Übung – OWASP Top 10

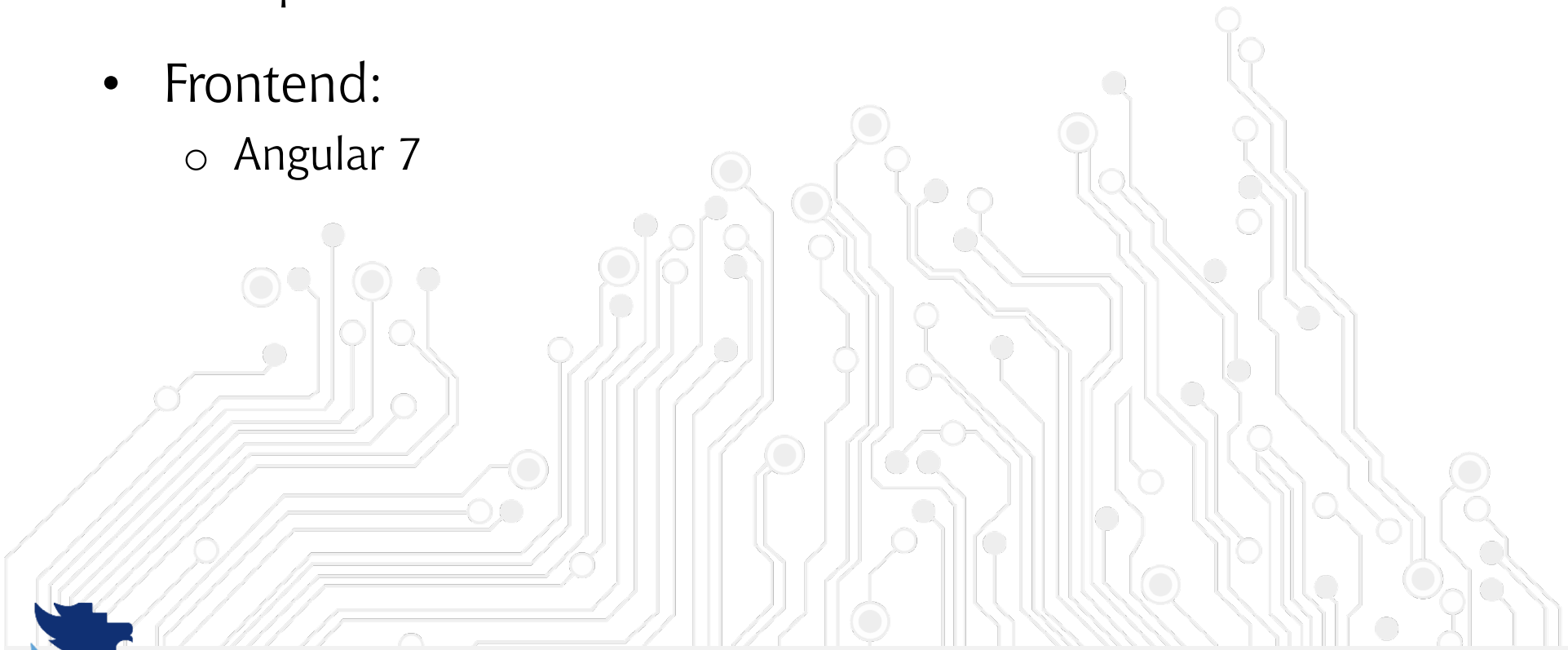
- Erstellen Sie eine Demo-Applikation zur Demonstration
  - Einheitliches Szenario und Technologiestack ist vorgegeben
  - Veröffentlichung der Applikation auf Github unter einer Open-Source-Lizenz (GPL, MIT, etc.)
- Bauen Sie eine der OWASP Top 10 Schwachstellen ein
  - Jede Gruppe wählt eine andere Schwachstelle aus
- Erklären Sie das Security-Problem und die Behebung der Schwachstelle anhand ihrer Demo-Applikation
  - ca. 10 Minuten Präsentation inkl. Live-Demo
- Durchführung in Gruppen zu 2 Personen
- **Deadline / Präsentation: 12.6.2019**

Szenario: Smart-Home Visualisierung (Mockup)

- Login mit Username und Passwort
- Ein Visualisierungs-Screen, mit dem Funktionen eines "Smart Home" gesteuert werden können
  - für alle Benutzer
  - (mind.) 3 Sensoren (Wert-Anzeige, z.B. Ist-Temperatur, Status, etc)
  - (mind.) 3 Aktoren (Wert-Änderung, z.B. Schalter, Soll-Temperatur, etc.)
- Ein Konfigurations-Screen
  - Unterschiedlich für "normale" Benutzer und "Administratoren"
  - z.B. Label für Sensoren/Aktoren, Schnittstellen-Config-Mockup, etc. für Admins
  - z.B. Name/Userprofil, etc. für "normale" Benutzer
- ein History / Log - Screen
  - Protokoll / Auflistung relevanter Aktivitäten (z.B. Konfigurationsänderungen, Einstellungen, etc.)
- Annahme: Visualisierung nutzt ein Backend für die eigentliche Steuerung (z.B. per CLI/Rest-API/etc.)

Technologie-Stack

- Backend:
  - NodeJS 9
  - MySQL
  - Express 4.16
- Frontend:
  - Angular 7



Übung – OWASP Top 10

- Bewertet wird:
  - „Korrekte“ Implementierung der Schwachstelle
  - Korrekte Behebung
  - Klarheit / Verständlichkeit der Präsentation/Darstellung
  - Bonuspunkte für einfaches Setup / gute Nachvollziehbarkeit der Probleme im Code

OWASP Top 10 – Gruppeneinteilung

A1 - Injection	XXXXX
	XXXXX
A2 - Broken Authentication	Christine Hegedüs
	Roman Jahn
A3 - Sensitive Data Exposure	Stephan Pillhofer
	Istvan Nagy
A4 - XML EE	
A5 - Broken Access Control	Manuel Trobolowitsch
	Daniel Zauner
A6 - Security Misconfig	
A7 - XSS	Paul Ablöscher
	Christian Kohout
A8 - Insecure Deserialzation	
A9 - Components w. known Vuln	
A10 - Insuff. Logging	Fischer Alexander
	Peter Helf