleitung

## Was war der Auftrag?

Unser Team wurde beauftragt, die Applikation "Basel Coin" zu erstellen, die zukünftig für die von Basel ausgegebene Kryptowährung zur Zahlung verwendet werden kann. Die Applikation muss folgende Sicherheitsmerkmale aufweisen:

* Ein sicheres Login mit Schutz gegen Injection - Angriffe.
* Effektives Session - Management mit Timeout - Funktionen.
* Protokollierung von Ereignissen mit Datum, Uhrzeit, Benutzer und Aktion.
* Validierung aller Eingabefelder, wie Login und Passwort.

Der Admin kann neue Benutzer anlegen und Kontostände verwalten, während die Benutzer sich einloggen, ihren Kontostand sehen und sich abmelden können. Zusätzlich zum Projekt müssen wir eine kurze und prägnante Dokumentation zu den Sicherheitsmerkmalen erstellen, um das Projektteam der Stadt Basel über die Sicherheit zu informieren.

# Anwendung

## Login

Um die Anwendung nutzen und den Benutzer identifizieren zu können, haben wir einen Login-Bereich erstellt. Dort kann man sich entweder mit seinem bestehenden Konto verbinden oder sich für ein neues anmelden.:

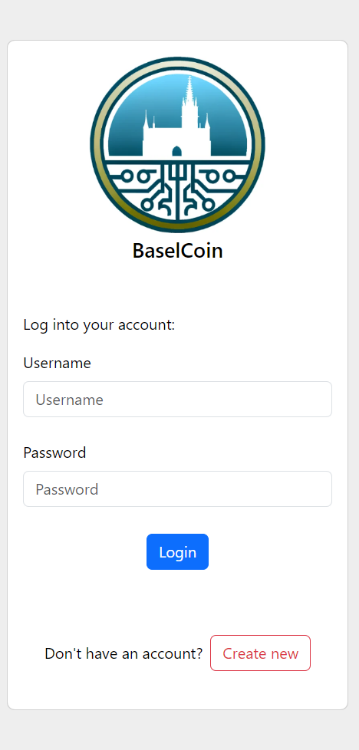
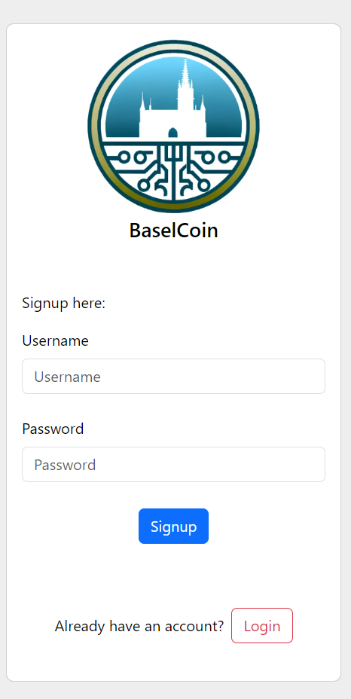


Abbildung 1: Login Ansicht der BaselCoin.

# Sicherheitsfeatures der Basel Coin

## Feature 1

Login mit Schutz gegen Injection: Die Anwendung verfügt über ein sicheres Login-System, das Benutzern ermöglicht, sich mit Benutzername und Passwort anzumelden. Dabei wird darauf geachtet, dass die Eingabefelder ordnungsgemäss validiert werden, um Injection-Angriffe zu verhindern, wie zum Beispiel SQL-Injection oder Cross-Site Scripting.

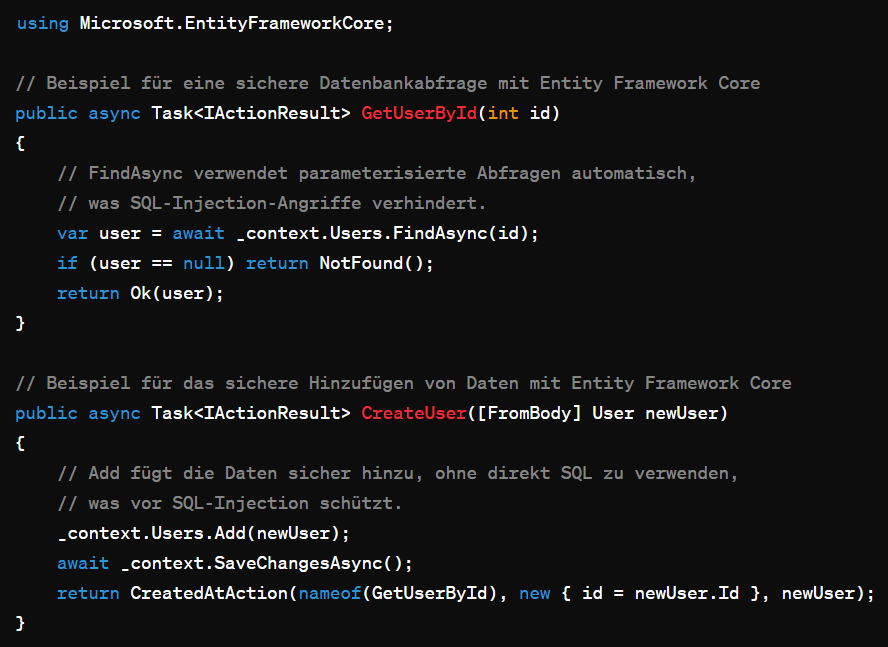
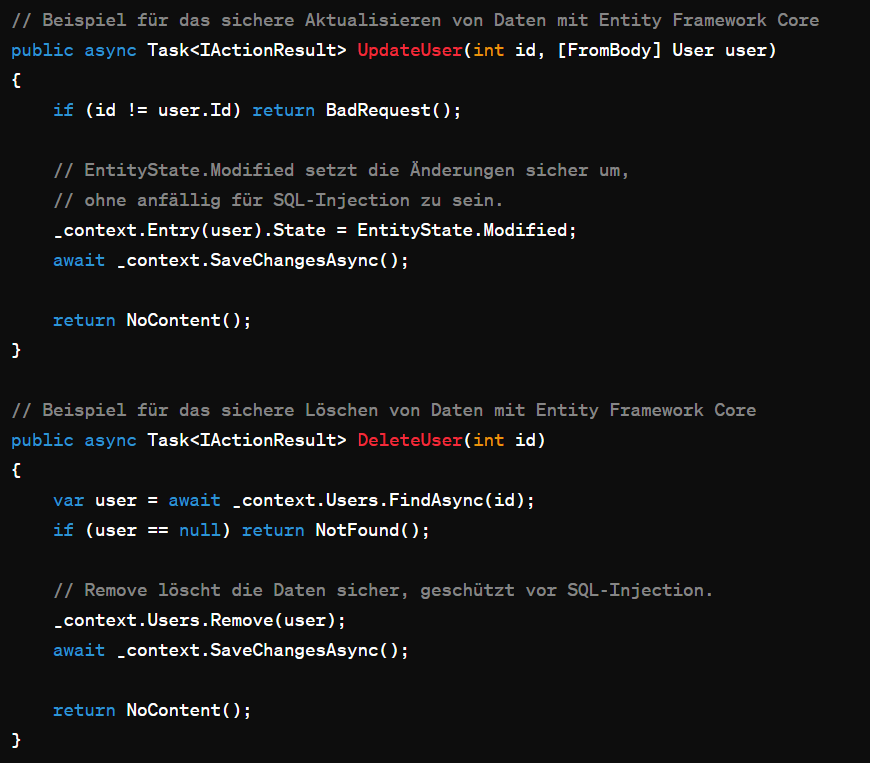


Abbildung 2: Codeabschnitt vom Feature 1.

## Feature 2

Effektives Session-Management: Das Session-Management der Anwendung stellt sicher, dass Benutzersitzungen sicher verwaltet werden. Es gibt Mechanismen, um die Sitzung nach einer bestimmten Zeit der Inaktivität (Idle Timeout) oder nach einer festgelegten Zeit (absolutes Timeout) automatisch zu beenden, um unbefugten Zugriff und Session-Hijacking zu verhindern.

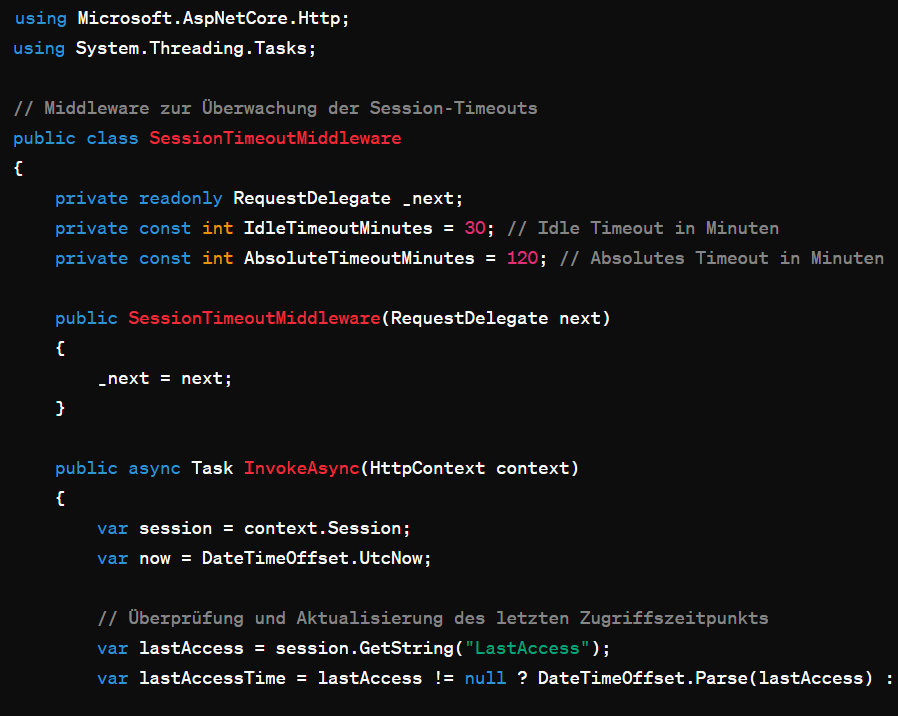
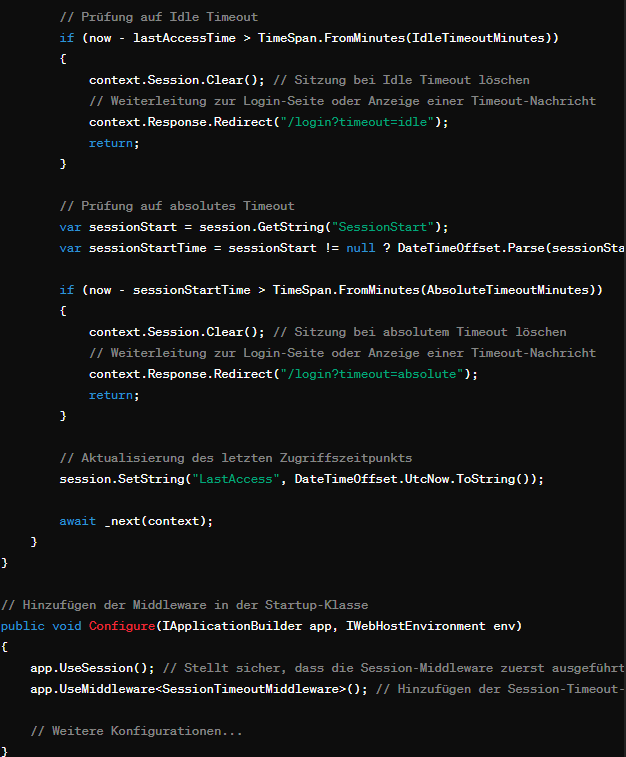


Abbildung 3: Codeabschnitt vom Feature 2.

## Feature 3

Protokollierung von Ereignissen: Die Anwendung protokolliert alle relevanten Ereignisse, wie beispielsweise Benutzeranmeldungen, Transaktionen oder Änderungen an Benutzerkonten. Jeder Eintrag im Applikationslog enthält Datum, Uhrzeit, den Typ des Ereignisses, den betroffenen Benutzer und die durchgeführte Aktion. Dadurch wird eine lückenlose Nachverfolgung von Aktivitäten ermöglicht, was die Sicherheit und Nachvollziehbarkeit der Anwendung verbessert.

## Feature 4

Input-Validierung: Alle Eingabefelder der Anwendung, einschliesslich Login, Passwort und andere Formularfelder, werden sorgfältig validiert, um sicherzustellen, dass nur gültige und erwartete Eingaben akzeptiert werden. Dadurch wird das Risiko von Angriffen, die auf fehlerhafte oder bösartige Eingaben abzielen, minimiert.

