

# Insufficient Logging

Alexander Fischer, Kevin Janisch, Peter Helf

# Was ist Insufficient Logging

- ▶ Nicht alle Zugriffe werden gelogged
- ▶ Logs sind nicht genau genug oder falsch
- ▶ Einige Teile der Applikation werden gar nicht überwacht

# Behebung von Insufficient Logging

- ▶ Sicher stellen das alles gelogged wird
- ▶ Alle wichtigen Details loggen
- ▶ Logs sollten leicht zu verstehen sein

# Beispielszenario

- ▶ Ein Angreifer testet alle User auf ein konkretes Passwort. Dies würde bei ungenügendem Logging nur als ein fehlerhafter Loginversuch pro User aussehen.
- ▶ Würde man hier die IP, von der der Request kommt loggen, könnte man schnell feststellen, dass man angegriffen wurde.

DEMO