**Case Study: Online Healthcare Portal**

**Scenario:**

A healthcare provider is developing a web application called **MyHealth** that allows patients to:

* View medical records
* Schedule appointments
* Make payments
* Communicate with doctors

The company wants to **identify security threats** using **PASTA**.

**Applying PASTA's 7 Stages**

**Stage 1: Define Objectives**

* **Business Goal:** Provide secure access to patient data.
* **Security Goal:** Prevent unauthorized access, data leaks, and fraud.
* **Compliance:** Must follow **HIPAA** regulations.

**Stage 2: Define Technical Scope**

* **Architecture:** Cloud-based, hosted on **Azure**.
* **Components:** Web frontend, backend API, database, authentication system.
* **Users:** Patients, doctors, administrators.

**Stage 3: Application Decomposition**

* **Data Flow:**
  + Patients enter credentials → Authentication server verifies → Backend API retrieves data → Frontend displays records.
* **Trust Boundaries:**
  + Public internet → Web app
  + Web app → Backend API
  + Backend API → Database

**Stage 4: Threat Analysis**

Using **STRIDE**, we identify threats:

* **Spoofing:** Fake login attempts.
* **Tampering:** Modification of medical records.
* **Repudiation:** Lack of audit logs.
* **Information Disclosure:** Data leaks.
* **Denial of Service:** Overloading the system.
* **Elevation of Privilege:** Unauthorized admin access.

**Stage 5: Vulnerability Analysis**

* **Weak authentication** → Brute-force attacks.
* **Unencrypted database** → Data exposure.
* **Unvalidated input** → SQL injection risk.

**Stage 6: Attack Simulation**

* **Scenario:** An attacker tries SQL injection to access patient records.
* **Impact:** Medical data is stolen.
* **Mitigation:** Use **parameterized queries** and **input validation**.

**Stage 7: Risk & Impact Analysis**

| **Threat** | **Risk Level** | **Mitigation** |
| --- | --- | --- |
| SQL Injection | High | Input validation, parameterized queries |
| Weak Authentication | High | Multi-factor authentication (MFA) |
| Data Leakage | Medium | Encrypt sensitive data |

**Final Recommendations**

1. **Implement MFA** for login security.
2. **Encrypt all sensitive data** in storage and transit.
3. **Use secure coding practices** to prevent injection attacks.
4. **Perform regular security audits** to identify new threats

