Aufgabenstellung Labor “Sichere Systeme”  
Risikoregister Irina Jörg/Finn Callies/Arne Kapell

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 Benutzer 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 | TBA |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 geprüft.   DSGVO schreibt Schutz der Daten gesetzlich vor.  CON.10.A2 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Authentifizierung (Anmeldung) erzwingen vor Zugriff (siehe R1).  Autorisierung (Berechtigungsprüfung) erzwingen vor Zugriff. | | | | Manueller Test Automatisierter Test Pentest | TBA |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R3 | Sicherheit der Datenübertragung | Hoch | Sehr hoch | Hoch | Reduzieren |
| Beschreibung | | | | | |
| Datenübertragung zwischen Webbrowser und Webserver und zwischen Webserver/Webanwendung und DB-Server könnte abgehört werden. | | | | | |
| Anforderungen | | | | | |
| Alle Kommunikation/Datenübertragung muss sicher (vertraulich, integritätsgeschützt) erfolgen.  DSGVO schreibt Schutz der Daten gesetzlich vor.  CON.10.A14  Betrifft: A1, A2, A3, A4 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Überall HTTPS (HTTP über TLS) einsetzen. | | | | Manueller Test Automatisierter Test | TBA |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R4 | Datenmanipulation | Hoch | Sehr hoch | Hoch | Reduzieren |
| Beschreibung | | | | | |
| Unbefugte könnten Daten in der DB (A1-A3) bzw. im Dokumenten-Speicher (A1) lesen oder verändern. | | | | | |
| Anforderungen | | | | | |
| Ein unbefugter Zugriff lesend oder schreibend muss verhindert werden.  DSGVO schreibt Schutz der Daten gesetzlich vor. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Datenübertragung schützen (siehe R3).  Eingabevalidierung (Webanwendung), Zugriffskontrolle (Berechtigungsprüfung) in der Webanwendung + DB-Server.  Kryptografische Verschlüsselung mit Integritätsschutz anbringen. (optional) | | | | Manueller Test Pentest Design Review | TBA |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R5 | Webanwendungs-Schwachstellen | Hoch | Hoch | Hoch | Reduzieren |
| Beschreibung | | | | | |
| Es verbleiben Web-typische Schwachstellen in der Anwendung die nicht entdeckt werden. | | | | | |
| Anforderungen | | | | | |
| Es sollten möglichst alle State-of-the-Art-Anforderungen für eine sichere Web-Anwendung erfüllt/abgedeckt sein. Da diese jedoch ständig im Wandel sind, bieten die Anforderungen im „OWASP Application Security Verification Standard“ eine gute Grundlage. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Sicherheitsrelevante Header setzen (z.B. Content-Security-Policy) und HTTP-Methoden verwenden.  Korrekte Konfigurationen für Eindämmung von CSRF verwenden. (CORS, CSRF)  Verwendung von JavaScript minimieren und Benutzer-Eingaben korrekt behandeln. | | | | Automatisierter Test Pentest  Code Review (SAST) | TBA |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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)  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 Pentest  Code Review | TBA |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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.  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.  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  Manueller Test | TBA |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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.  Analyse des Dokuments beim Upload (z.B. mit lokal laufendem Dritt-Anbieter-Tool). | | | | Manueller Test Automatisierter Test Pentest | TBD |