

IT 5 - Sicherheit mit Köpfchen

Zugänge schützen und typische Denkfehler erkennen



Für die Spielleitung: pro Hauptfrage ein Punkt. Sinngleiche Antworten und angegebene Varianten gelten. Mehrere verlangte Angaben zählen nur gemeinsam. Quellen sind anklickbar; eigene Knobelaufgaben sind ausdrücklich markiert.

RUNDE 01 / 05 FRAGEN

Wer darf hinein?

01 Authentifizierung

Auch richtig: Authentication

Sie klärt die Identität, noch nicht sämtliche erlaubten Aktionen.

Quelle: [OWASP: Autorisierung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

02 Autorisierung

Auch richtig: Authorization

Sie entscheidet über Berechtigungen für die konkrete Aktion.

Quelle: [OWASP: Autorisierung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

03 Zwei

Auch richtig: 2

Beispielsweise Wissen und Besitz; zwei Merkmale derselben Kategorie reichen nicht.

Quelle: [OWASP: Mehrfaktor-Authentifizierung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

04 Nein

Beide sind Wissensmerkmale und gehören zur gleichen Faktorkategorie.

Quelle: [OWASP: Mehrfaktor-Authentifizierung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

05 Biometrisches Merkmal

Auch richtig: Biometrie; Etwas, das man ist

Die Kategorie wird auch als etwas, das man ist, beschrieben.

Quelle: [OWASP: Mehrfaktor-Authentifizierung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

IT 5 - Sicherheit mit Köpfchen

RUNDE 02 / 05 FRAGEN

Passwörter richtig bewahren

06 Passwort-Hashing

Auch richtig: Hashing; Hashen

Dafür braucht es ein geeignetes, langsames Passwortverfahren mit zusätzlicher Absicherung.

Quelle: [OWASP: Passwortspeicherung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

07 Salt

Er sollte für jedes gespeicherte Passwort individuell erzeugt werden.

Quelle: [OWASP: Passwortspeicherung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

08 Pepper

Anders als individuelle Zufallszusätze ist dieser Wert geheim zu halten.

Quelle: [OWASP: Passwortspeicherung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

09 Argon2id

Bloßes SHA-256 ist für Passwortspeicherung zu schnell und erleichtert massenhaftes Raten.

Quelle: [OWASP: Passwortspeicherung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

10 Mehr Rechenaufwand

Auch richtig: Die Prüfung wird aufwendiger

Das verteuert sowohl legitime Prüfungen als auch massenhaftes Raten.

Quelle: [OWASP: Passwortspeicherung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

IT 5 - Sicherheit mit Köpfchen

RUNDE 03 / 05 FRAGEN

Webanwendungen absichern

11 Parametrisierte Abfragen

Auch richtig: Prepared Statements mit Parametern

Werte werden gebunden, statt als Teil des SQL-Textes zusammengesetzt.

Quelle: [OWASP: SQL-Injection verhindern \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/OWASP_SQL-Injection_verhindern.html)

12 Passende Ausgabekodierung

Auch richtig: HTML-Escaping; Output Encoding

Die Kodierung muss zum jeweiligen Ausgabe-Kontext passen.

Quelle: [OWASP: XSS verhindern \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/OWASP_XSS_verhindern.html)

13 Cross-Site Request Forgery

Auch richtig: CSRF

Er erschwert fremd ausgelöste, unerwünschte Aktionen im Kontext einer angemeldeten Sitzung.

Quelle: [OWASP: CSRF verhindern \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/OWASP_CSRF_verhindern.html)

14 TLS 1.3

Auch richtig: TLS; Transport Layer Security

Es sichert die Kommunikation zwischen den beteiligten Endpunkten.

Quelle: [RFC 8446: TLS 1.3 \(rfc-editor.org\)](https://rfc-editor.org/rfc/8446)

15 Nein

Protokolle dürfen nicht zu einer zusätzlichen Sammlung nutzbarer Zugangsdaten werden.

Quelle: [OWASP: Sicherheitsprotokollierung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/OWASP_Sicherheitsprotokollierung.html)

IT 5 - Sicherheit mit Köpfchen

RUNDE 04 / 05 FRAGEN

Berechtigungen und Betrieb

16 Prinzip der geringsten Rechte

Auch richtig: Least Privilege

Unnötige Rechte vergrößern den möglichen Schaden bei Fehlern oder kompromittierten Konten.

Quelle: [OWASP: Autorisierung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

17 Deny by Default

Auch richtig: Standardmäßig verweigern

Ein fehlender Erlaubnisfall soll nicht unbeabsichtigt Zugriff freigeben.

Quelle: [OWASP: Autorisierung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

18 Nein

Die Berechtigung muss an einer vertrauenswürdigen Stelle serverseitig geprüft werden.

Quelle: [OWASP: Autorisierung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

19 Wann, wo, wer und was

Auch richtig: When, where, who, what

Zeit, Herkunft beziehungsweise Ort, Akteur und Ereignis machen Vorfälle nachvollziehbar.

Quelle: [OWASP: Sicherheitsprotokollierung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

20 Wiederherstellungscodes

Auch richtig: Recovery Codes; Backup-Codes

Sie müssen geschützt aufbewahrt werden und sind nicht für die Weitergabe bestimmt.

Quelle: [OWASP: Mehrfaktor-Authentifizierung \(cheatsheetseries.owasp.org\)](https://cheatsheetseries.owasp.org/)

STICHFRAGE - NUR BEI GLEICHSTAND**1.000.000**

$10 \text{ hoch } 6 = 1.000.000$. Es zählt die kleinste absolute Abweichung.

Eigene Rätselaufgabe - Herleitung oben.

Neue Quizze? Zum kostenlosen Newsletter.

kneipenquiz.org/newsletter

Materialideen: kneipenquiz.org/quizmaterial

Dort: gekennzeichnete Amazon-Werbelinks.

