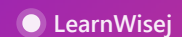


KI-Coding-Übung

Erstellen Sie das Beispielprojekt EnterpriseOps dieses Moduls mit ChatGPT oder Claude aus einem fertigen Prompt, der das Modell auf die Spezifikation des Moduls verweist – und prüfen, starten und erweitern Sie dann, was Sie erhalten, auch im Vergleich mit unserem eigenen Referenz-Build auf GitHub.



Dasselbe Modul – so gebaut, wie Sie in der Praxis wirklich bauen.

Alle anderen Abschnitte dieses Moduls erklären, wie „Sicherheitsarchitektur: Identität, SSO, Autorisierung, Audit und sicheres Deployment“ funktioniert. Dieser fordert Sie auf, es herzustellen: indem Sie einen Assistenten mit der Spezifikation des Moduls steuern und dann prüfen, ob das Ergebnis läuft und tut, was die Lab-Aufgabe beschreibt. Es ist der Arbeitsablauf, den Sie in echten Projekten nutzen werden – geübt an etwas, dessen richtige Lösung Sie bereits kennen.

Worum Sie bitten

Ergänzen Sie eine Simulation der Enterprise-Authentifizierung, das Mapping von Claims auf Berechtigungen, die Durchsetzung von Mandantenrollen, Autorisierung auf Service-Ebene, ein Review für sicheres HTML, eine Freigabe für Exporte und Audit-Logging für sensible Aktionen.

Das Modul verlangt diese Ergebnisse, und der Prompt unten fordert genau diese vom Assistenten an:

- ✓ Design des Identitäts-Mappings
- ✓ Berechtigungsmatrix
- ✓ Implementierung des Berechtigungsservices
- ✓ Bildschirm für das Audit-Log
- ✓ Checkliste zur Sicherheitshärtung

Warum es so aufgebaut ist

Eine serverseitige Architektur verkleinert viele Angriffsflächen im Browser, doch anspruchsvolle Systeme brauchen trotzdem eine Integration von Identitäten, Autorisierung auf Service-Ebene, Audit-Trails, sicheres Rendering und eine sichere Betriebskonfiguration.

Diese Begriffe muss der Assistent richtig verwenden. Geht die Antwort nachlässig mit ihnen um, hat er das Modul nicht verstanden:

Begriff	Was er hier bedeutet
OIDC/SSO-Grenze	Die Stelle, an der ein externer Identity Provider der Anwendung eine verifizierte Identität übergibt. Alles jenseits dieser Grenze liegt in der Verantwortung der Anwendung.
Claims-Mapping	Die Übersetzung providerspezifischer Claims in die eigenen Rollen und Berechtigungen der Anwendung, damit der Autorisierungscode nie vom Format eines bestimmten Identity Providers abhängt.
Berechtigungsservice	Ein einzelner Service, der beantwortet, ob der aktuelle Benutzer eine Aktion ausführen darf, sodass die Regel an einer Stelle liegt statt auf jedem Bildschirm.
Autorisierung auf Service-Ebene	Berechtigungen werden innerhalb der Anwendungsservices durchgesetzt, nicht nur in der UI, damit eine ausgeblendete Schaltfläche nie der einzige Schutz einer Operation ist.
Audit-Log	Ein manipulationssicherer Nachweis, wer wann was bei wichtigen Aktionen getan hat, damit sich Sicherheitsvorfälle untersuchen und Compliance-Anforderungen belegen lassen.
AllowHtml-Review	Die Prüfung jeder Stelle, an der ein Control rohes HTML zulässt, um sicherzustellen, dass von Benutzern gelieferte Inhalte bereinigt werden – denn ungeprüftes HTML ist ein Cross-Site-Scripting-Risiko.
Umgang mit Secrets	Connection Strings, Schlüssel und Tokens gehören in eine sichere Konfiguration oder einen Vault, niemals in die Versionsverwaltung oder in Einstellungen, die der Client sehen kann.
Sichere Header	HTTP-Antwortheader wie Content Security Policy und Strict Transport Security, die die Angriffsfläche der Anwendung im Browser verkleinern.

Selbst bauen – wählen Sie Ihren Assistenten

Beide Buttons öffnen einen neuen Tab, in dem **derselbe fertige Prompt** bereits eingetragen ist. Der Prompt verweist das Modell auf die Spezifikation dieses Moduls – eine einzelne Markdown-Datei mit der Lektion, der Lab-Aufgabe und den geforderten Ergebnissen –, sodass es mit dem echten Material arbeitet, statt zu raten, worum es in Modul 10 geht. Sie können [module-10.md](#) selbst öffnen, um genau zu sehen, was es lesen wird.



ChatGPT verwenden

Öffnet chatgpt.com mit dem Prompt dieses Moduls. Funktioniert mit GPT-5 oder Codex; jeder Tarif mit Websuche ruft die Spezifikation ab.



Claude verwenden

Öffnet claude.ai mit demselben Prompt. Wenn Sie Claude Code nutzen, können Sie ihn stattdessen in einem leeren Ordner in ein Terminal einfügen.



Unverändert abgeschickt, erhalten Sie ein Projekt, kein Code-Fragment

Der Prompt verlangt am Ende die gesamte Projektmappe als einzelne `.zip`-Datei mit Anleitung zum Kompilieren und Starten. Laden Sie sie herunter, öffnen Sie die Projektmappe in Visual Studio, drücken Sie F5, und EnterpriseOps startet auf `localhost`. Sie benötigen das .NET SDK und das NuGet-Paket `Wisej-4`; alles andere soll der Assistent laut Prompt selbst schreiben.

Ich arbeite gerade Modul 10 – „Sicherheitsarchitektur: Identität, SSO, Autorisierung, Audit und sicheres Deployment“ – des LearnWisej-Kurses „Enterprise Wisej.NET: von der Architektur in die Cloud“ durch und möchte das Beispielpjekt des Moduls gemeinsam mit dir erstellen. Bitte antworte auf Deutsch.

Lies zuerst die Modulspezifikation. Sie ist eine einzelne Markdown-Datei (auf Englisch) mit der vollständigen Lektion, der Lab-Aufgabe und den geforderten Ergebnissen:
<https://learnwisej.com/assets/courses/azure-docker/specs/module-10.md>

Erstelle dann ein vollständiges Wisej.NET-4-Projekt, das ich in Visual Studio öffnen kann:

1. Projekt „EnterpriseOps“, C#, net8.0 oder neuer, NuGet-Paket Wisej-4 4.1.x, Kestrel-Host, der `app.UseWisej()` aufruft.
2. Setze um, was das Lab der Spezifikation verlangt: Ergänzen Sie eine Simulation der Enterprise-Authentifizierung, das Mapping von Claims auf Berechtigungen, die Durchsetzung von Mandantenrollen, Autorisierung auf Service-Ebene, ein Review für sicheres HTML, eine Freigabe für Exporte und Audit-Logging für sensible Aktionen.
3. Liefere diese Ergebnisse und sag mir, wo sich jedes davon in der Projektmappe befindet:
 - Design des Identitäts-Mappings
 - Berechtigungsmatrix
 - Implementierung des Berechtigungsservices
 - Bildschirm für das Audit-Log
 - Checkliste zur Sicherheitshärtung
4. Halte dich an die Spezifikation, wo immer sie eine Wisej.NET-Klasse, -Eigenschaft oder ein -Event nennt – verwende genau diese. Wo sie eine Wahl offenlässt, sag mir, welche API du gewählt hast und warum.
5. Der Server bleibt maßgeblich: Zustand und Validierung leben in .NET, der Browser stellt dar und meldet zurück. Verlagere nie eine Entscheidung nach JavaScript, nur weil es dort einfacher ist.
6. Mach das Ergebnis vorführbar: Ich muss es starten und das Verhalten sehen können, um das es in diesem Modul geht – auch, was passiert, wenn etwas schiefgeht.

Bevor du Code schreibst, fasse in eigenen Worten zusammen, was du bauen wirst und wo jedes Teil liegen wird, damit ich den Entwurf korrigieren kann, solange das noch wenig kostet.

Wenn der Code fertig ist, packe die gesamte Projektmappe in eine einzelne .zip-Datei zum Herunterladen und nenne mir die genauen Schritte, um sie zu kompilieren und auszuführen.

Beantworte zum Schluss diese Fragen aus der Spezifikation und nutze dabei deine eigene Implementierung als Beleg:

- Wo wird die Autorisierung durchgesetzt?
- Welche UI-Elemente rendern HTML?
- Kann eine aktivierte Schaltfläche die Regeln des Service umgehen?

Frag mich nach allem, was unklar ist, bevor du anfängst.

Prüfen Sie dann, was zurückkommt

Code, der kompiliert, ist noch lange kein richtiger Code. Die spannenden Fragen sind Designfragen: Ist das wirklich das Wisej.NET-Control, das die Aufgabe verlangt? Folgt der Code dem Lebenszyklus, den das

Framework vorgibt? Liegt der maßgebliche Zustand auf dem Server – oder wurde er im Browser abgelegt, weil das bequemer war? Lesen Sie das Ergebnis als Reviewer, nicht als Kunde.

Die Checkliste liefert Ihnen dieses Modul. Beantworten Sie jeden Punkt anhand des Codes, den Sie gerade erhalten haben:

- ✓ Wo wird die Autorisierung durchgesetzt?
- ✓ Welche UI-Elemente rendern HTML?
- ✓ Kann eine aktivierte Schaltfläche die Regeln des Service umgehen?

Alles, was Sie korrigieren mussten, sollten Sie festhalten. Eine kurze Notiz zu den Konventionen und Entscheidungen, auf die Sie sich festgelegt haben – eingefügt in die erste Nachricht Ihrer nächsten Sitzung –, ist mehr wert als jeder noch so clevere Prompt.



Dieses Beispiel haben wir schon gebaut – vergleichen Sie Ihres mit unserem

Die Referenzimplementierung zu Modul 10 liegt im öffentlichen Beispiel-Repository. Bauen Sie zuerst Ihre eigene Version und öffnen Sie dann unsere: Die Unterschiede sind der interessante Teil.



[Beispiel zu Modul 10 auf GitHub öffnen](#)

Oder klonen Sie alle Beispiele mit `git clone https://github.com/iceteagroup/LearnWisej-Samples` und öffnen Sie [Enterprise Wisej.NET Course/Module 10](#).



Unser Beispiel ist ein Ausgangspunkt, kein fertiges Produkt

Es ist genauso entstanden wie Ihres – per Prompt und anschließend korrigiert – und endet bewusst dort, wo das Modul endet. Rechnen Sie mit Platzhaltern, wo Produktivcode hingehört, mit knapper Fehlerbehandlung und ohne Tests. Verstehen Sie das als Einladung: Nutzen Sie, was Sie in diesem Modul gelernt haben, und dazu den Assistenten, um es weiterzuentwickeln. Code zu verbessern, den Sie nicht selbst geschrieben haben, ist die Fähigkeit, die dieser Kurs eigentlich vermittelt.

Drei Prompts für den nächsten Schritt

Richten Sie Ihren Assistenten auf das Projekt, das Sie gerade gebaut haben – oder auf unseres –, und probieren Sie diese Prompts aus. Jeder ist eine Übung zum Prüfen und Erweitern, kein Neuschreiben.

- ✓ **Beweisen Sie, dass es wirklich funktioniert.** *"Geh dieses Projekt Ergebnis für Ergebnis anhand der Modulspezifikation unter <https://learnwisej.com/assets/courses/azure-docker/specs/module-10.md> durch und zeig mir den Beleg, dass jedes wirklich erledigt ist – den Codepfad, worauf ich klicken muss und was ich sehen sollte. Wo ein Ergebnis nur teilweise erfüllt ist, sag das klar, statt es schönzureden. Ergänze dann, was fehlt."*
- ✓ **Prüfen Sie es wie einen Pull-Request.** *"Führ mich durch diesen EnterpriseOps-Code, als würdest du den Pull-Request eines Kollegen prüfen und hättest ihn nicht selbst geschrieben. Wo lebt der Zustand, was passiert bei einer einzelnen Benutzeraktion von Anfang bis Ende, was würdest du zur Überarbeitung zurückgeben, und welche Teile würdest du nicht guten Gewissens einem Kunden vorlegen? Sei konkret und zitiere die Zeilen, die du meinst – fasse mir nicht den Entwurf zusammen."*
- ✓ **Tauschen Sie ein Teil aus, ohne die Schnittstellen zu verschieben.** *"Wähle den Teil dieses EnterpriseOps-Projekts, der am offensichtlichsten nur ein Platzhalter für etwas Echtes ist – eine Fake-Datenquelle, ein In-Memory-Speicher, ein vereinfachter Service – und ersetze ihn durch eine praxisnahe Implementierung. Der Vertrag auf beiden Seiten darf sich nicht ändern: dieselben Typen, dieselben Aufrufe, dasselbe Verhalten im Fehlerfall. Sag mir, was du durch die echte Implementierung behandeln musstest, was der Platzhalter nicht behandelt hat."*



Nehmen Sie es mit ins Lab

Das praktische Lab am Ende dieses Moduls verlangt dieselben Ergebnisse, die Sie gerade vom Assistenten haben erstellen lassen. Nutzen Sie, was Sie hier haben, als Gerüst für Ihre Antwort und als Beleg dafür – nicht als die Antwort selbst. Bewertet wird im Lab Ihre Argumentation, und dieser Teil muss von Ihnen stammen.