Aufgabenstellung Labor “Sichere Systeme”

Agenda

1. Einführung
2. Verwendete Tools
3. Architekturdiagramm
4. Schutzziele
5. Risikoregister
6. Umgesetzte Maßnahmen
7. Testdurchführung
8. Testergebnisse

1. Einführung

Die Webseite ermöglicht es Nutzern, ihre Gesundheitsdaten und Befunde zu verwalten, zu speichern und zu teilen. Nutzer können alle relevanten Daten wie Blutdruck, Blutzucker, Gewicht, Cholesterinwerte und andere wichtige Gesundheitsinformationen hochladen und speichern. Zudem können sie auch ihre persönlichen Befunde, Arztberichte und andere medizinische Dokumente hochladen und speichern.

Die Webseite ermöglicht es den Nutzern auch, ihre Gesundheitsdaten und Befunde mit ihren Ärzten und anderen medizinischen Fachkräften zu teilen. Dies ermöglicht ihnen, schnell und einfach auf medizinische Dienstleistungen zuzugreifen, wenn sie sie benötigen. Außerdem ermöglicht es den Nutzern, die medizinische Versorgung zu überwachen und zu verfolgen, indem sie ihre Gesundheitsdaten und Befunde mit ihren Ärzten und anderen medizinischen Fachkräften teilen und diskutieren.

Die Webseite bietet den Nutzern eine sichere und vertrauliche Umgebung, in der sie ihre Gesundheitsdaten und Befunde speichern, teilen und verwalten können. Die Webseite ist benutzerfreundlich und intuitiv zu bedienen, so dass die Nutzer schnell und einfach auf ihre Daten zugreifen und sie teilen können.

2. Verwendete Tools

Die Anwendung basiert auf dem Python Framework Django. Django abstrahiert viele grundlegende Funktionen von Webanwendungen wie Datenbankverwaltung, Authentifizierung, Suchfunktionen, Kontaktformulare und Content-Management-Systeme, die das Erstellen von Anwendungen vereinfachen. Zusätzlich bietet Django einige Sicherheitsfeatures darunter:

1. Cross-Site Request Forgery (CSRF) Protection: Dieses Feature schützt vor einem Angriff, bei dem böswillige Akteure versuchen, nicht autorisierte Aktionen von einem Benutzer in einer Anwendung auszuführen, indem sie diesen dazu bringen, eine manipulierte Anfrage an die Anwendung zu senden.

2. Benutzerauthentifizierung und Autorisierung: Mit dieser Funktion können Benutzer ihre Identität bestätigen und bestimmen, welchen Berechtigungen sie haben, um bestimmte Aktionen in der Anwendung auszuführen.

3. HTTP-Authentifizierung: Mit dieser Funktion können Benutzer Anforderungen an eine Anwendung senden, die eine Authentifizierung erfordern, bevor sie bearbeitet werden.

4. SSL/TLS-Verschlüsselung: Diese Funktion verschlüsselt Daten, die zwischen einem Server und einem Client übertragen werden, um sicherzustellen, dass diese Daten nicht von Dritten abgefangen werden können.

5. SQL Injection Protection: Diese Funktion schützt vor Angriffen, die versuchen, schädliche SQL-Abfragen über eine Web-Anwendung auf eine Datenbank zu senden.

6. Sichere Passwortspeicherung: Mit dieser Funktion werden Passwörter in einer sicheren Weise verschlüsselt gespeichert, um sicherzustellen, dass sie nicht von Dritten abgefangen oder gelesen werden können.

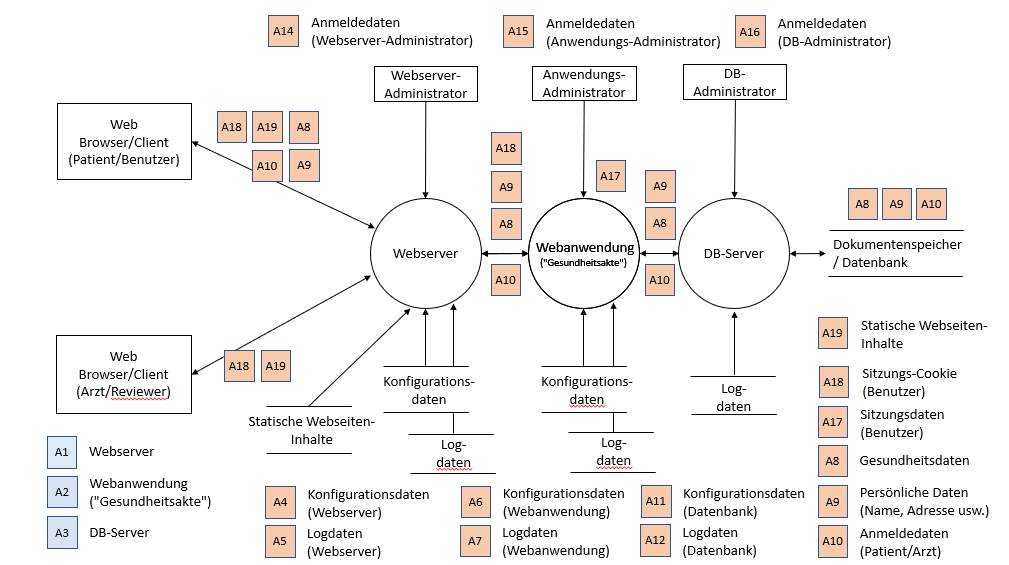
Als IDE wurde wurde hauptsächlich JetBrains PyCharm verwendet. Es bietet intelligente Code-Hervorhebung, Code-Vervollständigung, Refactoring, Debugging, Code-with-Me, Analysetools und ein integriertes Terminal. Es unterstützt auch die Verwendung von Frameworks wie Django.

Jegliche Dateien werden in einer relationalen Datenbank gespeichert, die auf Postgres basiert. Postgres ist eine sehr stabile, performante und skalierbare Datenbank, die eine Vielzahl von Anwendungen unterstützt, und kann problemlos in einer Multi-User-Umgebung betrieben werden. Es ist eine der am weitesten verbreiteten Datenbanken und wird von vielen Unternehmen, Organisationen und Regierungen verwendet.

Zuletzt wurde Github als webbasierte Plattform für die Versionsverwaltung verwendet. Es ermöglicht Benutzern, ein Projekt zu erstellen, es zu teilen, zu verfolgen und zu verwalten. Mit GitHub können Benutzer Projekte auf der Grundlage von Git-Repositories verwalten, zusammenarbeiten und gemeinsam an Code schreiben. Es ermöglicht Benutzern auch, ihre Projekte öffentlich oder privat zu veröffentlichen. Dieses Feature wird auch für die Abgabe verwendet.

3. Architekturdiagramm

Das Architekturdiagramm hat sich im Grunde kaum von der ursprünglichen Konzipierung ab. Da leider Niklas Schmidt nicht mehr Teil der Projektgruppe ist konnten nicht alle funktionalen Features vollständig implementiert werden. Beispielsweise ist eine Registrierung / Anmeldung über einen externen Authentifizierungsdienst wie Google nicht möglich.



4. Schutzziele

Die Schutzobjekte (Entnehmbar aus 3(Architekturdiagram)), besitzen jeweils unterschiedliche Schutzziele. Diese sind hier mit ihren Prioritäten aufgelistet:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Schutzobjekt** | **Beschreibung** | **Vertraulichkeit** | **Integrität** | **Verfügbarkeit** | **Sonstiges/Bemerkungen** |
| A1 | Webserver |  | (2) | (1) |  |
| A2 | Webanwendung |  | (2) | (1) |  |
| A3 | DB-Server |  | (2) | (1) |  |
| A4, A6, A11 | Konfigurationsdaten | (3) | (1) | (2) | Abhängig von den benötigten Inhalten |
| A5, A7, A12 | Logdaten | (3) | (1) | (2) |  |
| A8 | Gesundheitsdaten | (1) | (1) | (2) |  |
| A9 | Persönliche Daten | (1) | (2) | (3) |  |
| A10 | Anmeldedaten | (1) | (2) | (3) |  |
| A1 | Webserver |  | (2) | (1) |  |
| A2 | Webanwendung |  | (2) | (1) |  |
| A3 | DB-Server |  | (2) | (1) |  |
| A4, A6, A11 | Konfigurationsdaten | (3) | (1) | (2) | Abhängig von den benötigten Inhalten |
| A5, A7, A12 | Logdaten | (3) | (1) | (2) |  |
| A8 | Gesundheitsdaten | (1) | (1) | (2) |  |
| A9 | Persönliche Daten | (1) | (2) | (3) |  |
| A10 | Anmeldedaten | (1) | (2) | (3) |  |

5. Risikoregister

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |
| 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) | T7  T8  T9  T10 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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) | T11  T12  T13  T14  T15 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 | | | | | |
| Je nach Ausmaß ist der Schutz durch die DSGVO oder die ISO27001 definiert und muss erfüllt werden. | | | | | |
| 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) | T16  T17  T18  T19  T20 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R6 | Datenbankschwachstellen | [Hoch] | [Hoch] | [Hoch] | [Reduzieren] |
| Beschreibung | | | | | |
| Sicherheitslücke in der Datenbankanwendung wird bekannt | | | | | |
| Anforderungen | | | | | |
| Sicherheitslücken können zu unbefugtem Zugriff führen, bzw. zu einer Manipulation der Daten.  DSGVO schreibt Schutz der Daten gesetzlich vor. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Anwendung muss stets aktuelle gehalten werden.  -Automatische Updates  -Automatisch auf Updates prüfen  -regelmäßiges Patchen | | | | [Manueller Test] [Automatisierter Test] [Pentest] [Design Review] | T21  T22  T23  T24 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R7 | Serverausfall | [Mittel] | [Sehr hoch] | [Mittel] | [Reduzieren] |
| Beschreibung | | | | | |
| Anwendungsserver oder Datenbankserver fällt aus | | | | | |
| Anforderungen | | | | | |
| Verfügbarkeit des Dienstes muss gewährleistet werden. | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Erhöhung der Redundanz durch Servercluster. | | | | [Manueller Test] [Automatisierter Test] | T25  T26 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R8 | Rechenzentrumausfall | [[Niedrig] | [Sehr hoch] | [Niedrig] | [Akzeptieren] |
| Beschreibung | | | | | |
| Rechenzentrum fällt durch ein Erdbeben/Feuer/Flut komplett aus. | | | | | |
| Anforderungen | | | | | |
| ISO 27001 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Geo-Redondanz | | | | [Manueller Test] [Automatisierter Test] | T27  T28 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R9 | DOS-Angriff | [Hoch] | [Mittel] | [Mittel] | [Vermeiden]  [Transferieren] |
| Beschreibung | | | | | |
| Verfügbarkeit muss gewährleistet werden. | | | | | |
| Anforderungen | | | | | |
| ISO 27001  CON.10.A17 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Unterscheidung zwischen normalem und potenziell schädlichem Datenverkehr. Ggf. blockieren.  Bereitstellen von Firewalls.  Beauftragung eines externen Dienstleisters. | | | | [Manueller Test] [Automatisierter Test] [Pentest] | T29  T30  T31 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R10 | Zero Day Exploit | [Mittel] | [Sehr hoch] | [Mittel] | [Reduzieren]  [Akzeptieren] |
| Beschreibung | | | | | |
| Eine Komponente ist von einem Zero Day betroffen | | | | | |
| Anforderungen | | | | | |
| ISO 27001 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Akzeptieren, ggf. offline nehmen des Services.  Finanzielle Absicherung durch Versicherung | | | | [Manueller Test]  [Code Review] | T32  T33 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R11 | SQL-Injection | [Mittel] | [Sehr hoch] | [Mittel] | [Vermeiden] |
| Beschreibung | | | | | |
| Lesender Zugriff auf Datenbankeinträgen und deren Manipulation. | | | | | |
| Anforderungen | | | | | |
| DSGVO schreibt Schutz der Daten gesetzlich vor.  OWASP  CON.10.A9 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Automatischer Pentest  Datenbankzugriffe nur durch das Backend zulassen. | | | | [Manueller Test] [Automatisierter Test] [Pentest]  [Code Review] | T34  T35 T36  T37 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R12 | Falsche oder auch Infizierte Daten werden hochgeladen | [Sehr hoch] | [Mittel] | [Mittel] | [Vermeiden] |
| Beschreibung | | | | | |
| Benutzer lädt falsche Dateitypen hoch, oder gegebenenfalls Malware | | | | | |
| Anforderungen | | | | | |
| Es musss verhindert werden die schadhafte Software hochgeladen werden kann sowie Daten des falschen Datentyps  CON.10.A8 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Scan der Daten die hochgeladen werden, sowie das Whitelisting welche Datentypen von der Webanwendung angenommen werden. | | | | [Manueller Test] [Automatisierter Test] | T38  T40 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R13 | Passwörter von Benutzern haben eine zu geringe Sicherheit | [Sehr hoch] | [Hoch] | [Hoch] | [Reduzieren] |
| Beschreibung | | | | | |
| Benutzer verwenden laut BSI Standard Passwörter, welche nicht den geringst Anforderungen eines sicheren Passwords entsprechen. | | | | | |
| Anforderungen | | | | | |
| BSI-Richtlinie für sichere Passwörter  CON.10.A16 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Mindestanforderungen an Passwörter:  Mindestens 8 Zeichen  Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen  https://www.bsi.bund.de/dok/6596574  Benutzen einer MFA(Multi Factor Authentication) als Alternative. | | | | [Manueller Test] [Automatisierter Test] | T41  T42 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R14 | Fehlerhafte Implementierung von Kryptographie | Niedrig | [Hoch] | [Mittel] | [Vermeiden] |
| Beschreibung | | | | | |
| Kryptographisches Verfahren zur Verschlüsslung von Passwörtern wurde nicht korrekt implantiert. Damit ist es einfacher diese zu entschlüsseln, wenn Passwörter entwendet oder geleakt werden aus der Datenbank, in der sie gespeichert wurden. | | | | | |
| Anforderungen | | | | | |
| Passwörter müssen sicher verschlüsselt werden, wenn diese in der Datenbank gespeichert werden oder deren Hashes  CON.10.A18 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Mit Hilfe des Datenblattes und der Hersteller Anleitung soll das Kryptographisches Verfahren implementiert und geprüft werden, ob dieses korrekt agiert. | | | | [Manueller Test] [Automatisierter Test] [Design Review]  [Code Review] | T43  T44  T45  T46 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R15 | Kompromittierte Passwörter | [Mittel] | [Hoch] | [Mittel] | [Reduzieren] |
| Beschreibung | | | | | |
| Passwörter von Benutzerkonten werden durch bspw. R4 oder durch Wiederverwendung auf anderen Webseiten/ Phishing kompromittiert | | | | | |
| Anforderungen | | | | | |
| DSGVO schreibt Schutz der Daten gesetzlich vor.  CON.10.A16 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Durch 2FA können Accounts mit kompromittierten Passwörtern trotzdem vor fremden Zugriff geschützt werden. | | | | [Manueller Test] [Automatisierter Test] [Pentest] | T47  T48  T49 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RisikoID | Bedrohung | Eintrittswahrscheinlichkeit | Auswirkungen | Risiko | Behandlung |
| R16 | Brute-Force | [Hoch] | [Hoch] | [Hoch] | [Reduzieren] |
| Beschreibung | | | | | |
| Durch einen Brute-Force-Angriff kann das Passwort zu einem Benutzeraccounts durch ständiges Testen von zufälligen Kombinationen “erraten werden” | | | | | |
| Anforderungen | | | | | |
| Benutzerkonnten müssen vor Brute-Force angriffen geschützt werden.  CON.10.A6  CON.10.2.6 | | | | | |
| Maßnahmen | | | | Überprüfung | TestID |
| Bei mehrfacher (5-mal) falscher Eingabe des Passworts, werden weitere Eingaben erst nach einer Minute angenommen und dem Benutzer erscheint dies bezüglich eine Meldung  Einführung einer MFA (Multi Factor Authentication) | | | | [Manueller Test] [Automatisierter Test] [Pentest] | T50  T51  T52 |

6. Umgesetzte Maßnahmen

|  |  |  |  |
| --- | --- | --- | --- |
| **RisikoID** | **Bedrohung** | **Risiko-bewertung** | **Umgesetzte Maßnahmen** |
| R1 + R2 | Benutzer oder unangemeldete Dritte können Gesundheitsdaten oder persönliche Daten anderer Benutzer sehen. | Hoch | Zugriff ist ohne Anmeldung nicht möglich, jeder Nutzer erhält nur die für ihn freigegebenen Dokumente und kann nicht nach anderen Nutzern oder Dokumenten suchen |
| R3 | Sicherheit der Datenübertragung | Hoch | Anwendung läuft ausschlich lokal und benötigt zunächst kein HTTPS |
| R4 | Datenbankmanipulation | Hoch | Anwendung ist sicher gegen SQL-Angriffe, jeglicher Zugriff auf die Datenbank wird vom Django-Framework gehandhabt |
| R5, R6 | Webserver/Datenbank-Schwachstellen | Hoch | Es verbleiben typische Schwachstellen die regelmäßige Wartung erfordern |
| R9 | DOS-Angriffe | Mittel | Wird entsprechend an den Server-Host weitergegeben |
| R10 | Zero Day | Mittel | Erfordert entsprechend schnelle Reaktionszeit und Updates – Keine präventiven Maßnahmen möglich |

|  |  |  |  |
| --- | --- | --- | --- |
| **RisikoID** | **Bedrohung** | **Risiko-bewertung** | **Umgesetzte Maßnahmen** |
| R11 | SQL-Injection | Mittel | Anwendung ist sicher gegen SQL-Angriffe, jeglicher Zugriff auf die Datenbank wird vom Django-Framework gehandhabt |
| R12 | Falsche oder auch Infizierte Daten werden hochgeladen | Mittel | Nutzer können nur vorbestimmte Dateitypen hochladen, Infizierte Dateien müssten mithilfe eines Scanners erkannt werden |
| R13 | Passwörter haben eine zu geringe Sicherheit | Hoch | Passwortkomplexität wird vor der Registrierung geprüft |
| R14 | Fehlerhafte Implementierung von Kryptographie | Mittel | Django handhabt jegliche Kryptographie selbst |
| R15 | Kompromittierte Passwörter | Mittel | Wird entsprechend an den Server-Host weitergegeben |
| R16 | Brute-Force | Hoch | Integration von Captcha beim Login |

7. Testdurchführung

Die Tests wurden nach Rücksprache mit dem Dozenten mithilfe eines automatischen Penetration-Test-Tools durchgeführt. Pentesttools.com ist eine Website, auf der Benutzer verschiedene Tools und Dienste rund um Penetrationstests finden können. Auf der Website finden sie eine Vielzahl von Tools, die Benutzer zum Testen der Sicherheit einer Website oder eines Netzwerks verwenden können. Außerdem bietet die Website eine Vielzahl von Tutorials und Netzwerk- und Sicherheitsressourcen, die Benutzer bei der Planung und Durchführung von Penetrationstests unterstützen.

8. Testergebnisse

Details zu den durchgeführten Tests und ihre Ergebnisse finden sich im Abgabe [GitHub-Repository](https://github.com/vNmven0m/DHBW_SbD).