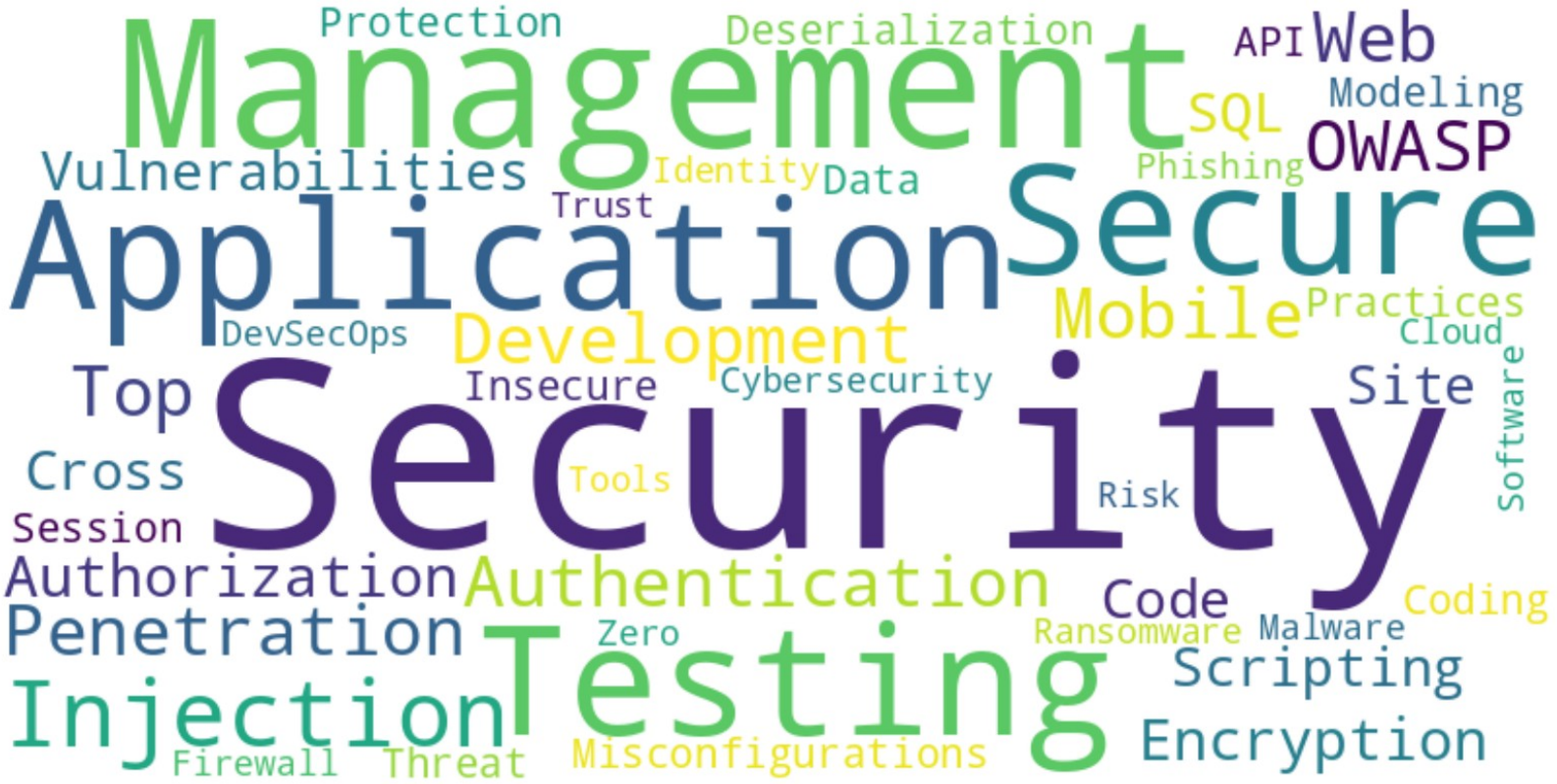
Application Security 101

Norbert Langner

2024-10-10

What GPT says?



Agenda

#1	10/10/24	Introduction to (Web) Application Security
#2	24/10/24	OWASP Top 10 Overview part 1
#3	07/11/24	OWASP Top 10 Overview part 2
#4	21/11/24	Secure Coding Practices
#5	05/12/24	Authentication and Authorization Mechanisms
#6	19/12/24	Web Application Security Testing
#7	16/01/25	Mobile Application Security
#8	30/01/25	Incident Response and Secure DevOps (DevSecOps)

Key information

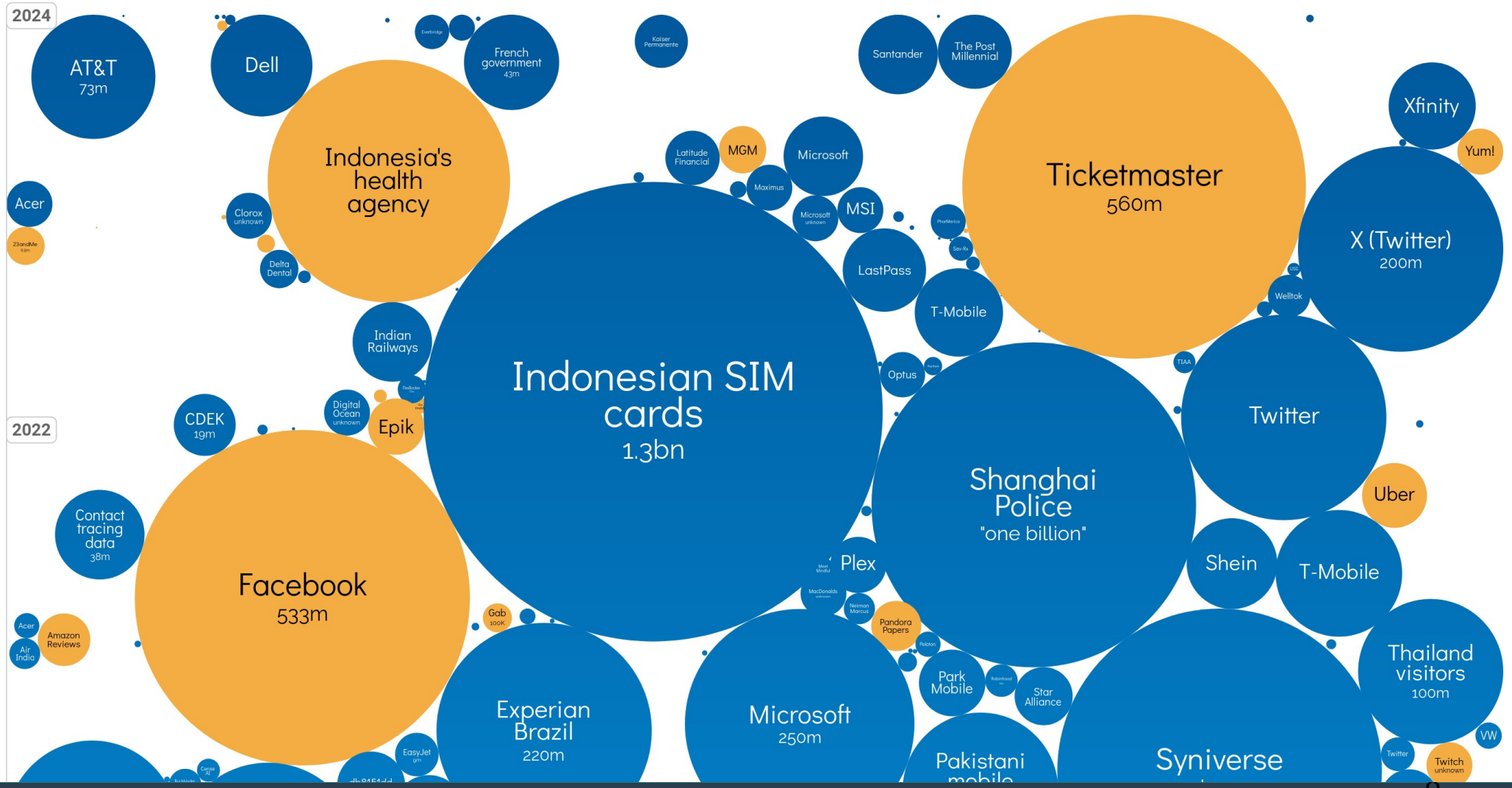
- **Exam in February**
  - Quiz [40%]
  - Concept task – description of potential security risks for presented scenario [60%]
  - Pass threshold: >50%
- **Literature**
  - OWASP Top 10 website
  - Web Application Security: Exploitation and Countermeasures for Modern Web Applications; Hoffman Andrew; O'Reilly 2020

Q&A


Zur Beachtung!

What is Application Security?

- https://livethreatmap.radware.com/
- GDPR
- Data privacy


2024
AT&T
73m
Dell
Everbridge
French government
43m
Kaiser Permanente
Santander
The Post Millennial
Xfinity
Yum!
Indonesia's health agency
Latitude Financial
MGM
Maximus
Microsoft
Microsoft unknown
MSI
Ticketmaster
560m
X (Twitter)
200m
Acer
23andMe
6.9m
Clorox
unknown
Delta Dental
LastPass
PharMerica
Sav-Rx
T-Mobile
Welltok
Indian Railways
Indonesian SIM cards
1.3bn
Optus
TIAA
Twitter
2022
CDEK
19m
Digital Ocean
unknown
Epik
Shanghai Police
"one billion"
Uber
Contact tracing data
38m
Facebook
533m
Plex
Shein
T-Mobile
Acer
Air India
Amazon Reviews
Gab
100K
MacDonalds
Neiman Marcus
Pandora Papers
Peloton
Park Mobile
Robinhood
Star Alliance
Thailand visitors
100m
Experian Brazil
220m
Microsoft
250m
Pakistani
Syniverse
EasyJet
VW
Twitter
Twitch
unknown

Considered topics

- **Web applications (frontend, backend)**
- **Mobile apps**
- **API (internal and external)**
- **Infrastructure**
  - Cloud
  - On-premise
  - IaaS vs PaaS

Basic Security Principles

CYBERSECURITY – INFOSEC CIA TRIAD

Safeguarding the accuracy and completeness of information and processing methods.

Includes the detection of alterations that occurred in storage, transit, process,...

Ensuring that information is accessible only to those authorized to have access.

Includes:

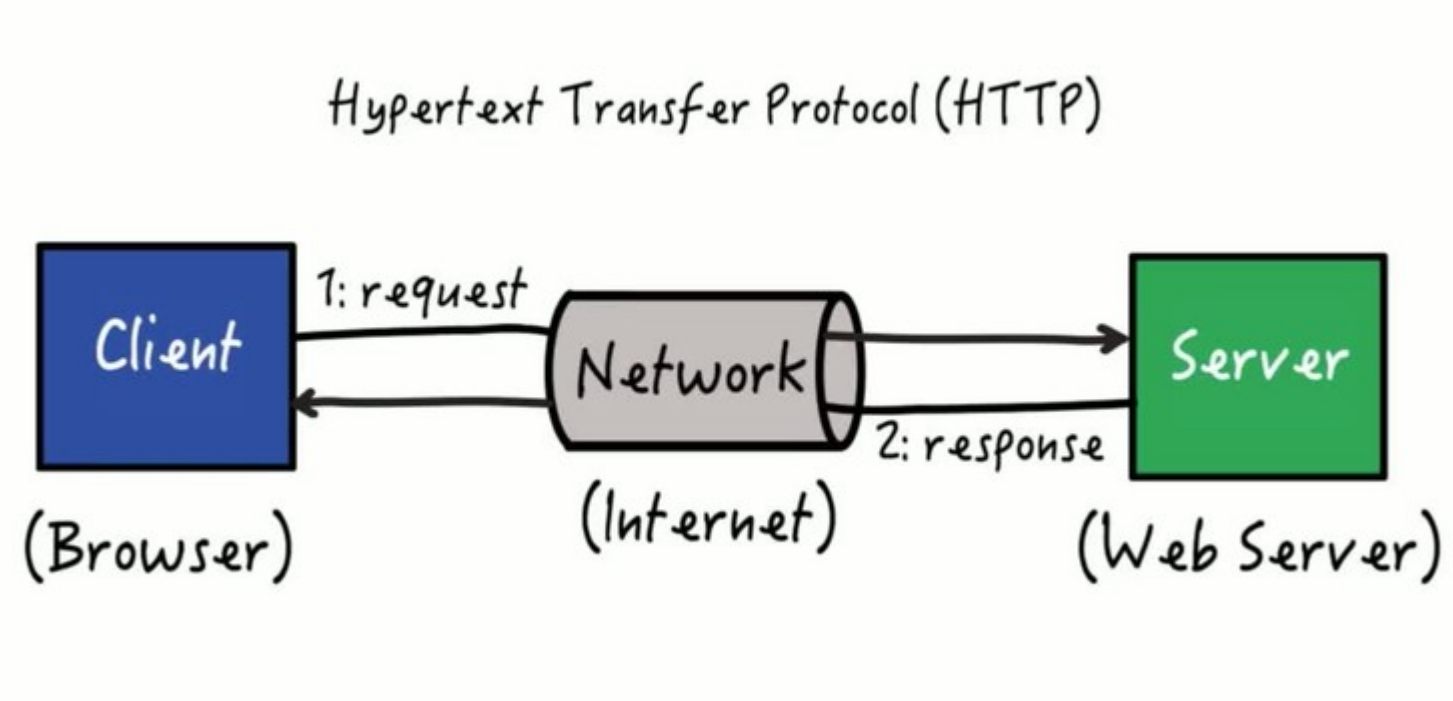
- Protection from unauthorized access and use;
- Protecting data on systems, in transit, in process,...

Ensuring that authorized users have access to information and associated assets when required.

Includes controls for:

Acceptable level of performance
Fault tolerance
Prevention of data loss and destruction
Reliable backups, redundancy,...

Introduction to HTTP/HTTPS

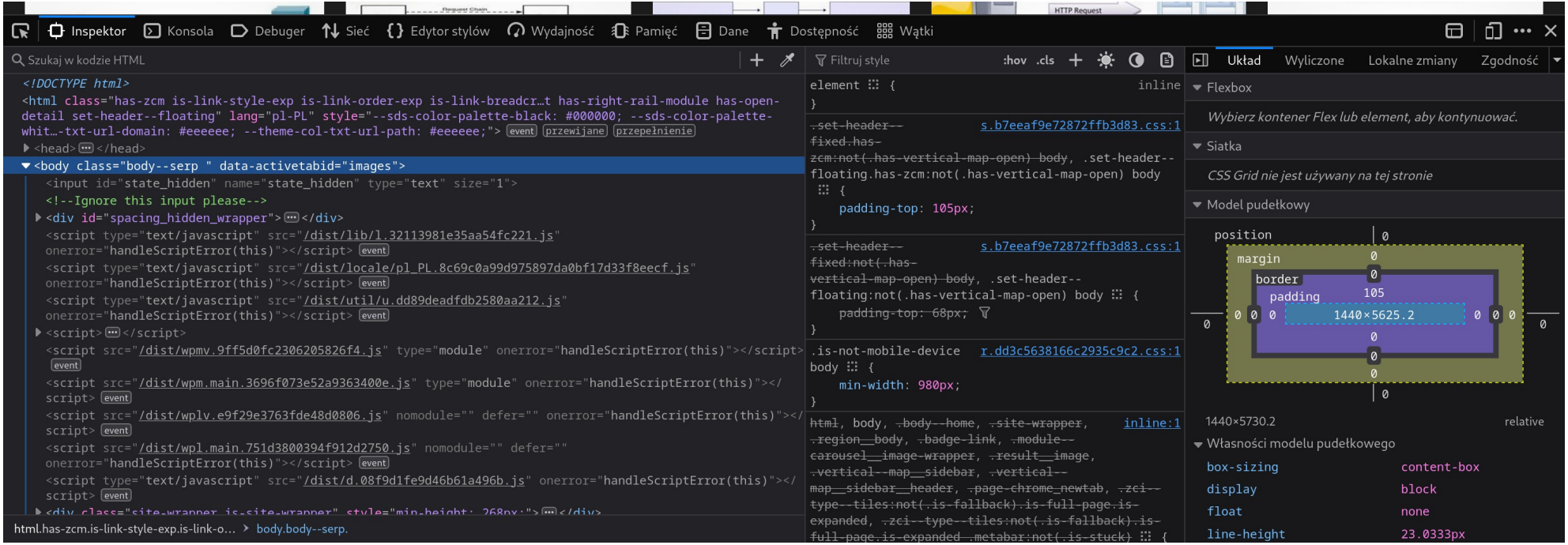


But... you know that already!

Cookies, Sessions, and Tokens

- How to identify user between requests?
- Cookies: httponly attribute – why it's important for apps?
- Sessions and JWT – what challenges do we

Overview of Web Development Tools



Common Web Application Security Issues

- Misconfigured Servers or SSL/TLS
- Insecure Session Management
- Weak Input Validation
- Unencrypted Sensitive Data
- Improper Access Control

Secure Application Design

- **Secure Design Patterns:**
  - Input Validation and Sanitization
  - Role-Based Access Control
  - Encryption Best Practices (Data at Rest and in Transit)

Tools for Application Security

- **Static Code Analysis Tools (SonarQube, ESLint for JavaScript Security)**
- **Dynamic Testing Tools (OWASP ZAP, Burp Suite)**
- **Security Plugins for IDEs**
  - GitHub Dependabot for Vulnerability Alerts
  - ESLint Security Plugin for JavaScript

Let’s try to hack something