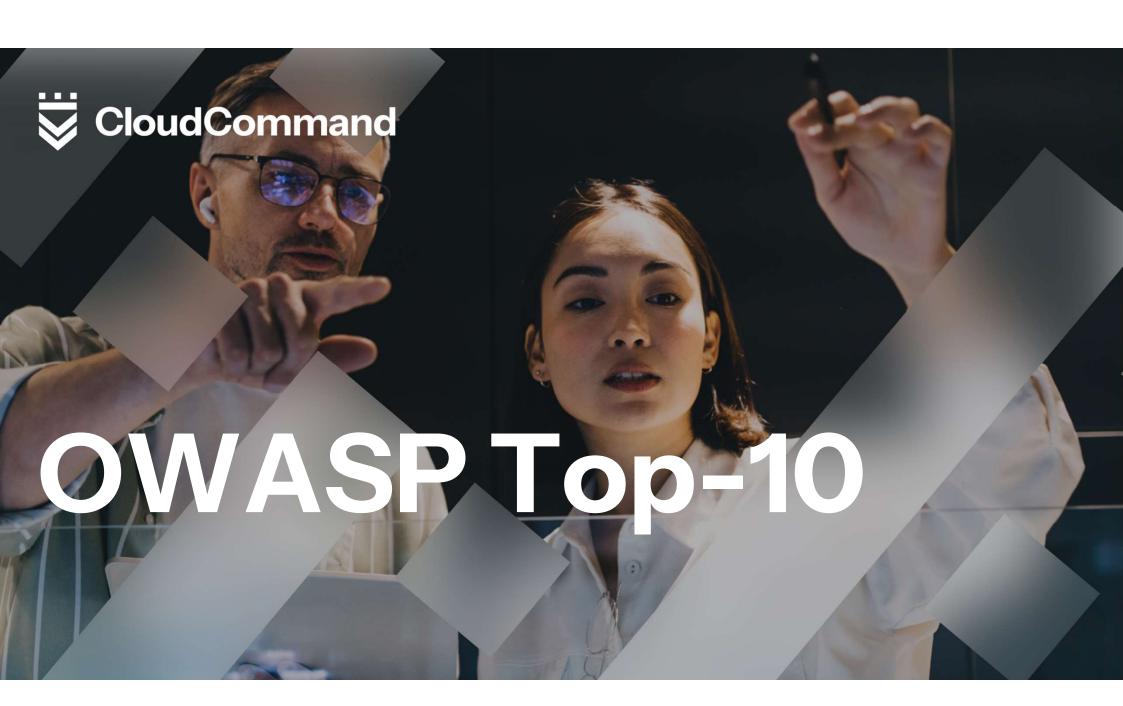


Cyber Security



AGENDA

OWASP Top-10 Liste:

01	Broken Access Control
02	Cryptographic Failures
03	Injection
04	Insecure Design
05	Security Misconfiguration



AGENDA

OWASP Top-10

06	Vulnerable and Outdated Components
07	Identification and
	Authentication Failures
08	Software and Data Integrity Failures
09	Security Logging and
	Monitoring Failures
10	Server-Side-Request Forgery (SSRF)



AGENDA

O1 Kurze Wiederholung



BASICS

01 – kurze Wiederholung

- Zielsetzung:

OWASP ist eine internationale Non-Profit-Organisation, die sich auf die Verbesserung der Sicherheit von Softwareanwendungen konzentriert.

- Open Source:

Alle Materialien, Tools und Projekte von OWASP sind frei verfügbar und quelloffen.

- Community-basiert:

OWASP lebt von einer aktiven Community aus Entwicklern, Sicherheitsexperten und Interessierten weltweit.

- Einfluss auf Standards:

OWASP wird von Unternehmen, Entwicklern und auch Gesetzgebern als Standard und Referenz in Sachen Anwendungssicherheit genutzt.



BASICS

01 – kurze Wiederholung

- Ausgeschrieben bedeutet OWASP:
 Open Web Application Security Project
- OWASP Top10 ist eine Liste der 10 relevantestens Gruppen an Schwachstellen in Webseiten bzw. Web-Applikationen
- Fokus auf Webseiten/ Webservern
 Die Liste ist nicht allumfassend, sondern beschreibt lediglich die 10 häufigsten Angriffe.
- Wird alle Paar Jahre angepasst -> wir betrachten OWASP 2021
 (Die aktuellste Liste findet sich auf Github.)



Gibt es noch Fragen?



