OWASP Top 10 2021

OWASP Switzerland Meeting

8.2.2022, Zürich, Peter Šufliarsky, peter.sufliarsky@compass-security.com

Structure of this Talk

1. OWASP Top 10 Introduction
2. Methodology
3. What’s new in OWASP Top 10 2021
4. OWASP Top 10 2021 Risks
5. Demos
6. Questions

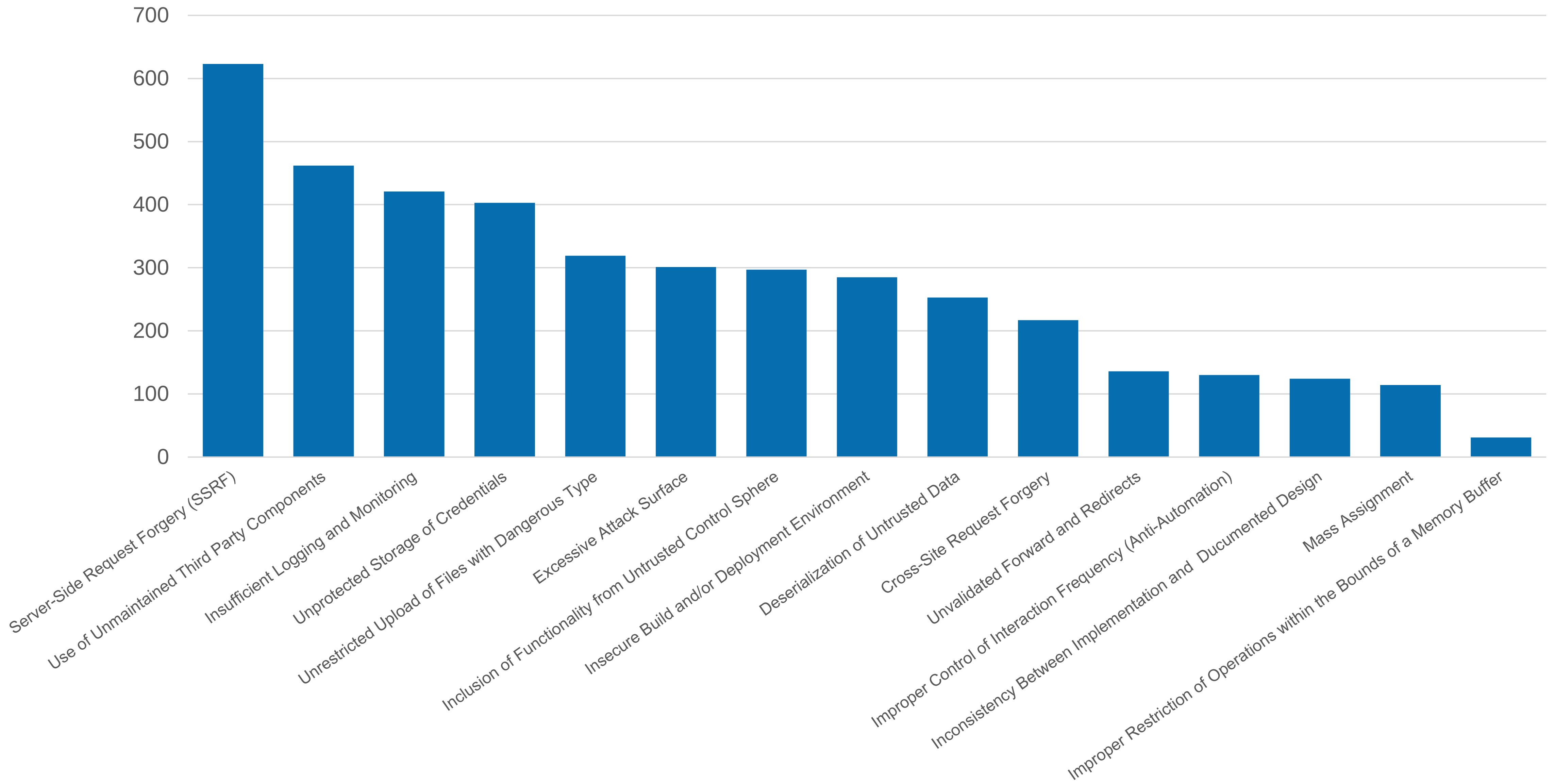
OWASP Top 10

- First Top 10 released in 2007
- Top 10 risks for web applications
- 7th update released on 24th September 2021

Methodology

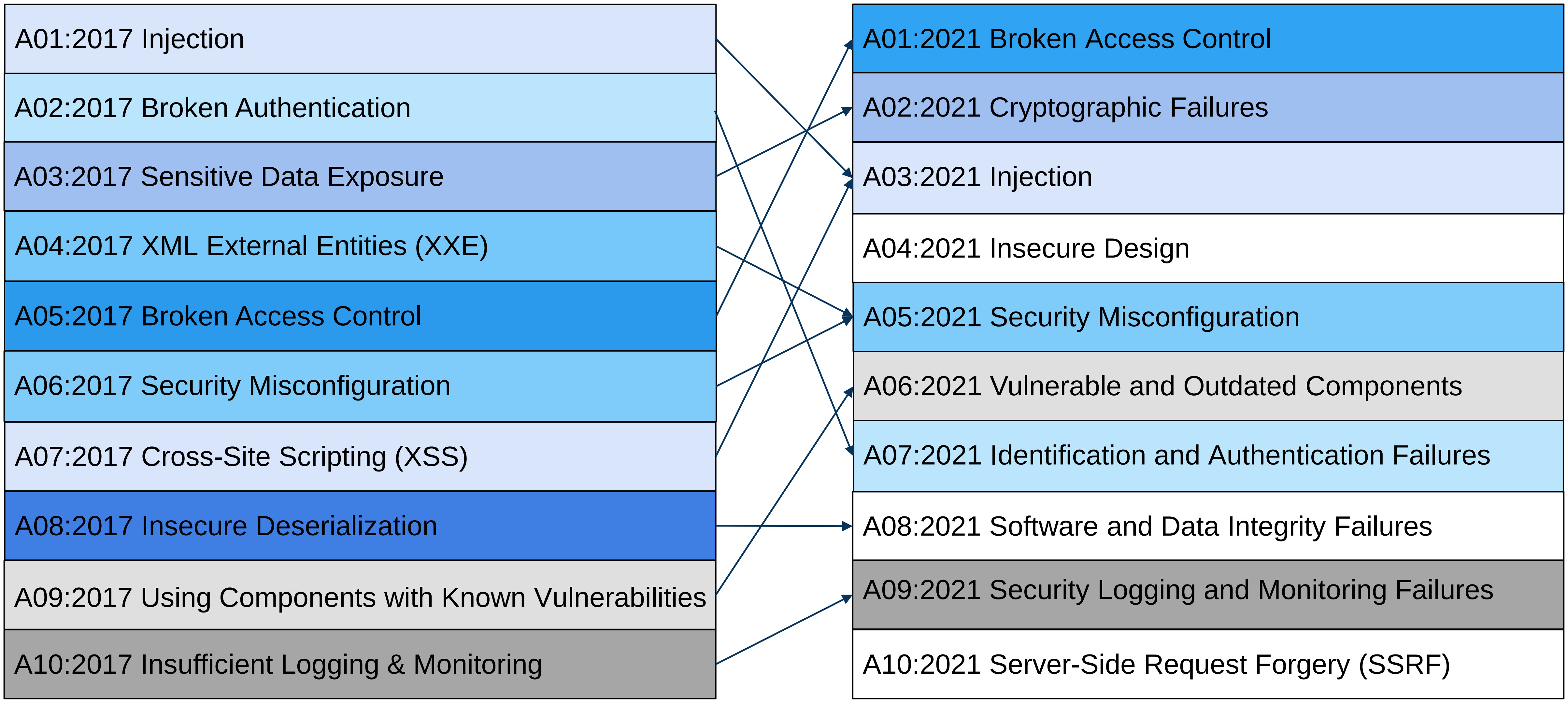
- Data set from 515k applications
- Community survey
- Focus on incidence rate rather than frequency

Community Survey



OWASP Top 10 2017

OWASP Top 10 2021



A01:2017 Injection

A02:2017 Broken Authentication

A03:2017 Sensitive Data Exposure

A04:2017 XML External Entities (XXE)

A05:2017 Broken Access Control

A06:2017 Security Misconfiguration

A07:2017 Cross-Site Scripting (XSS)

A08:2017 Insecure Deserialization

A09:2017 Using Components with Known Vulnerabilities

A10:2017 Insufficient Logging & Monitoring

A01:2021 Broken Access Control

A02:2021 Cryptographic Failures

A03:2021 Injection

A04:2021 Insecure Design

A05:2021 Security Misconfiguration

A06:2021 Vulnerable and Outdated Components

A07:2021 Identification and Authentication Failures

A08:2021 Software and Data Integrity Failures

A09:2021 Security Logging and Monitoring Failures

A10:2021 Server-Side Request Forgery (SSRF)

A01:2021 Broken Access Control

- Found 318 487 times in 3.81% of applications
- Violation of the principle of least privilege
- Bypassing access control checks by modifying the URL, IDOR
- Accessing APIs with POST, PUT, DELETE
- Elevation of privilege
- Metadata manipulation, JWT token / SAML message replaying or tampering
- Force browsing of authenticated / admin pages

A02:2021 Cryptographic Failures

- Found 233 788 times in 4.49% of applications
- Unencrypted protocols like HTTP, FTP, SMTP
- Weak cryptographic algorithms, weak hashing algorithms
- Default keys
- Strict-Transport-Security header (HSTS)
- Server certificate validation
- Proper use of random number generators

A03:2021 Injection

- Found 274 228 times in 3.37% of applications
- User-supplied data not validated, filtered or sanitized by the application
- Input directly concatenated or used
- XSS, SQL injection, OS command injection …

A04:2021 Insecure Design

- Found 262 407 times in 3.00% of applications
- Design flaws != Implementation defects
- Unclear business requirements concerning CIA
- Password recovery using questions and answers
- Missing protection against bots
- Unrestricted file upload
- Incorrect privilege assignment
- Insufficiently protected credentials

A05:2021 Security Misconfiguration

- Found 208 387 times in 4.51% of applications
- Missing security hardening
- Improperly configured cloud services
- Default accounts
- Error handling reveals too much information
- Not using secure defaults for application servers or development frameworks
- Missing security headers, Content-Security-Policy
- Outdated systems, disabled security features in up-to-date systems

A06:2021 Vulnerable and Outdated Components

- Found 30 457 times in 8.77% of applications
- Not knowing the versions of used components, including nested dependencies
- Unsupported or out of date software
- Creating technical debt by keeping old versions of components
- Patching based on a schedule, not considering the risks
- Not testing the compatibility of updated components

A07:2021 Identification and Authentication Failures

- Found 132 195 times in 2.55% of applications
- Possibility to brute-force credentials
- Default, weak or well known passwords
- Weak password recovery processes
- Missing or flawed MFA
- Exposed session tokens
- Session managed on the client-side only

A08:2021 Software and Data Integrity Failures

- Found 47 972 times in 2.05% of applications
- Insecure CI/CD pipelines
- Auto-update without integrity verification
- Insecure deserialization
- Not using SRI directives

A09:2021 Security Logging and Monitoring Failures

- Found 53 615 times in 6.51% of applications
- Not logging login failures or other interesting transactions
- Unclear log messages
- Logs only stored locally
- Alerting threshold not defined
- Penetration tests and scans do not trigger alerts
- Applications can not alert in real time

A10:2021 Server Side Request Forgery (SSRF)

- Found 9 503 times in 2.72% of applications
- Low incidence rate, above-average exploit and impact potential ratings
- Server fetching remote resources without validating the user-supplied URL

A11:2021 Next Steps

- Code Quality Issues
- Denial of Service
- Memory Management Errors

More About OWASP Top 10 2021

- Top 10:2021 – https://owasp.org/Top10
- Top 10 Supplemental Site – https://owasptopten.org

- Top 10 GitHub – https://github.com/OWASP/Top10
- OWASP Juice Shop GitHub - https://github.com/juice-shop/juice-shop

More about OWASP Top 10 2021

- OWASP Top 10 2021 - Andrew van der Stock

  https://www.youtube.com/watch?v=uLBCDBnMEt0

- The How and Why of the OWASP Top Ten 2021 - Brian Glas

  https://www.youtube.com/watch?v=nq-Igdk0o7s

Demos

Questions

COMPASS
SECURITY