Aufgabenstellung Labor “Sichere Systeme”  
Risikoregister [Name1/Name2/Name3]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 [Design Review]  Code Review (Manuell)  […] | T1 T2 T3 [T4] T5 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 (Berechtigunbgsprüfung) erzwingen vor Zugriff. | | | | Manueller Test Automatisierter Test Pentest [Design Review]  Code Review (manuell)  […] | T6 T7 T8 [T9] T10 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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: A8, A9, A10, A18, A19 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Überall HTTPS (http über TLS) einsetzen. | | | | Manueller Test Automatisierter Test] Pentest Code Review (SAST)  […] | T6 T7 T8 [T9] T10 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R3 | Sicherheit der Datenspeicherung | [Hoch] | [Sehr hoch] | [Hoch] | Reduzieren |
| Beschreibung | | | | | |
| Daten sollten bei at REST verschlüsselt gespeichert werden | | | | | |
| Anforderungen | | | | | |
| ASVS 4.0.3 V6.1  CON.10.A14  Betrifft: A8, A9, A10, A18, A19 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Daten verschlüsseln | | | | Manueller Test Automatisierter Test] Pentest Code Review (SAST)  […] | T11  T12  T13  T14 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R4 | Datenmanipulation | Hoch | Sehr hoch | Hoch | Reduzieren |
| Beschreibung | | | | | |
| Unbefugte könnten Daten (A8, A9) in der DB 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 [Automatisierter Test] [Pentest] [Design Review]  Code Review (SAST)  […] | T15  T16  T17  T18  T19 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 | | | | | |
| …. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Sicherheitsrelevante Header setzen (z.B. Content-Security-Policy) und http-Methoden verwenden. | | | | [Manueller Test] [Automatisierter Test] [Pentest] [Design Review]  Code Review (SAST)  […] | T20  T21  T22  T23  T24 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R6 | Fehlerhafte Authentifizierung | [Hoch] | [Hoch] | [Hoch] | [Reduzieren] |
| Beschreibung | | | | | |
| Authentifizierung durch vorhandenen Anmeldeinformationen, Brute-Force oder Nutzung von Sitzungs-ID | | | | | |
| Anforderungen | | | | | |
| ASVS 4.0.3 V2.1 – Passwortrichtlinien ( Zahlen, Zeichen, Unicode, Passwortänderung,…) | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Implementierung Multi-Faktor-Authentifizierung  Regeln für Kennwörter festlegen  Fehlgeschlagene Anmeldung begrenzen  Sitzungzeitlimit und SitzungsID nach abmelden ungültig | | | | [Manueller Test] [Automatisierter Test] [Pentest]  [Code Review]  […] | T 25  T26  T27  T28 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R7 | Hochladen von schädlichen Dateien während File-Upload | [Hoch] | [Hoch] | [Hoch] | [Reduzieren] |
| Beschreibung | | | | | |
| Schädlichen Dateien können durch die File-Upload Funktion ( für Daten und Befunde) hochgeladen und ausgeführt werden | | | | | |
| Anforderungen | | | | | |
| CON.10.A5 - Upload Funktionen  ASVS 4.0.3 V12.1 – Keine zu großen Dateien zulassen, komprimierte Dateien auf Größe und Anzahl prüfen, Ein User soll mit seinen Dateien den Speicherort nicht füllen  ASVS 4.0.3 V12.2 – Dateien aus nicht vertrauenswürdigen Quellen auf erwarteten Dateityp überprüfen  ASVS 4.0.3 V12.4 – Dateien mit limitierten Berechtigungen speichern und auf bösartigen Inhalt überprüfen( durch Anti Virus Scanner)  ASVS 4.0.3 V12.5 – Anwendung darf nur bestimmte Dateierweiterungen verarbeiten | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Benutzer kann Daten nur im vorgegebenen Pfad speichern und Ablageort nicht beeinflussen  Maximum Größe einer Datei festlegen  Maximum Anzahl von Dateien festlegen | | | | [Manueller Test] [Automatisierter Test] [Pentest] [Design Review]  [Code Review]  […] | T29  T30  T31  T32  T33 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R8 | Unzureichende Nutzung von Monitoring und Logging | [Mittel] | [Hoch] | [Hoch] | [Reduzieren] |
| Beschreibung | | | | | |
| Um mögliche Angriffe zu erkennen ist ein ausreichendes Logging und Analyse von Login, Ausgeführte und Veränderte Daten wichtig, | | | | | |
| Anforderungen | | | | | |
| ASVS 4.0.3 V7.1 – Logging Inhalte (Keine Credentials oder andere sensitiven Daten loggen, Session Tokens in einer gehaschten form, erfolgreiche und fehlgeschlagene Authentifizierungen und Fehler, sowie zum analysieren benötigten Informationen  ASVS 4.0.3 V7.3 – Logging schützen ( Komponenten sind encoded, geschützt vor unautorisiertem Zugriff, Timezone …  ASVS 4.0.3 V7.4 – Umgang mit Errors (Meldung bei Fehlern, für erwartete und unerwartete Fehler Exceptions/Error Handler ) | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Fehlerprotokollierung, Alerting bei wichtigen Fehlern  Logging von Konfigurations- ( Ausgeführte und Veränderte?) und Logdaten | | | | [Manueller Test] [Automatisierter Test] [Pentest] [Design Review]  [Code Review]  […] | T34  T35  T36  T37  T38 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R9 | Nutzung unsicherer Komponenten | [Mittel]  [Niedrig] | [Sehr hoch] [Hoch] | [Mittel]  [Niedrig] | [Vermeiden] |
| Beschreibung | | | | | |
| Nutzung von unsicheren Komponenten wie unsichere und externe libraries | | | | | |
| Anforderungen | | | | | |
| CON.8.A6 – Verwendung von externen Bibliotheken aus vertrauenswürdigen Quellen  CON.8.20 – Externe Komponenten überprüfen  CON.8.A17 – Vertrauenswürdige Entwicklungswerkzeuge auswählen  ASVS 4.0.3 V14.2 – Dependencies ( Jede Komponente Up-to-Date, unnötige Komponenten entfernen, 3rd-Party Komponenten von sicheren Quellen nutzen, 3rd party libraries sandboxen) | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Integrität der externen Bibliotheken sicherstellen – von sicheren/verifizierten Quellen | | | | [Automatisierter Test] [Pentest] [Design Review]  [Code Review] | T39  T40  T41  T42 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R10 | Unzureichendes Session-Management | [Hoch] | [Hoch] | [Hoch] | [Reduzieren] |
| Beschreibung | | | | | |
| Wird eine Session-ID sichtbar ausgegeben und wird ausgelesen, kann diese für Angriffe ausgenutzt werden (Ausgeben als autorisierten Benutzer für Zugriff auf Webanwendung) | | | | | |
| Anforderungen | | | | | |
| ASVS 4.0.3 3.1 – Session Token nie in URL Parameter  ASVS 4.0.3 3.2 – Session Token (Neue Session-ID bei jeder User Authentifizierung, Speichern der Tokens mit sicheren Methoden, generieren durch kryptografische Algorithmen)  ASVS 4.0.3 3.3 – Session beenden (Logout invalidiert Session Token, Re-authentifizierung, nach Passwort Änderung aktive Session terminieren, User soll aktiven Session sehen und sich abmelden können  ASVS 4.0.3 3.7 – Anwendung hat valide Login Session/benötigt weitere Authentifizierung bevor sensitive Daten oder Veränderungen am Account durchgeführt werden | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Session Time Out bei Inaktivität  Session-ID nicht in URL  Neue Session-ID bei jeder User Authentifizierung | | | | [Manueller Test] [Automatisierter Test] [Pentest] [Design Review]  [Code Review]  […] | T43  T44  T45  T46  T47 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R10 | [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] |