Aufgabenstellung Labor „Sichere Systeme“
Risikoregister [David Fambach/Jonas Grohe/Vincent Hundeloh]

Auswirkungen Eintrittswahrscheinlichkeit	Niedrig	Mittel	Hoch	Sehr hoch
Sehr hoch	Niedrig	Mittel	Hoch	Sehr hoch
Hoch	Niedrig	Mittel	Hoch	Hoch
Mittel	Niedrig	Niedrig	Mittel	Mittel
Niedrig	Niedrig	Niedrig	Niedrig	Niedrig

RisikoID	**Bedrohung**	**Eintrittswahrscheinlichkeit**	**Auswirkungen**	**Risiko**	**Behandlung**
[RId]	[Kurztext]	[Sehr hoch] [Hoch] [Mittel] [Niedrig]	[Sehr hoch] [Hoch] [Mittel] [Niedrig]	[Sehr hoch] [Hoch] [Mittel] [Niedrig]	[Vermeiden] [Reduzieren] [Transferieren] [Akzeptieren]
Beschreibung					
[Text]					
Anforderungen					
[Text]					
Maßnahmen				Überprüfung	TestID
[Text]				[Manueller Test] [Automatisierter Test] [Pentest] [Design Review] [Code Review] […]	[TId]

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R1	Unbefugte ohne Benutzer in der Anwendung können Gesundheitsdaten oder persönliche Daten anderer Benutzer sehen.	Hoch	Sehr hoch	Hoch	Reduzieren
Beschreibung					
Unbefugte ohne Benutzeraccount in der Anwendung können Gesundheitsdaten oder persönliche Daten anderer Benutzer sehen. Betrifft: A8, A9					
Anforderungen					
• Alle Zugriffe auf die Anwendung müssen authentifiziert erfolgen. • DSGVO schreibt Schutz der Daten gesetzlich vor. • BSI CON.10.A1 • OWASP V1.2.3					
Maßnahmen				Überprüfung	TestID
Benutzerverwaltung und Authentifizierung (Anmeldung) erzwingen vor Zugriff.				Manueller Test Automatisierter Test Pentest Code Review	T1, T2, T3, T4

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R2	Benutzer der Anwendung können Gesundheitsdaten oder persönliche Daten anderer Benutzer sehen.	Hoch	Sehr hoch	Hoch	Reduzieren
Beschreibung					
Benutzer der Anwendung können Gesundheitsdaten oder persönliche Daten anderer Benutzer sehen. Betrifft: A8, A9					
Anforderungen					
• Vor jedem Zugriff wird die Berechtigung des Benutzers durch den Dateiablagedienst überprüft und der Zugriff gegebenenfalls abgelehnt. • DSGVO schreibt Schutz der Daten gesetzlich vor. • CON.10.A2					
Maßnahmen				Überprüfung	TestID
Authentifizierung (Anmeldung) erzwingen vor Zugriff (siehe R1). Autorisierung (Berechtigunbgsprüfung) erzwingen vor Zugriff.				Manueller Test Automatisierter Test Pentest Code Review	T5, T6, T7, T8

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R3	Sicherheit der Datenübertragung	Hoch	Sehr hoch	Hoch	Reduzieren
Beschreibung					
Datenübertragungen zwischen Webbrowser und Webserver beziehungsweise zwischen Webserver und Dateiablagedienst beziehungsweise zwischen Dateiablagedienst und DB-Server können durch Dritte mitgelesen werden.					
Anforderungen					
• Alle Kommunikation/Datenübertragung muss sicher (vertraulich und integritätsgeschützt) erfolgen. • DSGVO schreibt Schutz der Daten gesetzlich vor. • CON.10.A14 Betrifft: A8, A9, A10, A13, A18					
Maßnahmen				Überprüfung	TestID
Für Verbindungen zwischen Webanwendung und Webserver, Webserver und Dateiablagedienst sowie Dateiablagedienst und Datenbank TLS einsetzen. Der Webserver setzt den HTTP-Header Strict-Transport-Security (OWASP ASVS V14.4.5)				Manueller Test Automatisierter Test Pentest Code Review	T9, T10, T11, T12

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R4	Datenmanipulation	Hoch	Sehr hoch	Hoch	Reduzieren
Beschreibung					
Durch Abfragemanipulation können unbefugt Daten (A8, A9) aus der Datenbank gelesen oder verändert werden.					
Anforderungen					
• Ein unbefugter Datenbankzugriff, ob lesend oder schreibend, muss verhindert werden. • Der Dateiablagedienst muss resistent gegen SQL-Injection-Angriffe sein (BSI CON.10.A9) • DSGVO schreibt Schutz der Daten gesetzlich vor. Betrifft: A8, A9					
Maßnahmen				Überprüfung	TestID
Datenübertragung schützen (vgl. R3) Eingabevalidierung in der Webanwendung Eingabevalidierung im Dateiablagedienst Verwendung von Prepared SQL Statements durch den Dateiablagedienst Kryptografische Verschlüsselung mit Integritätsschutz anbringen (vgl. R11)				Manueller Test Code Review	T13, T14

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R5	Webanwendungs-Schwachstellen	Hoch	Hoch	Hoch	Reduzieren
Beschreibung					
Es verbleiben typische Webschwachstellen in der Anwendung die nicht entdeckt werden.					
Anforderungen					
• Die Webanwendung ist resistent gegen XSS • Die Webanwendung, Webserver und Dateiablagedienst sind resistent gegen Session Hijacking • Der Webserver und Dateiablagedienst sind resitent gegen Session Prediction • Der Webserver ist resistent gegen Path Traversal • Der Webserver und Dateiablagedienst ist resistent gegen CSRF					
Maßnahmen				Überprüfung	TestID
Der Webserver und der Dateiablagedienst reflektieren keine Benutzereingaben als HTML/CSS/JS Der Webserver setzt den HTTP-Header Content-Security-Policy (OWASP ASVS V14.4.3) Der Webserver setzt den HTTP-Header X-Content-Type-Options (OWASP ASVS V14.4.4) Die Webanwendung verwendet keine Benutzereingaben zur DOM-Modifikation Die Webanwendung zeigt Sitzungsgeheimnisse nicht in der URL an Der Webserver prüft auf auffällge Änderungen des UserAgent Headers im Laufe einer Sitzung. Der Webserver stellt sicher, dass Sitzungen nicht unbegrenzt gültig. Alle Sitzungsgeheimnisse werden zufällig durch einen CSRNG gezogen. Der Webserver prüft nachdem eine angefragte Ressource im Dateisystem gefunden wurde, ob die Datei im freigegebenen Bereich liegt.				Manueller Test Automatisierter Test Code Review	T15, T16, T17

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R6	Benutzer verwenden unsichere Passwörter	Sehr hoch	Hoch	Hoch	Reduzieren
Beschreibung					
Benutzer wählen aus Bequemlichkeit, Unwissenheit oder anderen Gründen unsichere Passwörter für die Authentifizierung. Dadurch werden Sicherheitsmechanismen, die auf der Integrität des Benutzerkontos aufbauen, unwirksam.					
Anforderungen					
• Das Erraten des Kennworts mittels Bruteforce oder durch Nutzung von Wörterbüchern und Rainbowtables soll unwirtschaftlich sein.					
Maßnahmen				Überprüfung	TestID
Single-Sign-On über einen externen IDP ermöglichen. Das Passwort muss gewisse Vorgaben erfüllen um verwendet werden zu können. Zum Speichern und Prüfen von Passwörtern wird eine geeignete Hashfunktion und ein Salz verwendet.				Automatisierter Test Pentest Design Review	T18, T19, T20

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R7	Benutzer vergessen Passwörter	Hoch	Mittel	Mittel	Reduzieren
Beschreibung					
Wegen hoher Anforderungen (siehe R6) an das Passwort ist dieses nicht sehr einprägsam. Hinzu kommt, dass die Gesundheitsakte von den meisten Benutzern nicht regelmäßig verwendet wird. Infolgedessen werden viele Benutzer ihr Zugangsdaten vergessen und somit ihre verschlüsselten Daten verlieren (vgl. Konzept „Schützen von Data-at-rest“).					
Anforderungen					
• Benutzer werden auf dieses Risiko aufmerksam gemacht und Möglichkeiten zur Vermeidung genannt.					
Maßnahmen				Überprüfung	TestID
Bei der Erstellung des Kontos wird darauf hingewiesen, dass es sich bei der Anwendung nicht um einen Onlinespeicher, sondern um eine Datenaustauschplattform handelt. Das hat zur Folge, dass die Verfügbarkeit der Daten der Vertraulichkeit und der Integrität der Daten untergeordnet ist. Bei der Erstellung des Kontos wird darauf hingewiesen, dass in der Anwendung zum Schutz der Vertraulichkeit die Daten Ende-zu-Ende verschlüsselt werden. Das hat zur Folge, dass beim Zurücksetzen des Anmeldekennworts sämtliche gespeicherte Daten gelöscht werden. Bei der Erstellung des Kontos wird darauf hingewiesen, dass zum Verwalten von komplexen Passwörtern ein Passwortmanager eine große Hilfe ist. Bei der Initialisierung kryptografischer Parameter wird dem Benutzer angeboten, eine Wiederherstellungsdatei abzuspeichern, die es ermöglicht, nach einem Zurücksetzen des Kennworts weiterhin auf verschlüsselte Daten zuzugreifen (vgl. Konzept "Schützen von Data-at-rest").				Manueller Test Code Review	T21, T22

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R8	Überlastung der Speicherressourcen durch zu viele Dokumente.	Hoch	Niedrig	Niedrig	Reduzieren
Beschreibung					
Benutzer belegen übermäßig viele Speicherressourcen, indem sie Dateien in ihr Profil laden und verhindern so, dass anderen Benutzern dieser Speicherplatz zur Verfügung steht.					
Anforderungen					
• Das System ist resistent gegen einen DoS durch zu hohe Speicherbelegung durch einzelne Benutzer					
Maßnahmen				Überprüfung	TestID
Pro Benutzer wird der verwendbare Speicherplatz beschränkt. Pro Benutzer wird eine Netzwerkquota gesetzt. BSI CON.10.A17				Manueller Test	T23

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R9	Benutzer der Anwendung laden bösartige Dateien hoch	Niedrig	Hoch	Niedrig	Reduzieren
Beschreibung					
Benutzer der Anwendung laden bösartige Dateien hoch. Diese könnten dann von anderen Benutzern heruntergeladen und geöffnet werden und dadurch ihr System infizieren.					
Anforderungen					
• Das Hochladen einer solchen Datei soll erschwert und wenn möglich verhindert werden. • Benutzer sollten vor dem Ausführen / beim Herunterladen einer Datei vor Risiken gewarnt werden.					
Maßnahmen				Überprüfung	TestID
Nur Dateien mit freigegebenen Dateiendungen dürfen hochgeladen werden. Benutzer werden beim Herunterladen vor möglichen Risiken gewarnt				Manueller Test Automatisierter Test	T23, T24

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R10	Unbefugte sehen geheime Konfigurationsparameter ein	Niedrig	Hoch	Niedrig	Reduzieren/ Akzeptieren
Beschreibung					
Unbefugte Prozesse oder Benutzer können geheime Konfigurationsparameter einsehen, insbesondere kryptografische Schlüssel, die von einer Anwendungskomponente benötigt werden, zum Beispiel zum Erbringen eines Identitätsnachweises.					
Anforderungen					
• Geheime Konfigurationsparameter werden vertraulich gespeichert • OWASP ASVS V1.6.2 wird explizit nicht eingesetzt (vgl. Konzept "Schützen von konfigurierten Geheimnissen produktiver Systeme") Betrifft: A4, A6					
Maßnahmen				Überprüfung	TestID
Ausgeben einer Warnung an den Administrator, falls für geheime Konfigurationsparameter im Dateisystem ungünstige Zugriffsrechte gesetzt sind. Diese Maßnahme ist sehr einfach umsetzbar, ermöglicht aber nur die Erkennung eines einzelnen, speziellen Szenarios und reduziert damit formell das bezeichnete Risiko. Weil dies aber die einzige Maßnahme ist, wäre es irreführend, die Risikobehandlung als kommentarlos als Reduzieren zu bezeichnen, weil das nur unerheblich unter dem Ursprungsrisiko liegende Restrisiko de facto akzeptiert wird.				Manueller Test	T25

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R11	Privilegierte Benutzer sehen Gesundheitsdaten anderer Benutzer ein	Mittel	Hoch	Mittel	Reduzieren
Beschreibung					
Privilegierte Benutzer können Gesundheitsdaten anderer Benutzer einsehen. Dieses Risiko unterscheidet sich von R1 dahingehend, dass der Benutzer, der unbefugt Daten einsehen kann, berechtigterweise erweiterte Rechte auf Systemen der Anwendung hat.					
Anforderungen					
• Maßnahmen, die die Möglichkeiten priveligierter Benutzer beschränken, Vertraulichkeit und Integrität gespeicherter Gesundheitsdaten zu verletzen, und deren Aufwand ihren Nutzen nicht unangemessen übersteigt, werden implementiert. • DSGVO schreibt Schutz der Daten gesetzlich vor. Betrifft: A8					
Maßnahmen				Überprüfung	TestID
Einsatz von Ende-zu-Ende-Verschlüsselung für Benutzerdaten mittels asymmetrischer Kryptografie (vgl. Konzept „Schützen von Data-at-rest“) Maßnahmen gemäß R1				Manueller Test Design Review Code Review	T26, T27, T28

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R12	Privilegierte Benutzer sehen personenbezogene Daten anderer Benutzer ein	Mittel	Hoch	Mittel	Akzeptieren
Beschreibung					
Privilegierte Benutzer können personenbezogenen Daten anderer Benutzer einsehen. Dieses Risiko unterscheidet sich von R1 dahingehend, dass der Benutzer, der unbefugt Daten einsehen kann, berechtigterweise erweiterte Rechte auf Systemen der Anwendung hat. Für priveligierte Benutzer, die aus geschäftlichen Gründen auf die oder eine Telmenge der gespeicherten personenbezogenen Daten zugreifen müssen, besteht die Möglichkeit, dass dieser Zugang missbraucht wird. Aufgrund der Datenminimierung nach DSGVO ist die Menge der vorhandenen und damit zugreifbaren Daten bereits minimal. Das Ergreifen weiterer technischer Maßnahmen gegen einen Missbrauch des Zugangs wäre risikobasiert nicht angemessen. Stattdessen sollten für den Betrieb der Anwendung gegebenenfalls geeignete organisatorische Maßnahmen implementiert werden, die dieses Risiko auf ein akzeptables Maß reduzieren (NDO).					
Anforderungen					
• DSGVO schreibt Schutz der Daten gesetzlich vor. Betrifft: A9					
Maßnahmen				Überprüfung	TestID
n/a				n/a	n/a

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R13	Eine Person, die kein Arzt ist, gibt vor, ein Arzt zu sein.	Mittel	Hoch	Mittel	Reduzieren
Beschreibung					
Eine Person gibt sich als Arzt aus, um sich so das Vertrauen von anderen Benutzern erschleichen und sie zum Austausch der Patientendaten animieren.					
Anforderungen					
• Benutzer sollen ihr Gegenüber zu jeder Zeit eindeutig identifizieren können.					
Maßnahmen				Überprüfung	TestID
Jedem Benutzer wird bei der Erstellung seines Kontos eine eindeutige ID zugewiesen. Der Empfänger gibt sie an Personen weiter, von denen er Dokumente erhalten möchte. Der Sender kann mit dieser Nummer sein Gegenüber eindeutig identifizieren: Vor der ersten Dateifreigabe gibt der Sender die Identifikationsnummer an, um das Benutzerprofil des Empfängers zu finden. Nachdem eine gültige Identifikationsnummer angegeben wurde, werden allgemeine Profilinformationen zur eingegebenen Nummer angezeigt und erneut durch den Benutzer bestätigt. Erst danach steht dieser Empfänger für Freigaben im Profil des Senders zur Verfügung. Weil die Identifikationsnummern in nicht vorhersagbarer Folge zugewiesen werden, ist deren Abschätzung erheblich erschwert und es ist unwahrscheinlich, dass ein Fehler des Senders bei der Eingabe der Nummer eine Nummer erzeugt, die einem anderen Profil zugeordnet ist.				Manueller Test Design Review	R29, R30

RisikoID	Bedrohung	Eintrittswahrscheinlichkeit	Auswirkungen	Risiko	Behandlung
R14	Die Webanwendung wird zum Abgreifen sensibler Daten manipuliert	Mittel	Hoch	Mittel	Reduzieren
Beschreibung					
Eine schadhafte Veränderung der Webanwendung führt zu einer Offenlegung von sensiblen Daten, beispielsweise von Gesundheitsdaten oder Passwörtern.					
Anforderungen					
• Die Integrität der Webanwendung, also von HTML-, CSS-, JavaScript- und anderen Ressourcen, muss sichergestellt werden					
Maßnahmen				Überprüfung	TestID
Verwendung von TLS für die Übertragung der Webanwendung (vgl. R3) Verwendung eines TLS-Serverzertifikats, das es Benutzern erlaubt, die Identität des Servers vor der Verwendung der Webanwendung zu überprüfen. Dabei ist zu berücksichtigen, dass dadurch nur ein Schutz erzielt wird, solange die gefälschte Webanwendung unter dem echten Hostnamen abgerufen wird und solange der Fälscher keinen Zugriff auf die private Komponente des verwendeten Zertifikats hat.				Manueller Test	R31