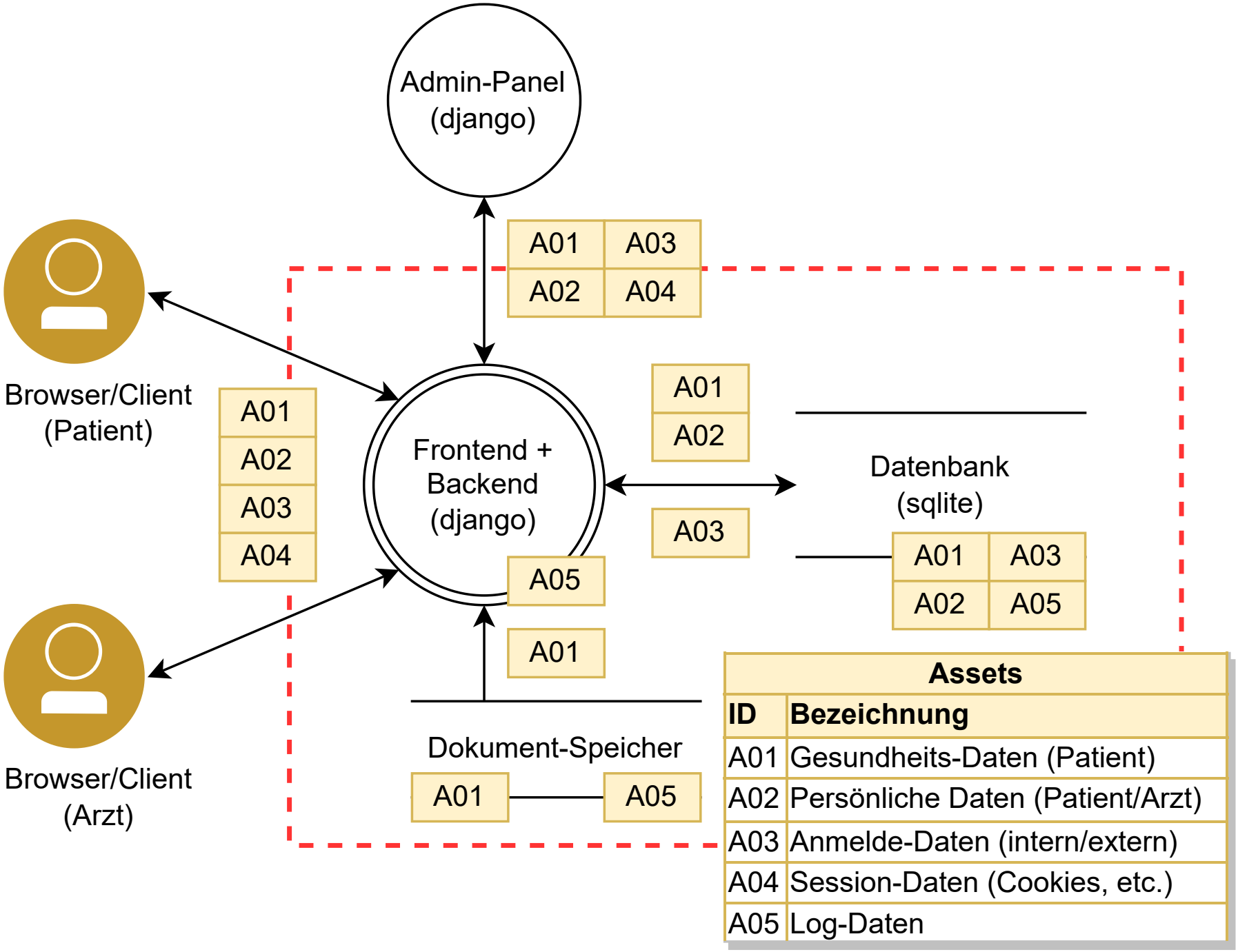
Projekt: Security by Design (Semester 5)

# Patient Data Management System

## Sicherheitsanforderungen & Bedrohungsanalyse

*Irina Jörg, Finn Callies, Arne Kapell*

# Threat Modeling




| Assets | |
|---|---|
| **ID** | **Bezeichnung** |
| A01 | Gesundheits-Daten (Patient) |
| A02 | Persönliche Daten (Patient/Arzt) |
| A03 | Anmelde-Daten (intern/extern) |
| A04 | Session-Daten (Cookies, etc.) |
| A05 | Log-Daten |

# Schutzziele

| Asset | Vertraulichkeit | Integrität | Verfügbarkeit |
|---|---|---|---|
| **A01**: Gesundheits-Daten | X(1) | X(1) | X(2) |
| **A02**: Persönl. Daten | X(1) | X(2) | X(3) |
| **A03**: Anmelde-Daten | X(1) | X(2) | X(3) |
| **A04**: Session-Daten | X(1) | X(3) | X(2) |
| **A05**: Log-Daten | X(2) | X(1) | X(3) |

# Technologie-Stack

- Django (Python) für Frontend und Backend
  - integriertes Admin-Interface
- Datei-basierte Datenbank (SQLite)


# Risiko-Register

# Risiko-Register (1/4)

| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
|---|---|---|---|---|---|
| R6 | Verwendung von Eingabefeldern für Angriffe | Hoch | Hoch | Hoch | Reduzieren |
| **Beschreibung** | | | | | |
| Durch mögliche Eingabe von Befehlen in textbasierten Eingabefeldern besteht das Risiko von Zugriff auf Daten, unbefugte Manipulation der Datenbank und Einschleusen von Code, der zur Freilegung von Cookies und Session-Token führen kann. (XSS)<br><br>CON.10.A15 | | | | | |
| **Anforderungen** | | | | | |
| Es ist notwendig, dass ein solches Eingeben nicht durchgeführt werden kann. | | | | | |
| **Maßnahmen** | | | | Überprüfung | TestID |
| Eingabevalidierung in allen Eingabefeldern integrieren. (auch auf Server-Seite) | | | | Automatisierter Test<br>Pentest<br>Code Review | TBA |

# Risiko-Register (2/4)

| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
|---|---|---|---|---|---|
| R7 | Verfügbarkeits-Ausfall von Datenbank und Dokumenten-Speicher | Mittel | Hoch | Mittel | Transferieren |
| **Beschreibung** | | | | | |
| Durch Ausfall der Datenbank oder der Verbindung zu dieser wird die Verfügbarkeit nicht erfüllt.<br>Ein Zugriff auf die Daten ist nicht mehr möglich und eine | | | | | |
| **Anforderungen** | | | | | |
| Aufbau einer Ausfallsicheren Datenbankumgebung und regelmäßiges Erstellen eines Backups einführen. Es soll ein Zugriff rund um die Uhr bereitgestellt werden.<br>Die DSGVO schreibt in Artikel 32 vor, dass die “Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen“ gegeben sein muss. | | | | | |
| **Maßnahmen** | | | | Überprüfung | TestID |
| Einführen eines regelmäßigen Backups an einem gesonderten Speicherort und Aufbau eines Datenbanksystems mit mindestens 2 Datenbanken. (HA) | | | | Automatisierter Test<br>Manueller Test | TBA |

# Risiko-Register (3/4)

| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
|---|---|---|---|---|---|
| R8 | Unbefugter Zugriff auf System-Administration | Mittel | Sehr hoch | Mittel | Vermeiden |
| **Beschreibung** | | | | | |
| Ein Angreifer bekommt Zugang zu einem Administrator Account und bekommt so vollständigen Zugriff auf die Umgebung. | | | | | |
| **Anforderungen** | | | | | |
| Accounts mit Administrator-Rechten sollen gesondert geschützt werden und einen erfolgreichen Angriff möglichst vollständig verhindern. | | | | | |
| **Maßnahmen** | | | | Überprüfung | TestID |
| Gesonderte Eingabevalidierung und Authentifizierung für Accounts mit Administrator-Rechten. | | | | Pentest | TBA |

# Risiko-Register (4/4)

| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
|---|---|---|---|---|---|
| R9 | Schadcode-Einschleusung durch Datei-Upload | Mittel | Sehr hoch | Mittel | Transferieren |
| **Beschreibung** | | | | | |
| Duch die Möglichkeit zum Dokumenten-Upload könnten auch solche mit enthaltenem Schadcode in das System gelangen. | | | | | |
| **Anforderungen** | | | | | |
| Potenzielle Angreifer dürfen keinen (schädlichen) Code im System ausführen. | | | | | |
| **Maßnahmen** | | | | Überprüfung | TestID |
| Die Anwendung öffnet ein Dokument nie und legt es nur im Speicher ab bzw. leitet es an den Abrufenden weiter.<br><br>Analyse des Dokuments beim Upload (z.B. mit lokal laufendem Dritt-Anbieter-Tool). | | | | Manueller Test<br>Automatisierter Test<br>Pentest | TBD |

# Vielen Dank fürs Zuhören!

**Fragen?**