German OWASP Day 2025

Top 10:2025-RC1
- Neuerungen und Hintergründe -

Torsten Gigler
(torsten.gigler@owasp.org)

Who Are We (project team)?

- **Goals:** Transparency, conceptual integrity and to include our community
- **Team:** Andrew van der Stock, Brian Glas, Neil Smithline,
  Tanya Janca (new in this version), Torsten Gigler
- **Where the team lives:**
  USA: 2, Australia: 1, Canada: 1, Germany: 1

- **Über mich (Torsten Gigler)**
  - interner IT-Sicherheits-Berater und -Architekt (> 25 Jahre)
  - **bei OWASP seit 2013 aktiv:**
    - **Co-Lead OWASP-Top10-Projekt** (seit 2017, Contributor seit 2013)
    - Mitorganisator **OWASP Stammtisch München** (seit 2015)
    - Contributor '**O-Saft** - OWASP SSL Advanced Forensic Tool'
    - Projekt-Lead "OWASP Open Security Information Base (**OSIB**)" (2023)

German
OWASP
Day 2025

01 What the Top Ten is (and isn’t)

What the Top Ten is (and isn’t):

- **Top 10 Risks to Web Apps**
- First released in 2003, **2025 is the 8th update**
- A **data-driven awareness document**
- An **appetizer** for **secure coding** and **code review**
- **Not a standard** or compliance checklist
- **Although there are 10 items, please do not stop there.** 🙏

Quick disclosure: The Top Ten items are finalized,
but the writing is still in draft. We want and need your feedback

German OWASP Day 2025

02 How the 2025 List was Built

High Level Process

- We **ask for data...** **It takes 14-16 months**
- **Normalize the data**
- Pull **National Vulnerability Database** for **CVE -> CWE**
- **Normalize Exploit** and **Impact** from **CVSS**
- Determine the **formula weighting**
- **Group CWEs** into **logical categories**
- **Build a data Top Ten**
- Run **Community Survey**
- Weigh the **survey** with the **data**
- Determine the **new Top Ten**
- **Write** a lot, discuss, write more, review, feedback, discuss, release

Data Factors

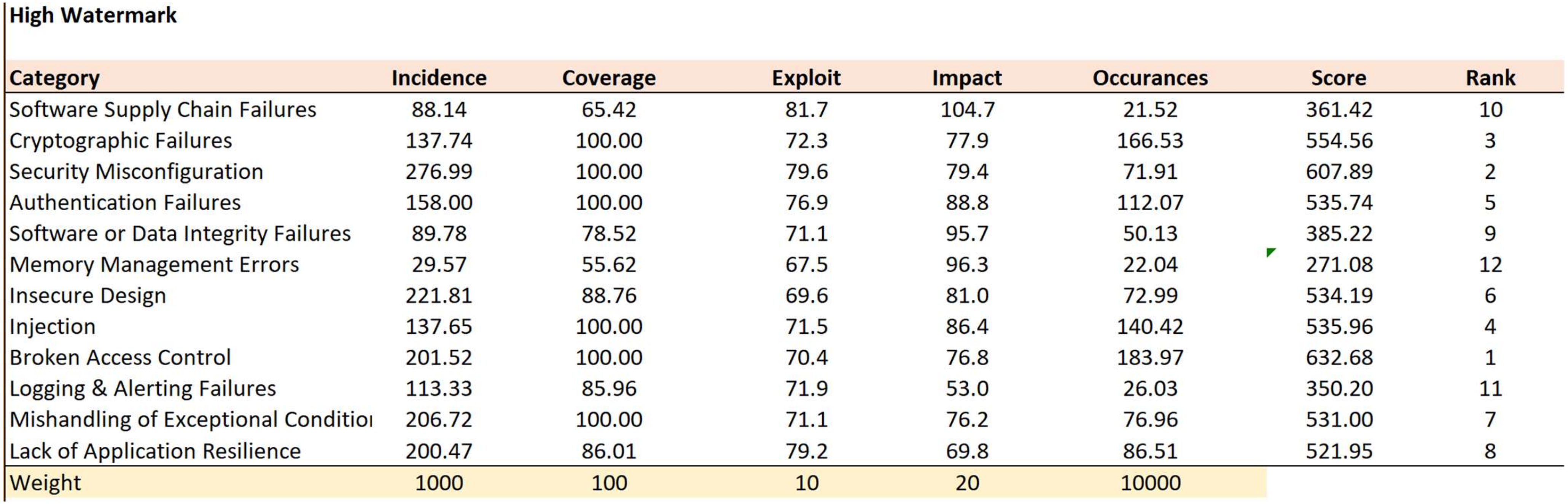
Data stats:

- **2017: >100.000 APPs, 30 CWEs**
- **2021: >500.000 APPs, 390 CWEs**
- **2025: >2.800.000 APPs, 686 CWEs**

→ Contributors:

- Accenture (Prague)
- Bugcrowd
- Contrast Security
- CryptoNet Labs
- Intuitor SoftTech Services
- Orca Security
- Probley
- Semgrep
- Sonar
- usd AG
- Veracode
- Wallarm
- … Anonymous (multiple)

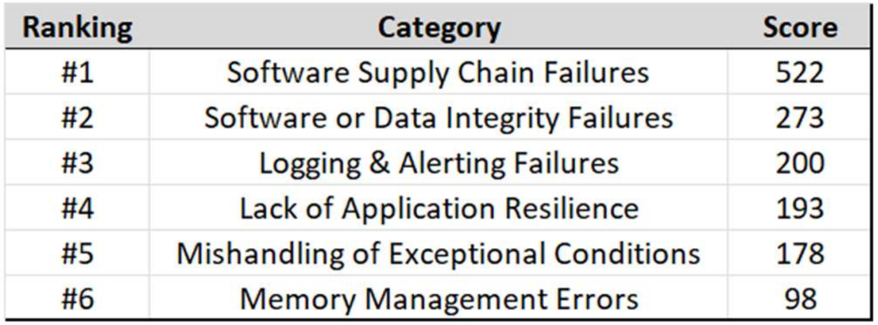
Data Factors



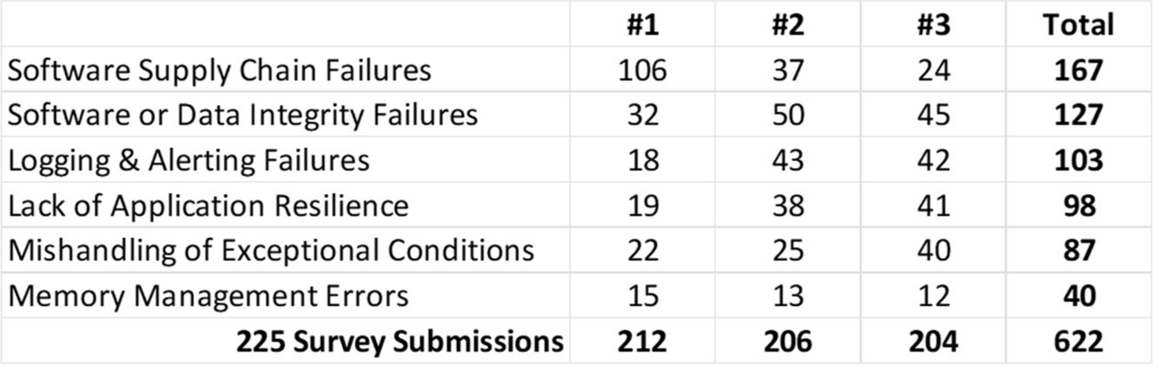
High Watermark

Category	Incidence	Coverage	Exploit	Impact	Occurances	Score	Rank
Software Supply Chain Failures	88.14	65.42	81.7	104.7	21.52	361.42	10
Cryptographic Failures	137.74	100.00	72.3	77.9	166.53	554.56	3
Security Misconfiguration	276.99	100.00	79.6	79.4	71.91	607.89	2
Authentication Failures	158.00	100.00	76.9	88.8	112.07	535.74	5
Software or Data Integrity Failures	89.78	78.52	71.1	95.7	50.13	385.22	9
Memory Management Errors	29.57	55.62	67.5	96.3	22.04	271.08	12
Insecure Design	221.81	88.76	69.6	81.0	72.99	534.19	6
Injection	137.65	100.00	71.5	86.4	140.42	535.96	4
Broken Access Control	201.52	100.00	70.4	76.8	183.97	632.68	1
Logging & Alerting Failures	113.33	85.96	71.9	53.0	26.03	350.20	11
Mishandling of Exceptional Conditioi	206.72	100.00	71.1	76.2	76.96	531.00	7
Lack of Application Resilience	200.47	86.01	79.2	69.8	86.51	521.95	8
Weight	1000	100	10	20	10000		

The Survey Results



Ranking	Category	Score
#1	Software Supply Chain Failures	522
#2	Software or Data Integrity Failures	273
#3	Logging & Alerting Failures	200
#4	Lack of Application Resilience	193
#5	Mishandling of Exceptional Conditions	178
#6	Memory Management Errors	98



	#1	#2	#3	Total
Software Supply Chain Failures	106	37	24	**167**
Software or Data Integrity Failures	32	50	45	**127**
Logging & Alerting Failures	18	43	42	**103**
Lack of Application Resilience	19	38	41	**98**
Mishandling of Exceptional Conditions	22	25	40	**87**
Memory Management Errors	15	13	12	**40**
225 Survey Submissions	**212**	**206**	**204**	**622**

German OWASP Day 2025

03 The New Top 10

The OWASP Top Ten 2025

A01:2021 → A01:2025 Broken Access Control

A05:2021 ↗ A02:2025 Security Misconfiguration

A06:2021 ↗ **A03:2025 Software Supply Chain Failures** ⬅ **Greatly Expanded!**

A02:2021 ↘ A04:2025 Cryptographic Failures

A03:2021 ↘ A05:2025 Injection

A04:2021 ↘ A06:2025 Insecure Design

A07:2021 → A07:2025 Authentication Failures

A08:2021 → A08:2025 Software or Data Integrity Failures

A09:2021 → **A09:2025 Logging & Alerting Failures** ⬅ **Expanded!**

A10:2025 Mishandling of Exceptional Conditions ⬅ **Brand New!**

A03:2025 Software Supply Chain Failures

- In **2017** this was "**Using Components with Known Vulnerabilities**"
- In **2021** this was "**Vulnerable and Outdated Components**"
- And now, for **2025**, this is "**Software Supply Chain Failures**"
  - "Supply chain vulnerability" has become a commonly used term
- It is **ranked #3 because**:
  - It was top-ranked in the **community survey** with 50% (106 out of 212) ranking it #1 with 100% ranking it in top 3
  - These attacks are **growing in frequency** (but only 11 CVEs, yet)
  - However, when **tested** and reported in the contributed data, this category has the **highest average incidence rate** at 5.19%.

A09:2025 (Security) Logging & Alerting Failures

- In **2017** this was "**Insufficient Logging & Monitoring**"
- In **2021** this was "**Security Logging and Monitoring Failures**"
- And now, for **2025**, this is “(**Security) Logging & Alerting Failures**“, stays at 9th (data was 11th, survey was 3rd)
- **Slight name change** to emphasize the alerting function needed to induce action on relevant logging events
- Not many CWEs (5), not much CVE/CVSS data, but detecting and responding to breaches is critical
- **Can be challenging to test**. Request reports from the Blue Team after a penetration or Red Team test

A10:2025 Mishandling of Exceptional Conditions

- This category is **brand new**. It was very close in the **data** to “Lack of Application Resilience”, but the **community feedback** brought it just over the threshold
- **Contains 24 CWEs, focuses** on **improper error handling**, **logical errors**, **failing open**
- **Programs fail to prevent**, **detect**, and **respond** to **unusual** and **unpredictable situations**, which leads to crashes, unexpected behavior, and sometimes vulnerabilities
- Any time an **application is unsure** of its **next instruction**, an exceptional condition has been mishandled.

German
OWASP
Day 2025

THANK YOU!

owasp.org/Top10