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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R1 | Externe ohne Benutzerkonto oder unzureichende Berechtigungen haben können Gesundheitsdaten oder persönliche Daten anderer Benutzer sehen. | Mittel | Sehr hoch | Hoch | Reduzieren |
| Beschreibung | | | | | |
| Externe ohne Benutzerkonto oder unzureichende Berechtigungen haben können Gesundheitsdaten oder persönliche Daten anderer Benutzer sehen. | | | | | |
| Anforderungen | | | | | |
| Alle Zugriffe auf die Anwendung müssen authentifiziert erfolgen. Umgehung des Einloggens für den Zugriff nicht möglich  DSGVO schreibt Schutz der Daten gesetzlich vor.  BSI CON.10.A1  OWASP ASVS V1.2.3 – Einsatz von sicheren Authentifizierungs-Mechanismen  OWASP ASVS V1.4.5 – attribut- oder merkmalsbasierte Zugriffskontrolle einsetzten  OWASP ASVS 1.8.1 – alle sensitiven Daten müssen identifiziert und klassifiziert werden  Betroffene Assets: A1, A2 | | | | | |
|  | | | | Überprüfung | TestID |
| Benutzerverwaltung und Authentifizierung (Anmeldung) erzwingen vor Zugriff.  Versuchten Zugriff mit Fehlermeldung stoppen. | | | | Manueller Test (Unit-Test) Automatisierter Test | T1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R2 | Benutzer der Anwendung können Gesundheitsdaten oder persönliche Daten anderer Benutzer sehen. | Mittel | Sehr hoch | Hoch | Reduzieren |
| Beschreibung | | | | | |
| Benutzer der Anwendung können ohne Freigabe Gesundheitsdaten oder persönliche Daten anderer Benutzer sehen. | | | | | |
| Anforderungen | | | | | |
| Vor jedem Zugriff sollen die Berechtigungen des Benutzers geprüft werden.   DSGVO schreibt Schutz der Daten gesetzlich vor. CON.10.A2 Zugriffskontrolle bei Webanwendungen  Betroffene Assets: A1, A2 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Authentifizierung (Anmeldung) und Autorisierung (Berechtigungsprüfung) vor Zugriff (siehe R1) erzwingen.  Einblenden einer Fehlermeldung bei versuchtem Zugriff. | | | | Unit Test Automatisierter Test Pentest | T2 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R3 | Informationsabgriff über Datenübertragung | Hoch | Sehr hoch | Hoch | Reduzieren |
| Beschreibung | | | | | |
| Datenübertragung zwischen Webbrowser und Webserver und zwischen Webserver/Webanwendung und DB-Server könnte abgehört werden. Durch das Abfangen der Daten könnten Informationen über Benutzer sichtbar werden. | | | | | |
| Anforderungen | | | | | |
| Alle Kommunikation/Datenübertragung muss sicher (vertraulich, integritätsgeschützt) erfolgen. Auslesen von Informationen über das Mitschneiden der Datenübertragung darf nicht möglich sein.   CON.10.A14 Sichere http-Konfiguration bei Webanwendungen  OWASP ASVS 1.9.1 – Verschlüsselte Kommunikation zwischen Komponenten  OWASP ASVS 1.9.2 – Anwendungs-Komponenten sollen die Authentizität des Kommunikationssenders überprüfen  Betroffene Assets: A1, A2, A3, A4 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Lückenloser Einsatz von HTTPS (HTTP über TLS). | | | | Manueller Test |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R4 | Datenmanipulation und -abfrage | 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. Das Senden von Abfragen via Inputfelder oder URL darf nicht zu einem erfolgreichen Zugriff führen.  OWASP ASVS 4.1.2 - Nicht manipulierbare Daten von Zugriffskontrollen  OWASP ASVS 4.2.2 – Verwendung starker Anti CSRF Funktionen  Betroffene Assets: A1, A2, A3, A4, A5 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Datenübertragung schützen (siehe R3). Eingabevalidierung (Webanwendung)  Zugriffskontrolle (Berechtigungsprüfung) in der Webanwendung + DB-Server. | | | | Manueller Test Design Review | T5  T6 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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.  OWASP ASVS 5.1.1 - Gegen http-Parameter Attacken gesichert  OWASP ASVS 5.1.3 – Inputvalidierung  CON.10.A10 Restriktive Herausgabe sicherheitsrelevanter Informationen  Betroffene Assets: A1-A5 | | | | | |
| 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.  Positive Eingabevalidierung von Feldern | | | | Automatisierter Test Pentest  Code Review (SAST) | T7 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 Verhinderung von Cross-Site-Request-Forgery (CSRF)  CON.10.A9 Schutz vor SQL-Injektion  OWASP ASVS 5.1.3 – Inputvalidierung  OWASP ASVS 1.5.1 – Verarbeitung der Informationen aus Eingabefeldern | | | | | |
| 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 | T7 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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. Je nach Ursache kann dadurch ein Datenverlust hervorgerufen werden. | | | | | |
| 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  Aufbau eines Datenbanksystems mit mindestens 2 Datenbanken. (HA) | | | | Automatisierter Test  Manueller Test | - |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 erlangt 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.  Admin Seite nur über eingeloggten Benutzer mit Administrator-Rechten möglich. | | | | Pentest  Unit-Test | T9 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R9 | Schadcode-Einschleusung durch Datei-Upload | Mittel | Sehr hoch | Mittel | Transferieren |
| Beschreibung | | | | | |
| Durch 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.  CON.10.A5 Upload-Funktionen | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Analyse des Dokuments beim Upload (z.B. mit ClamAV).  Eingrenzen der erlaubten Datei-Formate für den Upload. | | | | Manueller Test Automatisierter Test | T10 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R10 | Auslesen von Informationen über log-Einträge | Mittel | Sehr hoch | Mittel | Transferieren |
| Beschreibung | | | | | |
| Bei unkontrolliertem Code können Informationen in den Log-Einträgen vorhanden sein, wodurch ein Angriff auf die Anwendung möglich wird. | | | | | |
| Anforderungen | | | | | |
| Log-Einträge dürfen keine Informationen über die Anwendung oder die Nutzer der Anwendung preisgeben. Dazu sollten adäquate Richtlinien für Log-Einträge erstellt werden.  OWASP ASVS 1.7.1 – Einheitliches Logging Format  OWASP ASVS 7.1.1 – Keine Anmeldedaten loggen, Session Token nur in gehashter Form  OWASP ASVS 7.1.2 Keine sensitiven Daten loggen  Betroffene Assets: A4, A5 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Print-Befehle aus dem Code entfernen.  Logeinträge nur auf das Nötigste reduzieren. | | | | Manueller Test | - |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R11 | Unerkannte Schwachstellen in dem Code-Repository | Mittel | Hoch | Mittel | Verhindern |
| Beschreibung | | | | | |
| Durch veraltete Pakete oder Bibliotheken können eventuell vorhandene Schwachstellen dieser im eigenen Code zu Angriffspunkten führen. Ebenfalls gefährlich sind verwendete Schlüssel, die sich unwissentlich im Code befinden. | | | | | |
| Anforderungen | | | | | |
| Vor dem Deployment der Anwendung muss der Code auf veraltete Pakete und Bibliotheken (Dependencies) und Secrets hin gescannt werden.  OWASP ASVS 1.14.3 - Pipeline soll vor möglichen Schwachstellen warnen und angemessene Aktionen ergreifen  OWASP ASVS 1.14.4 – Beim Build-Prozess automatisch die Sicherheit überprüfen | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verwenden von CodeQL und Dependabot für das Erkennen von Schwachstellen im Code.  Einbinden von gitleaks für das Scannen nach Secrets. | | | | Automatisierter Test | --- |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R12 | Zugang zu Benutzerkonten durch unzureichende Passwörter | Mittel | Sehr hoch | Gering | Reduzieren |
| Beschreibung | | | | | |
| Durch zu kurze und/oder aus bekannten Eckdaten der Person bestehende Zugangsdaten ist ein Erraten bzw. Brutforcen der Passwörter möglich und somit ein unbefugter Zugriff auf das Benutzerkonto möglich. Falls ein Passwort durch den Nutzer nicht gut genug geschützt wurde oder er es wissentlich oder wissentlich freigegeben hat, führt dies ebenso zu einem potenziellen unbefugten Zugriff. | | | | | |
| Anforderungen | | | | | |
| Passwörter müssen so erstellt werden, dass sie bestimmte Sicherheitsanforderungen erfüllen, um das Risiko des Erratens bzw. Bruteforcens zu verringern. Außerdem muss ein sicheres Zurücksetzten des Passwortes möglich sein.  OWASP ASVS 2.1.1 – Passwörter sollen Mindestlänge von 12 Zeichen erfüllen  OWASP ASVS 2.1.5 - Passwort soll änderbar sein  OWASP ASVS 2.1.11 – Das Einfügen von Passwörtern soll auch über Passwortmanager möglich sein  OWASP ASVS 2.5.4 – Default Benutzerkonten und/oder Accounts wie root sollen nicht vorhanden sein  OWASP ASVS 2.5.1 – Token für das Zurücksetzten von Passwörtern darf nicht im Klartext vorliegen  OWASP ASVS 2.5.2 - Keine Sicherheits-Fragen oder Passwort Tipps  OWASP ASVS 2.5.3 – Passwort zurücksetzten darf nichts über das aktuelle Passwort freigeben | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Passwörter müssen eine Mindestlänge, mindestens eine Zahl haben und keine Ähnlichkeiten zur Person aufweisen.  Zurücksetzten der Passwörter erfolgt über E-Mail und legt zu keinem Zeitpunkt das alte oder neue Passwort frei sowie den dafür benötigten Token. | | | | Manueller Test | -- |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R13 | Benutzung von Sessions durch andere Personen/Benutzer | Mittel | Sehr hoch | Gering | Verhindern |
| Beschreibung | | | | | |
| Durch unsicheren Umgang mit Session-Tokens können andere Personen/Benutzer die Session benutzten, um Zugang zur Anwendung zu bekommen. | | | | | |
| Anforderungen | | | | | |
| Session- Tokens müssen so geschützt sein, dass sie nicht wiederverwendet werden können und nicht offenliegen. Außerdem soll ein Schließen der Session (bzw. Löschen des Session-Tokens) nach einem bestimmten Zeitraum oder Aktion erfolgen.    OWASP ASVS 3.1.1 – Session Tokens nicht als URL-Parameter anzeigen  OWASP ASVS 3.2.1 – Neuen Session Token bei Anmeldung generieren  OWASP ASVS 3.2.4 – Session Tokens werden mit akzeptierten kryptographischen Verfahren erstellt  OWASP ASVS 3.3.1 – Logout soll den aktuellen Session-Token ungültig machen  OWASP ASVS 3.4.1 – bei Session-Tokens soll das „sicher“ Attribut gesetzt sein | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Markieren der Session-Tokens als sicher.  Schließen der Session nach 30 Minuten und bei Schließen des Browsers.  Session-Token nur im gehashtem Zustand übertragen.  Session-Tokens werden nicht in der URL übertragen. | | | | Manueller Test | - |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R14 | DDOS-Angriff auf die Datenbank | Hoch | Mittel | Gering | Verhindern |
| Beschreibung | | | | | |
| Durch eine sehr hohe Anzahl an gleichzeitigen Zugriffen auf die Webanwendung bzw. Datenbank kann der Datenbank-Dienst nicht mehr verfügbar sein und ein Zugriff auf die Datenbank und Webanwendung nicht mehr möglich. | | | | | |
| Anforderungen | | | | | |
| Datenbank muss trotz Ausnahmesituationen verfügbar sein und ihre Aufgaben erfüllen können. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Verbindung zur Datenbank so einrichten, dass auch bei erhöhter Anzahl an Zugriffen die Verbindung nicht abbricht. | | | | Automatisierter Test  Manueller Test | T8 |