[root@netsec]>

IT Security

Klausur an der Hochschule Karlsruhe - Technik und Wirtschaft
Wintersemester 2021/22, Mittwoch, 02.02.2022, 14:00 Uhr

Name:_____ Punkte:_____/100 (40 zum Bestehen) Note:____

Disclaimer:
- Zugelassene Hilfsmittel: keine ausser Stifte und Lineal
- Der Lösungsweg muss bei allen Aufgaben ersichtlich sein

Aufgabe 1: Begriffswelt

__/10 __/10 Punkte

Sie sind Haupt-Committer des verbreiteten Open-Source Frameworks „log4K“, mit dem vor allem Medienwiedergabe vorzüglich in Überwachungsinfrastrukturen integriert werden kann.

Security hat einen hohen Stellenwert in solch verbreiteten Open-Source Infrastrukturen und Sie bemühen sich um Informationen für die breite Öffentlichkeit. Wie assoziieren Sie die Begriffe in den Spalten A und B? Bitte verbinden!

Spalte A	
Compliance	Funktionsbeteiligt
Zuverlässigkeit	Topologische Maßnahme
Statische Redundanz	Protokollschwäche
Hierarchisches Modell	Return Address
Insel	Risiko Management
Circuit Level Proxy	Zertifizierbar
DoS	Zeitintervall
Buffer Overflow	Threat Modelling
Entwurfsphase	Composed of
ISO 27001	Transportschicht

Aufgabe 2: Safety

A)__/8 B)__/8 C)__/6 D)__/6 E)__6 __/34 Punkte

A) Wenn Sicherheitslücken in einem so erfolgreichen Projekt wie log4K gefunden werden – dann ist es natürlich enorm wichtig, dass sie schnell gefixt werden. Allerdings gehen Sie als Haupt-Commiter sehr gerne Snowboarden, weshalb Ihre Verfügbarkeit nur bei 50% liegt. Ihr Co-Committer hat dasselbe Hobby, weswegen er auch nur eine Verfügbarkeit von 50% hat. Ein weiterer Committer mag keinen Wintersport und ist daher zu 75% verfügbar. Zudem sind Sie alle auf die Build Infrastruktur angewiesen welche, laut dem Anbieter Gridpub, eine Verfügbarkeit von 80% bietet. Wie hoch ist die Gesamtverfügbarkeit Ihres Projektes in Bezug auf die Lieferfähigkeit von Bugfixes?

Tipp: Bruchrechnen…

B) Ein Unternehmen, welches durch die Nutzung von Ihrem Projekt log4K sehr, sehr erfolgReich wurde möchte Ihr Projekt finanziell unterstützen. Sie könnten das Geld selbst einstecken und Ihre Verfügbarkeit auf 80% erhöhen (leider indem Sie als Konsequenz etwas weniger Snowboarden gehen) oder einen 2. Anbieter einer alternativen Buildinfrastruktur hinzunehmen, der ebenfalls eine Verfügbarkeit von 80% garantiert. Zeigen Sie (durch Berechnung) welche Variante die höhere Gesamtverfügbarkeit Ihres Projektes zur Folge hätte.

C) Erklären Sie bitte: Handelt es sich bei Ihrer Betrachtung in A) und B) eher um eine Frage der Zuverlässigkeit oder der Verfügbarkeit im Sinne der Vorlesungsdefinition?

D) Die Zuordnung zu verschiedenen Maßnahmen-Klassen ist im Lastenheft wohl auch noch nicht ausgefüllt worden. Bitte helfen Sie, indem Sie die Maßnahmen den Schutzzielen in der unten stehenden Tabelle zuordnen:

	Redundanz	**„Firewall++“**	**Kryptographie**	**Policies**
Verfügbarkeit				
Integrität				
Vertraulichkeit				
Zurechenbarkeit				
Rechtsverbindlichkeit				

E) Machen Sie bitte für alle in D) gefundenen Zuordnungen jeweils sehr kurz einen konkreten Umsetzungs- / Implementierungsvorschlag.

Aufgabe 3: Security

A)__/5 B)__/5 C)__/5 D)__/5 E)__/7 F)__/6 G)__/6 H)__/7 I)__/5 J)__/5 __/56 Punkte

A) Für Log4K ist ein sicherer Entwicklungsprozess erforderlich. Ordnen Sie die SSDLC Aktivitäten der richtigen Phase zu:

Anforderungsphase	Fuzzing Tests
Entwurfsphase	Bedrohungsmodellierung
Entwicklungsphase	Reaktionsplan
Überprüfungsphase	Risikobewertung
Deploymentphase	Statische Code Analyse

B) Neben technischen Maßnahmen sind auch Regeln ein wichtiger Mechanismus, um Security zu stärken. Entwerfen Sie eine Policy (min. 5 Regeln) für Freiwillige, die sich an Ihrem Open-Source Projekt bei gridpub beteiligen möchten.

C) Identitäten spielen bei der Sicherheit eine große Rolle. Welche Identitäten auf welchen (Protokoll-) Ebenen kennen Sie bei einem öffentlichen Web-Server? Nennen Sie jeweils eine Möglichkeit, diese zu Spoofen und beschreiben Sie im Sinne eines Threat Models welche Maßnahmen Sie empfehlen würden um diese Angriffe zu verhindern.

D) Sie haben im Support-Blog für Ihre Open-Source Software eine Persistent/Stored XSS Lücke vom berühmten Bughunter Lord "R00b1n ^" gemeldet bekommen.
Welche Konsequenzen kann die Lücke für die Besucher der Webseite haben?

E) Informieren Sie die Öffentlichkeit, indem Sie (am besten mit Hilfe einer Skizze) erklären, wie so ein XSS Angriff abläuft!

F) Welche Hinweise/Strategien/Regeln könnten Sie Ihren Committern geben, damit sie in Zukunft keine XSS Lücken mehr programmieren?

G) Könnte ein Angreifer mit Hilfe einer XSS Lücke euch ein (D)DoS Angriff durchführen? Falls ja: erweitern oder erneuern Sie die Skizze aus E) entsprechend.

H) Schreiben Sie in Pseudocode einen Scanner, welcher „im Internet“ nach Installationen von log4K sucht und alarmiert wenn die Versionsnummer nicht aktuell ist (und somit eine bekannte Sicherheitslücke existiert).

I) Beschreiben Sie (kurz) in welchen Phasen ein Cyberangriff üblicherweise abläuft und für jede Phase (in Stichpunkten) was das Ziel der Phase ist.

J) Sie befassen sich mit Möglichkeiten, die Sicherheitsmechanismen bei der Entwicklung Ihres Open Source projektes zertifizieren zu lassen. Welche der folgenden Möglichkeiten spielen können hierzu sicherlich nicht herangezogen werden (bitte streichen):

- IT 32005
- ISO Common
- ISO 27001
- IT Mundschutz
- IT-Grundschutz