THE 2025 OWASP TOP TEN

WEB APPLICATION SECURITY UP-TO-DATE

Christian Wenz
info@christianwenz.de
@chwenz

confoo 2026, Montréal

OWASP Top Ten 2025

1. BROKEN ACCESS CONTROL =
2. SECURITY MISCONFIGURATION ⬆
3. SOFTWARE SUPPLY CHAIN FAILURES ⬆
4. CRYPTOGRAPHIC FAILURES ⬇
5. INJECTION ⬇
6. INSECURE DESIGN ⬇
7. AUTHENTICATION FAILURES =
8. SOFTWARE OR DATA INTEGRITY FAILURES =
9. LOGGING AND ALERTING FAILURES =
10. MISHANDLING OF EXCEPTIONAL CONDITIONS ★

#1: Broken Access Control

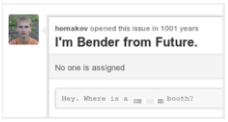
2013 list: Insecure Direct Object References & Missing Function Level Access Control

Access Control for data

Access Control for functions

Mass Assignment

The curse of model binding



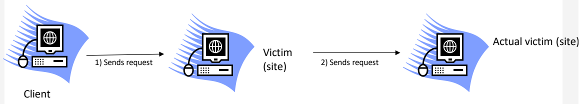
homakov opened this issue in 1001 years

I'm Bender from Future.

No one is assigned

Hey. Where is a [redacted] booth?

Server-Side Request Forgery (SSRF)



#2: Security Misconfiguration

I am not an administrator!

In the age of devops, maybe I am

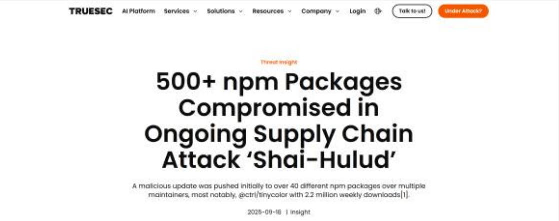
Harden server/operating system

Do not send detailled error messages to the client

Use browser security headers and cookie flags

XXE

#3: Software Supply Chain Failures



Threat insight

500+ npm Packages Compromised in Ongoing Supply Chain Attack 'Shai-Hulud'

A malicious update was pushed initially to over 40 different npm packages over multiple maintainers, most notably, @ctrl/tinycolor with 2.2 million weekly downloads[1].

2025-09-16 | Insight

https://www.truesec.com/hub/blog/500-npm-packages-compromised-in-ongoing-supply-chain-attack-shai-hulud

#4: Cryptographic Failures

Use encryption everywhere

HTTPS only (enforce, if viable)

- HTTP Strict Transport Security
- „secure" flag for cookies

#5: Injection

Different types of injection

- SQL injection
- LDAP injection
- XPath injection
- CSV injection

We are talking about SQL injection, of course. And cross-site scripting.

SQL Injection

SQL contains commands and data

Separating them can prevent the attack

Approach #1: parameterized queries/prepared statements -> separation
Approach #2: OR mapper -> no queries

XSS Protection

Escape output (< > " ' &)

Browser protection (X-XSS-Protection) 💀

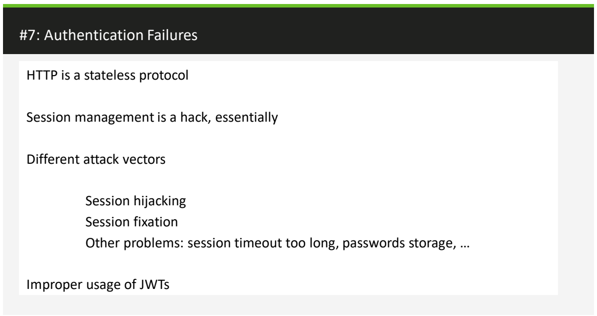
Content Security Policy

#6: Insecure Design

Threat Modeling

Reference architectures

„shift left"



#7: Authentication Failures

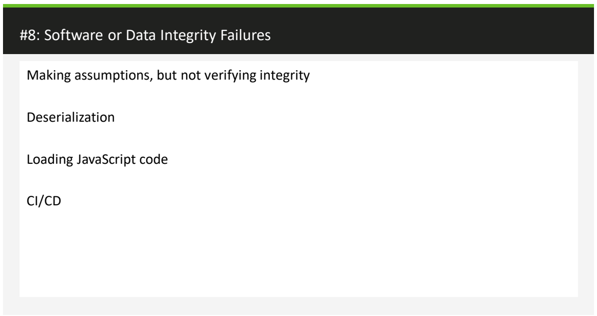
HTTP is a stateless protocol

Session management is a hack, essentially

Different attack vectors

- Session hijacking
- Session fixation
- Other problems: session timeout too long, passwords storage, …

Improper usage of JWTs



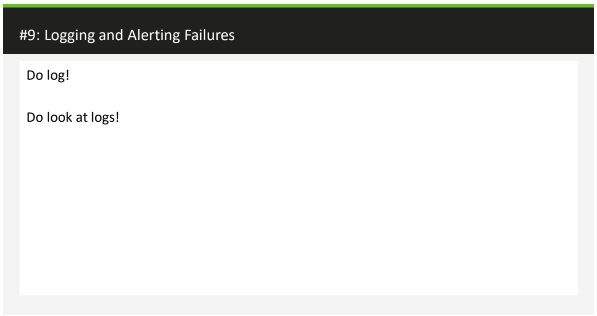
#8: Software or Data Integrity Failures

Making assumptions, but not verifying integrity

Deserialization

Loading JavaScript code

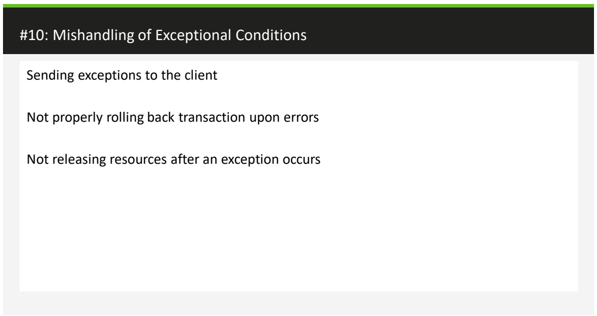
CI/CD



#9: Logging and Alerting Failures

Do log!

Do look at logs!

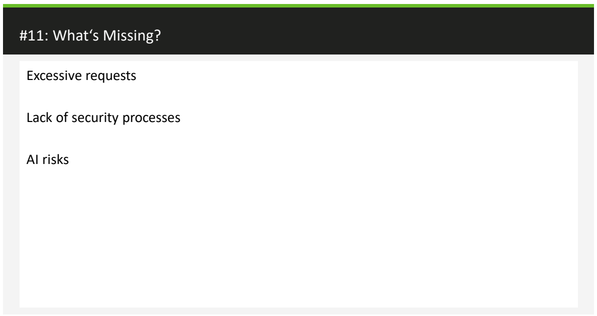


#10: Mishandling of Exceptional Conditions

Sending exceptions to the client

Not properly rolling back transaction upon errors

Not releasing resources after an exception occurs

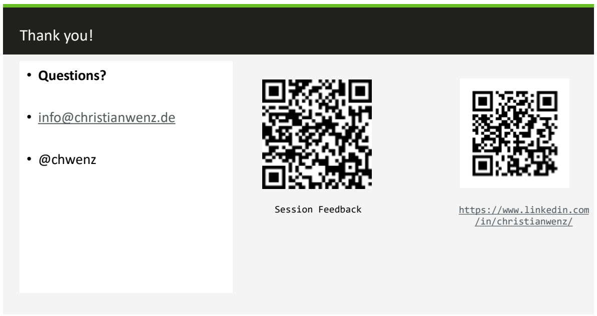


#11: What's Missing?

Excessive requests

Lack of security processes

AI risks



Thank you!

- **Questions?**
- info@christianwenz.de
- @chwenz

Session Feedback

https://www.linkedin.com/in/christianwenz/