Aufgabenstellung Labor "Sichere Systeme" Modul „Security by Design"- WS 2022

Aufgabenstellung

Erstellen Sie eine Webanwendung für die Speicherung und Verwaltung persönlicher medizinischer Daten und Befunde (persönliche Gesundheitsakte). Nutzer der Anwendung sollen über einen Webbrowser auf die Anwendung zugreifen, persönliche Daten pflegen und eigene medizinische Daten und Befunde erstellen bzw. hochladen, einsehen und verwalten können. Darüber hinaus soll es möglich sein, ausgewählte Informationen und Dokumente aus der persönlichen Gesundheitsakte mit ausgewählten Ärzten und anderen Personen zu teilen bzw. lesenden Zugriff zu ermöglichen.

Aufgaben im Einzelnen

Da die Aufgabe dem Zweck dienen soll, Grundlagen zur Konzeption und Bereitstellung sicherer Systeme zu erlernen und zu erproben, werden keine umfangreichen oder besonderen Anforderungen hinsichtlich Umfang, Funktionalität und anderer nicht-funktionaler Eigenschaften gestellt. Die Anwendung soll grundsätzlich im oben beschriebenen Umfang benutzbar sein und korrekt funktionieren, es kommt aber nicht auf eine Vielzahl von Auswahlmöglichkeiten, Dokumentenformate, besondere Ergonomie der Benutzeroberfläche oder Performanz der Antwortzeiten an. Der Fokus der Anforderungen und gewünschten Eigenschaften soll auf dem Thema Sicherheit liegen.

1. Identifizieren, präzisieren und dokumentieren Sie zunächst die in diesem Geschäftsumfeld (*business context*) zu erwartenden zu schützenden Objekte, deren Schutzziele und Sicherheitsanforderungen. Berücksichtigen Sie dabei auch Ihnen bekannte rechtliche und regulatorische Vorschriften (*regulatory context*). Entwerfen Sie dann eine geeignete Architektur und wählen Sie eine geeignete Technologie bzw. Plattform zur Realisierung der Anwendung (*technology context*). Überprüfen und ergänzen Sie zu schützende Objekte, Schutzziele und Sicherheitsanforderungen mittels einer architektonischen Bedrohungsanalyse (*threat modeling*).

2. Erstellen Sie ausgehend von den Ergebnissen der architektonischen Bedrohungsanalyse ein Register für die in Ihrem Projekt identifizierten Sicherheitsrisiken. Bestimmen Sie dazu Eintrittswahrscheinlichkeit und mögliche Schäden der identifizierten Bedrohungen und das daraus resultierende Risiko. Entscheiden Sie für jedes Risiko wie es behandelt werden soll und im Falle einer Reduzierung, welche Maßnahmen dafür durchgeführt werden und wie diese überprüft werden sollen. Dokumentieren Sie Ihre Ergebnisse im Risikoregister Ihres Projektes.

3. Implementieren Sie die Anwendung unter Berücksichtigung der identifizierten Anforderungen, Risiken, den zur Risikobehandlung festgelegten Maßnahmen und allgemeinen Grundlagen sicheren Programmierens.

4. Testen und überprüfen Sie die Anwendung hinsichtlich der Grundfunktionalität, den identifizierten Sicherheitsanforderungen und den zur Risikobehandlung implementierten Maßnahmen. Erstellen Sie dazu einen Testplan, nutzen Sie geeignete Testmethoden und -werkzeuge und dokumentieren Sie die Testergebnisse.

5. Führen Sie die Schritte 1.-4. im Entwicklungs- und Bereitstellungsprozess in geeigneter Weise verzahnt und wiederholt durch.

Durchführung und Bewertung

Die Aufgabe soll in Gruppen von jeweils 3 Personen bearbeitet werden (in Ausnahmefällen, bzw. wenn notwendig auch 2 Personen nach Abstimmung mit dem Dozenten).

Teil 1. der Aufgabenstellung wird im Kurs zusammen in einer der sechs Laboreinheiten begonnen und dann in den Gruppen geeignet fortgeführt.

Die ersten Ergebnisse der Teile 1. und 2. werden in weiteren Laboreinheiten in der ersten Hälfte des Laborprojektes von jeder Gruppe präsentiert und vom Dozenten bewertet (siehe dazu „Bewertungsschema“ unten). Dabei ist darauf zu achten, dass alle Personen in jeder Gruppe ihren jeweiligen Teil präsentieren und in gemeinsamer wissenschaftlicher Diskussion erläutern können.

Die Ergebnisse der Teile 3. und 4. werden in weiteren Laboreinheiten in der zweiten Hälfte des Laborprojektes von jeder Gruppe präsentiert und vom Dozenten bewertet (siehe dazu „Bewertungsschema“ unten). Dabei ist darauf zu achten, dass alle Personen in jeder Gruppe ihren jeweiligen Teil präsentieren und in gemeinsamer wissenschaftlicher Diskussion erläutern können.

Die Dokumentation der zu schützenden Objekte, der Schutzziele und der Sicherheitsanforderungen, der Bedrohungsanalyse, das Risikoregister der Sicherheitsrisiken inklusive der Risikobehandlung und Maßnahmen sowie Source Code, Testpläne und Testergebnisse werden vom Dozenten pro Gruppe bewertet. Die aufgeführten Einzelbewertungen werden vom Dozenten in eine Gesamtbewertung pro Gruppe zusammengeführt (siehe dazu „Bewertungsschema“ unten).

Die in den Laboreinheiten nicht für gemeinsame Aufgaben, Präsentationen und Diskussionen benötigte Zeit wird geeignet zur Arbeit in den einzelnen Gruppen und zum Wissensaustausch zwischen den Gruppen und dem Dozenten genutzt.

Bewertungsschema

	Prozent	Punkte	Kriterien
Anwendungsarchitektur, Schutzobjekte, Schutzziele und Sicherheitsanforderungen, Bedrohungsanalyse, Risikoregister, Risikobehandlung und Maßnahmen	30%	36	Vollständigkeit (12) Verständlichkeit (12) Angemessenheit (12)
Lauffähige Anwendung, Komponenten und Modulaufbau, Testplan, Werkzeuge und Testergebnisse	50%	60	Angemessenheit und Korrektheit der programmtechnischen Umsetzung (40) Angemessenheit, Abdeckung und Automatisierung des Testplans (20)
Review der Dokumentation, des Source Codes, des Testplans und der Testergebnisse	20%	24	Struktur, Verständlichkeit und Konsistenz zur Präsentation (24)
Gesamt	100%	120	

Punkte	Note
120	1,0
118-119	1,1
116-117	1,2
114-115	1,3
112-113	1,4
110-111	1,5
108-109	1,6
106-107	1,7
104-105	1,8
102-103	1,9
100-101	2,0
98-99	2,1
96-97	2,2
94-95	2,3
92-93	2,4
90-91	2,5
88-89	2,6
86-87	2,7
84-85	2,8
82-83	2,9
80-81	3,0
78-79	3,1
76-77	3,2
74-75	3,3
72-73	3,4
70-71	3,5
68-69	3,6
66-67	3,7
64-65	3,8
62-63	3,9
60-61	4,0
<60	NB