NAME DES DOZENTEN: TIMO PAGEL / BJÖRN KIMMINICH

KLAUSUR: IT-SICHERHEIT / A18 A + B

QUARTAL: (3/2021)

Name des Prüflings: Matrikelnummer: Zenturie:

_____ _____ _____

Dauer : 90min

Datum: XX.XX.2021

Seiten der Klausur **mit** Deckblatt:

Hilfsmittel: Taschenrechner

Bemerkungen:

- ***Bitte prüfen Sie zunächst die Klausur (alle Teile) auf Vollständigkeit***
- **Bitte lösen Sie nicht die Heftung**

Es sind 120 Punkte erreichbar!
Zum Bestehen der Klausur sind 60 Punkte ausreichend!

Aufgabe	**Erreichbare Punkte**	**Erreichte Punkte**
1	10	
2	13	
3	19	
4	12	
5	20	
6	16	
7	16	
8	14	
Summe	**120**	

Note:_____ Prozentsatz: _____ Ergänzungsprüfung:_____

Datum:_____ Unterschrift:_____

Datum:_____ Unterschrift:_____

Aufgabe 1 (10 Punkte)

	Beantworten Sie die folgenden Fragen:	**stimme zu**	**stimme nicht zu**
a)	Eine Allowlist wird umso sicherer, je mehr Dinge sie explizit verbietet.		
b)	Ein Virtual Private Network dient immer dem Zugang zu einem Intranet vom Internet aus.		
c)	Würmer sind Viren mit Schadcode von mindestens 42 Zeilen Länge.		
d)	Geheim gehaltene Verschlüsselungsalgorithmen sind sicherer als öffentliche.		
e)	Das Signieren von E-Mails stellt deren Integrität sicher.		
f)	Viren verbreiten sich heutzutage ausschließlich über Phishing E-Mails.		
g)	Trojaner verbreiten sich eigenständig von System zu System.		
h)	Nur hochwertige Netzwerk-Firewalls schützen Systeme vor Zero-Day Exploits.		
i)	Vertraulichkeit, Integrität & Abstreitbarkeit sind die 3 zentralen IT-Schutzziele.		
j)	Die Integrität kann nur durch aktive Angriffe beeinträchtigt werden.		

Jede richtige Antwort wird mit 1 Punkt, jede falsche oder nicht gegebene Antwort mit 0 Punkten bewertet.

Aufgabe 2 (13 Punkte)

(2.1) (4 Punkte) Nennen Sie zwei konkrete Arten von Malware, sowie stichpunkthaft deren Wirkungsweise und übliche Verbreitungsmethode.

Malware	**Wirkung / Verbreitung**

(2.2) (2 Punkte) Nennen Sie zwei mögliche Methoden die Verfügbarkeit eines Systems sicherzustellen.

(2.3) (4 Punkte) Nennen Sie zwei konkrete Anwendungsfälle von Verbindungsverschlüsselung inkl. eines dafür verwendeten Protokolls oder Verfahrens.

Anwendungsfall	**Protokoll / Verfahren**

(2.4) (3 Punkte) Erläutern Sie kurz die Aufgaben eines Cyber Incident Response Teams (CIRT) im Vergleich zu einem Security Operations Center (SOC).

Aufgabe 3 (19 Punkte)

(3.1) (13 Punkte) Nennen Sie alle Risiken auf der OWASP Top 10 von 2017. Kreuzen Sie anschließend an, welches die drei höchstplatzierten Risiken sind. Die Angabe der exakten Reihenfolge ist nicht nötig.

Risiko	**Top 3?**

(3.2) (6 Punkte) Um was für ein Projekt handelt es sich beim OWASP Juice Shop? Erläutern Sie mögliche Zielgruppe(n) und Einsatzszenarien für dieses Projekt.

Aufgabe 4 (12 Punkte)

(4.1) (4 Punkte) Erläutern Sie kurz den Zweck von Input Validation bei Webanwendungen. Worauf muss man als Entwickler besonders achten?

(4.2) (4 Punkte) Erläutern Sie die bestgeeigneten Maßnahmen zur Verhinderung von Injection Schwachstellen allgemein.

(4.3) (4 Punkte) Welche spezifischeren Maßnahmen können gegen eine SQL Injection getroffen werden?

Aufgabe 5 (20 Punkte) Erläutern Sie im Detail die Angriffe Reflected XSS und DOM XSS. Verdeutlichen Sie dabei wesentliche Unterschiede zwischen diesen beiden Varianten von Cross-Site Scripting.

Aufgabe 6 (16 Punkte)

(6.1) (7 Punkte) Skizzieren Sie den Vorgang der Serialisierung und Deserialisierung von Daten.

(6.2) (4 Punkte) Erläutern Sie mögliche Angriffe gegen einen unsicheren Deserialisierungvorgang.

(6.3) (5 Punkte) Nennen Sie fünf mögliche Präventionsmaßnahmen gegen Deserialisierungsangriffe.

Aufgabe 7 (16 Punkte)

(7.1) (6 Punkte) Erläutern Sie die Methodik des Static Application Security Testing (SAST).

(7.2) (10 Punkte) Grenzen Sie die Stärken und Schwächen von SAST gegeneinander ab.

Stärken	**Schwächen**

Aufgabe 8 (14 Punkte)

(8.1) (6 Punkte) Erläutern Sie ausführlich drei unterschiedliche Authentifizierungsfaktoren.

(8.2) (8 Punkte) Wie können Passwörter besonders sicher gespeichert und gegen Brute-Force Angriffe resistent gemacht werden?

Viel Erfolg!