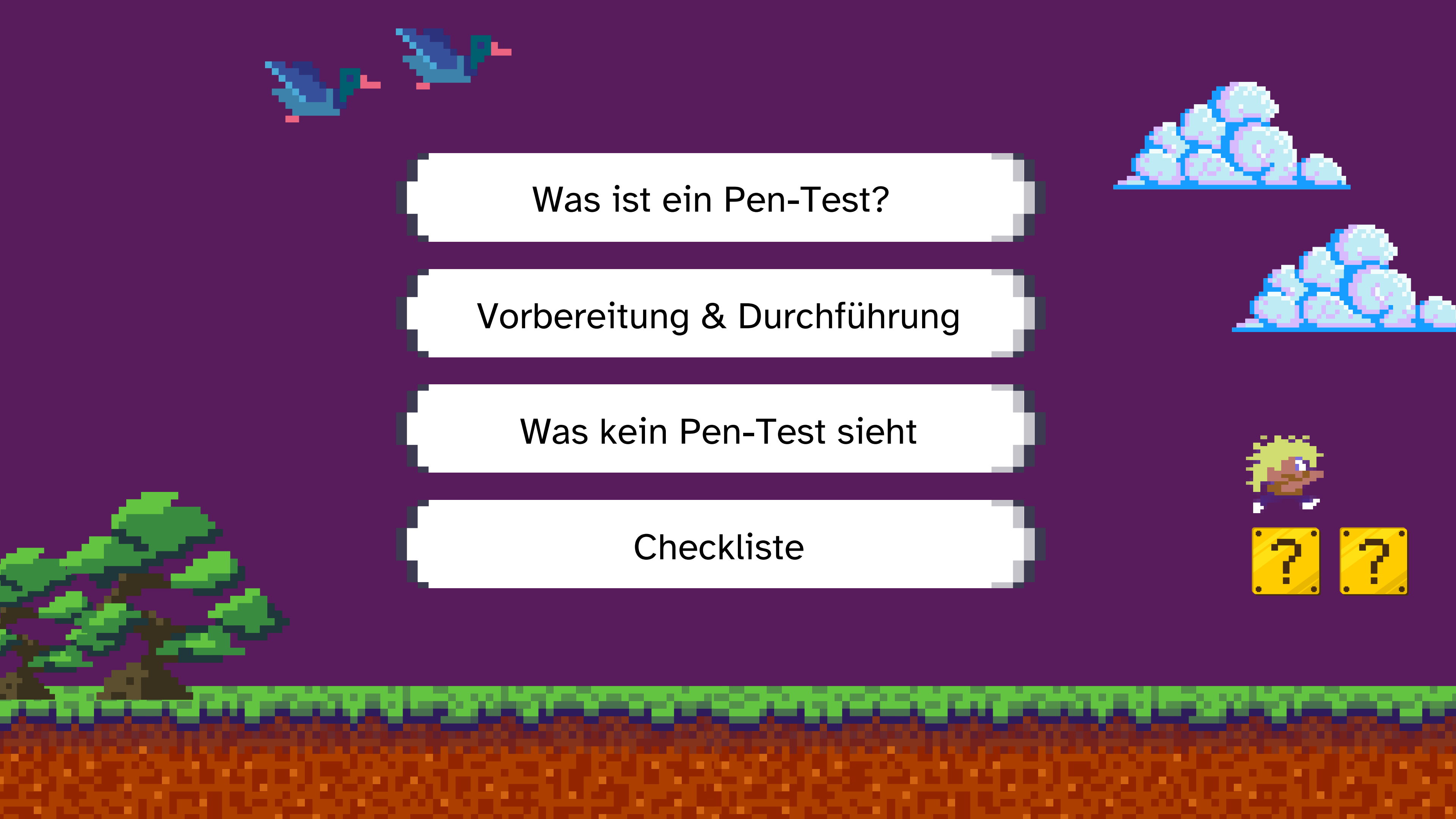


ANGRIFF IST DIE BESTE VERTEIDIGUNG: WORDPRESS UNTER BESCHUSS

WordCamp Mannheim | 04.07.2026 | Manja Neumann



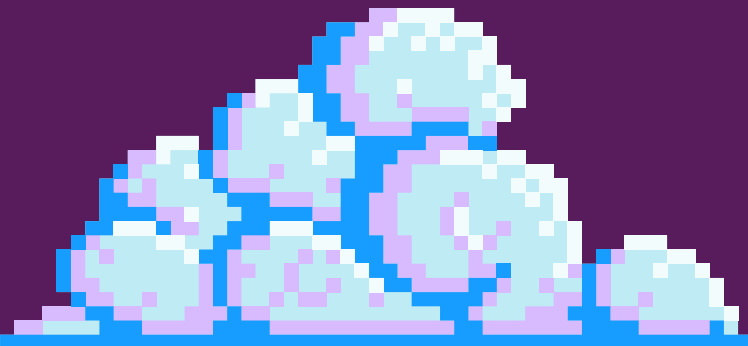


Was ist ein Pen-Test?

Vorbereitung & Durchführung

Was kein Pen-Test sieht

Checkliste



MANJA NEUMANN

WordPress & WooCommerce Freelancer
Meetup-Organisator Düsseldorf
Keine Sicherheits-Expertin!

 lechatinformatique
 manjaneumann



WAS IST EIN PEN-TEST?

- Echte Menschen versuchen ins System einzudringen
- Im Auftrag, mit freundlicher Absicht
- Kein automatischer Scan

Ziel:

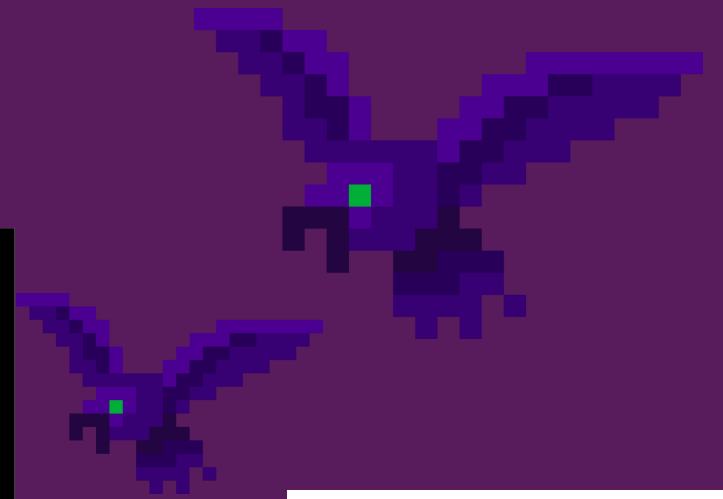
Schwachstellen finden, bevor es jemand anderes tut



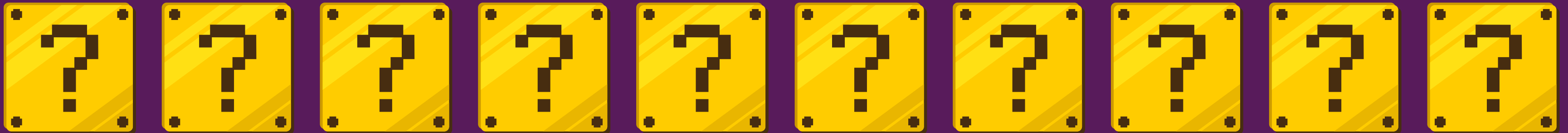
WAS IST OWASP?

- Open Worldwide Application Security Project
- Non-Profit-Organisation, die sich mit Web-Sicherheit beschäftigt
- Veröffentlicht die OWASP Top 10: die häufigsten Sicherheitslücken im Web

Ein OWASP-konformer Pentest prüft genau diese Schwachstellen



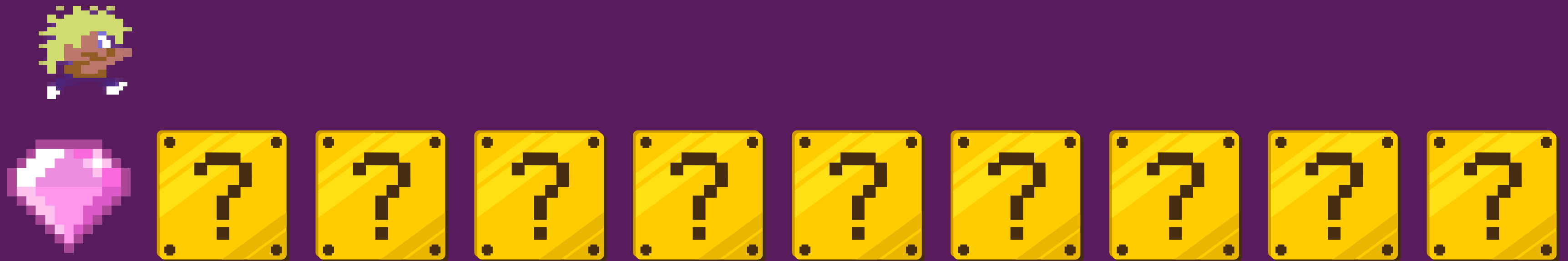
DIE OWASP TOP 10



A10: Mishandling of Exceptional Conditions

Fehler verraten zuviele Informationen

DIE OWASP TOP 10



A09: Security Logging and Alerting Failures

Fehlende oder unzureichende Überwachung von Angriffen oder Fehlversuchen

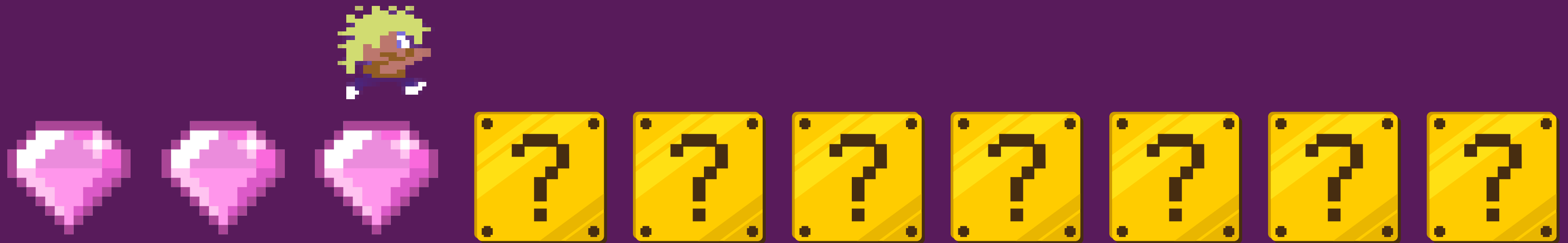
DIE OWASP TOP 10



A08: Software or Data Integrity Failures

Kann jemand unbemerkt Dateien auf dem Server ändern?

DIE OWASP TOP 10



A07: Authentication failures

Schwache Passwörter, kein 2FA, ungeschützter Login

DIE OWASP TOP 10



A06: Insecure design

Sicherheitsaspekte wurden in der Architektur oder Logik nicht eingeplant

DIE OWASP TOP 10



A05: Injection

Fremde Eingaben über Formulare oder Suchfelder werden nicht korrekt gefiltert und führen zu gefährlichem Code.

DIE OWASP TOP 10



A04: Cryptographic Failures

Unsichere oder fehlende Verschlüsselung

DIE OWASP TOP 10



A03: Software Supply Chain Failures

Plugins oder Themes mit Sicherheitslücken

DIE OWASP TOP 10



A02: Security Misconfiguration

Schlechte oder fehlende Standardeinstellungen

DIE OWASP TOP 10



A01: Broken Access Control

Jemand greift auf Dinge zu, auf die er keinen Zugriff haben sollte.

DIE WP TOP 5



A03: Software Supply Chain Failures

A01: Broken Access Control

A07: Authentication failures

A05: Injection

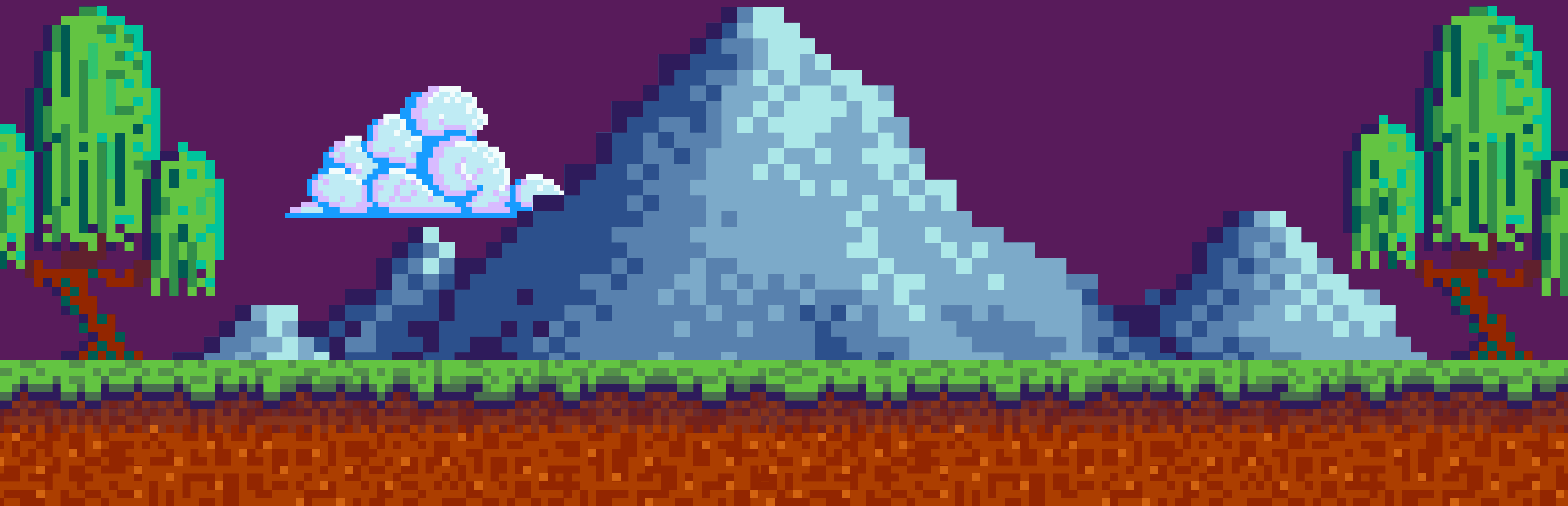
A02: Security Misconfiguration

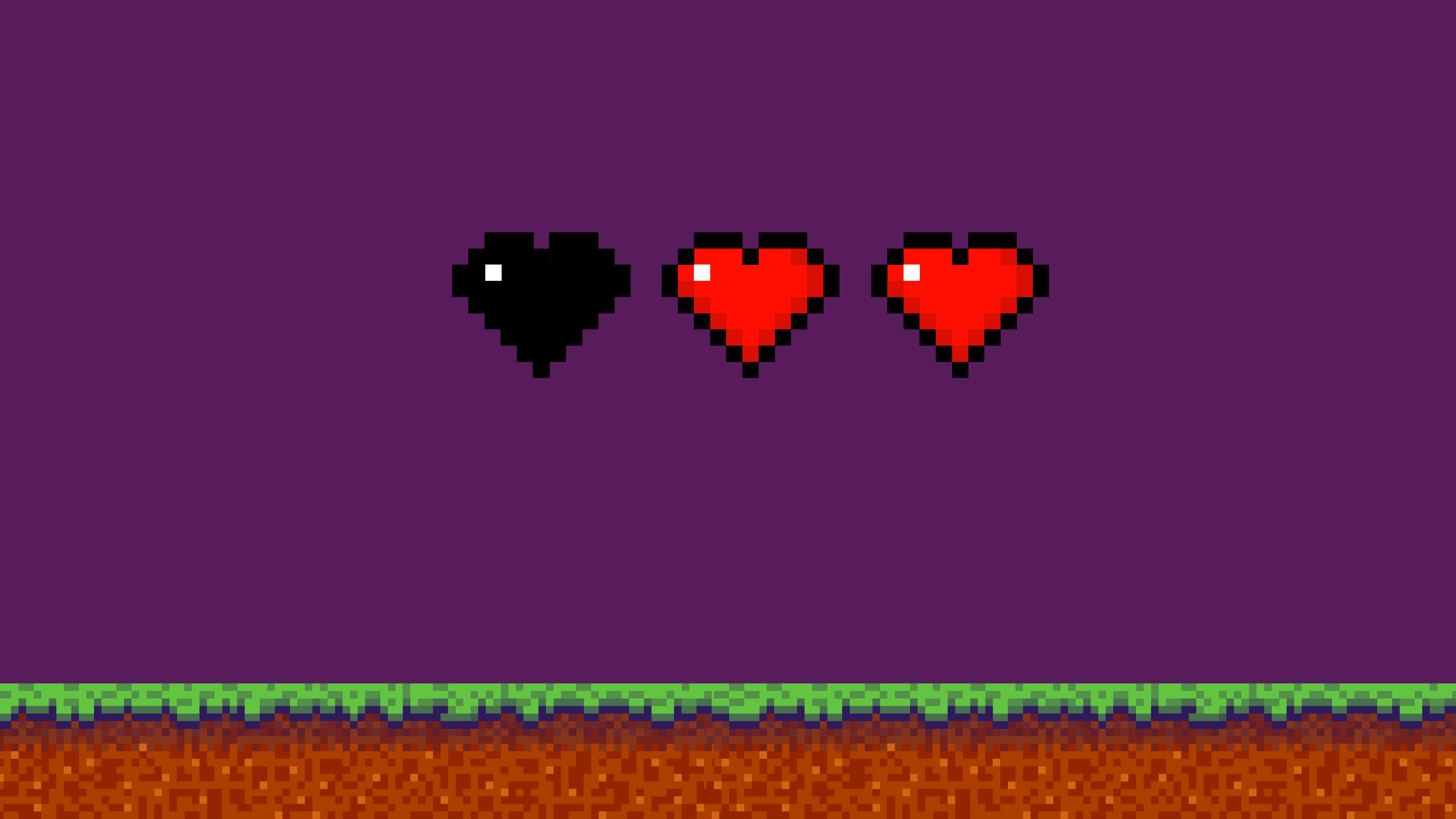
DAS SCHWEIZER KÄSE MODELL

Jede einzelne Scheibe hat Löcher, aber viele Scheiben übereinander lassen die Löcher immer weniger werden.



ARE YOU READY?



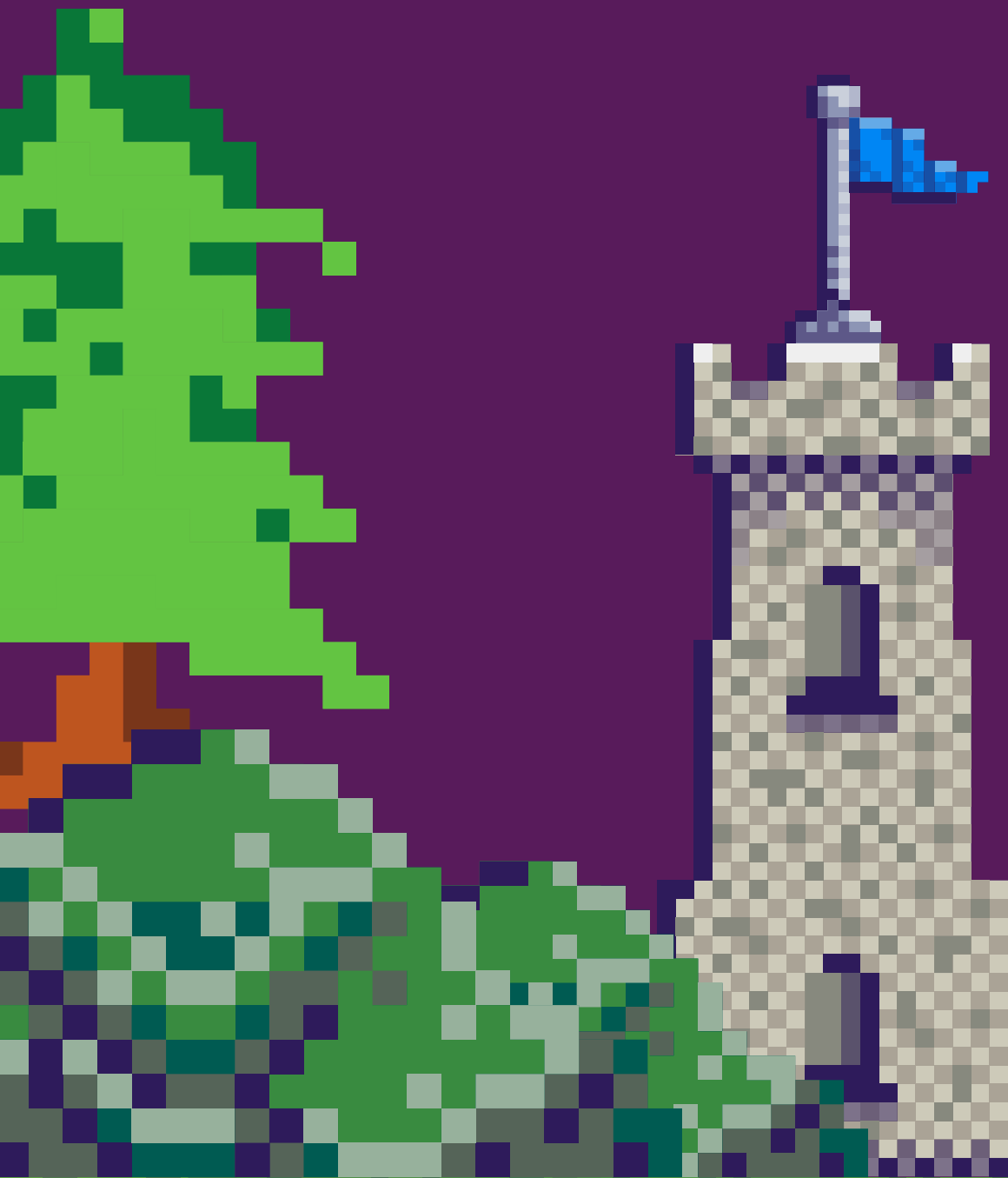


MIT PLUGIN-AUTOREN SPRECHEN

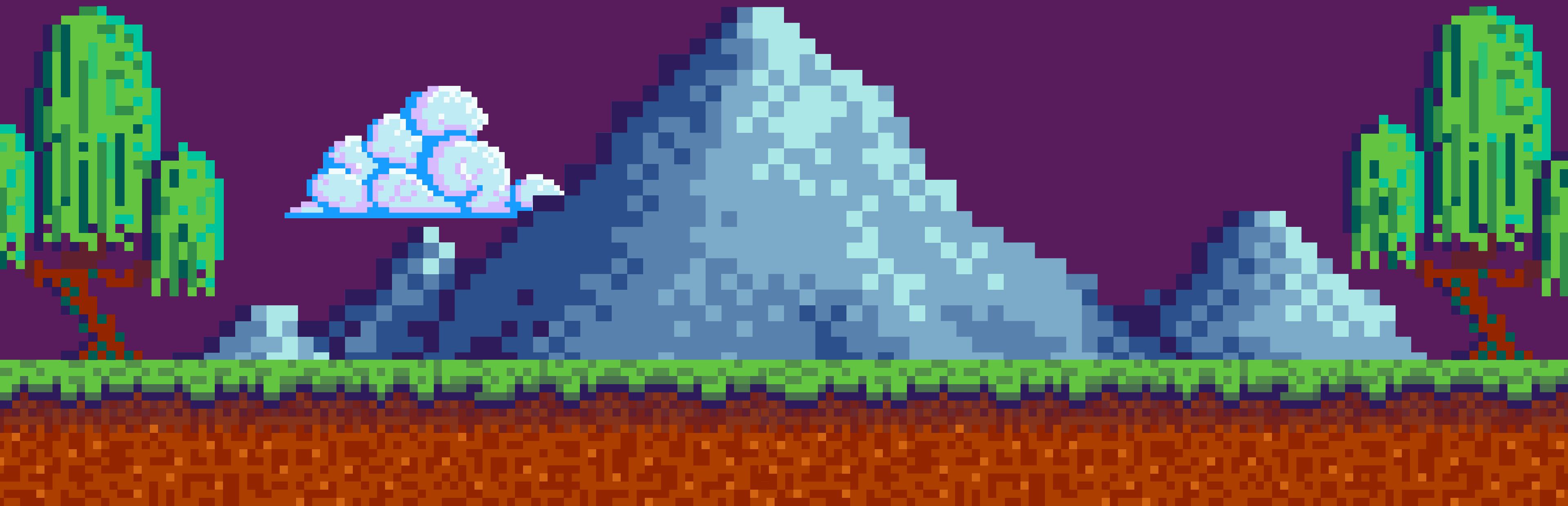
Ist uns doch egal.

Hier ist ein Fix,
wir tauschen
gerade aus.

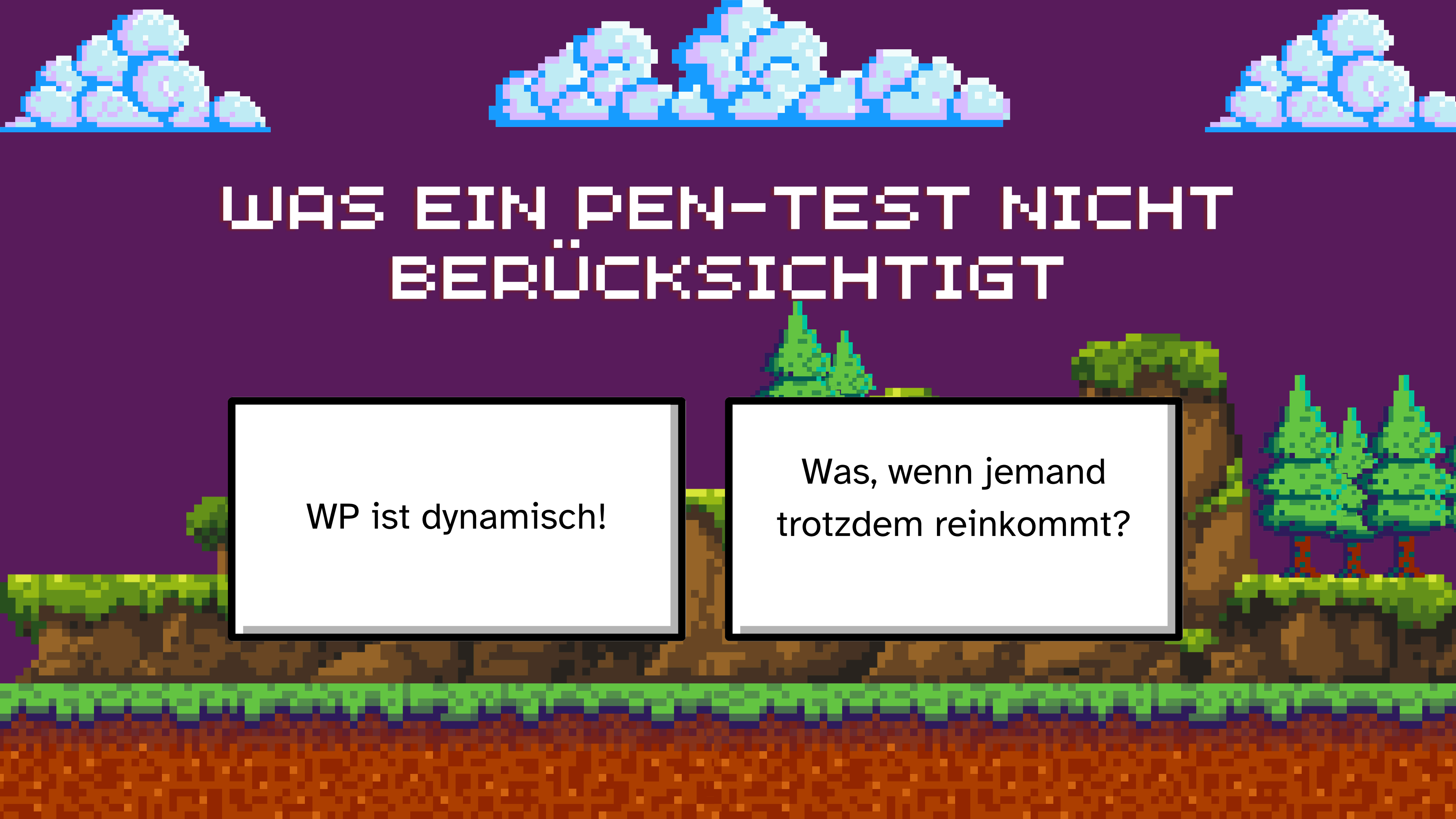
Stimmt nicht!



ARE YOU READY?







WAS EIN PEN-TEST NICHT BERÜCKSICHTIGT

WP ist dynamisch!

Was, wenn jemand
trotzdem reinkommt?

SELBSTTEST MIT ZAP & WPSCAN

ZAP

- Allgemeiner Scanner
- Open Source
- Hoher Einarbeitungsaufwand
- hat MCP-Server

→ zaproxy.org

WPScan

- WordPress-spezifischer Scanner
- Prüft Core, Plugins und Themes gegen eine eigene Datenbank
- Kostenloser API-Key für begrenzte Scans

→ wpscan.com

MEINE CHECKLISTE





THANKS FOR
PLAYING

END

