
OWASP 2025
GLOBAL
AppSec
USA
The OWASP
Top Ten 2025
Neil Smithline
Tanya Janca

Agenda

1. Housekeeping
2. What is OWASP & The Top Ten
3. How the 2025 List Was Built
4. Overview of the New Top Ten
5. The Familiar Eight
6. New! #3 Software Supply Chain Failures
7. New! #10 Mishandling of Exceptional Conditions
8. Honorable Mentions
9. How to Use the Top Ten in Your Organization
10. Community & Next Steps

TOP 10

Who's giving this talk?

Neil Smithline

- Security Architect, Engineer, and Executive
- Professional developer since 1991
- Past 25 years with cybersecurity focus
- Have started numerous cybersecurity programs
- Inventor holding 7 software patents
- Working on OWASP Top-10 since 2010, co-lead since 2017
- Hospice volunteer
- Loves walking in the woods in New England winters with his wife and dog

The mandatory ‘about me’ slide.

Tanya Janca

- Secure Coding Trainer at SheHacksPurple Consulting
- Author: Alice and Bob Learn Secure Coding
  & Alice and Bob Learn Application Security
- 28+ years in tech, Sec + Dev
- Founder: We Hack Purple, OWASP DevSlop, #CyberMentoringMonday, WoSEC
- Advisor: Smithy, Katilyst
- Contributor: OWASP Top Ten, StackOverflow
- Board Member: Forte Group

Welcome to The OWASP Top Ten 2025!

Quick disclosure:

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

Agenda

1. Housekeeping
2. What is OWASP & The Top Ten
3. How the 2025 List Was Built
4. Overview of the New Top Ten
5. The Familiar Eight
6. New! #3 Software Supply Chain Failures
7. New! #10 Mishandling of Exceptional Conditions
8. Honorable Mentions
9. How to Use the Top Ten in Your Organization
10. Community & Next Steps

TOP 10

Who are we (OWASP)?

- The Open Worldwide Application Security Project
- A non-profit, projects, chapters, and conferences, but most of all: **a community of like-minded individuals**
- OWASP's mission is to be the global open community that improves software security through education, tools, and collaboration.
- By providing free and open-source resources, best practices, and a community for sharing knowledge, OWASP aims to make software security visible so that individuals and organizations can make informed decisions about risks

What the Top Ten is (and isn't):

- Top 10 Risks to Web Apps – not Top 10 impacts, likelihoods, or vulnerabilities
- First released in 2003, 2025 is the 8th update
- Not a standard or compliance checklist.
- A data-driven awareness document to help organizations prioritize.
- Although there are 10 items, please do not stop there. 🙏

How best to use the Top Ten

- The Top Ten is a starting point, not an end goal
- For security awareness programs and training
- To help build an organization's first AppSec program
- For prioritization of vulnerabilities and remediation
- As a checklist for secure coding and code review
- For penetration and other testing
- ~~For compliance~~. Just kidding!

Agenda

1. Housekeeping
2. What is OWASP & The Top Ten
3. How the 2025 List Was Built
4. Overview of the New Top Ten
5. The Familiar Eight
6. New! #3 Software Supply Chain Failures
7. New! #10 Mishandling of Exceptional Conditions
8. Honorable Mentions
9. How to Use the Top Ten in Your Organization
10. Community & Next Steps

TOP 10

Community-Driven Process

- It's built from data from organizations, millions of records + hundreds of survey respondents
- Acknowledgement: **we want to thank every single person and company who answered the data call and survey, and those of you will review the writing and provide feedback in the future.**

Who Are We (project team)?

- Collaborative - all of us do all the things
- Goals: conceptual integrity and to include our community

	What they primarily do
Brian Glas	Co-lead, author, data scientist, data analysis, risk rankings, interface to data sources, and more
Torsten Gigler	Co-lead, author, data analysis, risk rankings, document template, website, English editor, German translation, and more
Neil Smithline	Co-lead, author, data analysis, risk rankings, website, valuable counsel and advice, and more
Andrew van der Stock	Co-lead, author, data analysis, risk rankings, persnickety grammar person, often gets interviews and media outlet requests, and more
Tanya Janca	Co-lead, newest member, author, project manager/nerd herder, also does interviews/media

More Deets on the Process

- Go to **Brian's Talk!** The Making of the OWASP Top 10
- Room: Senate
- Nov 7 (tomorrow), 11:00 am to 11:45 am

Making of T10

Current Status

- All data has been received and processed
- Community survey has been completed
- 2025 Top 10 list is complete
- A release candidate for the document is live at https://owasp.org/www-project-top-ten/
- Needs proof-reading and editing
- Community feedback about textual descriptions, and such
- Yes – this means you

Agenda

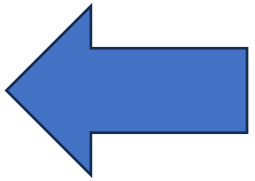
1. Housekeeping
2. What is OWASP & The Top Ten
3. How the 2025 List Was Built
4. Overview of the New Top Ten
5. The Familiar Eight
6. New! #3 Software Supply Chain Failures
7. New! #10 Mishandling of Exceptional Conditions
8. Honorable Mentions
9. How to Use the Top Ten in Your Organization
10. Community & Next Steps

TOP 10

The OWASP Top Ten 2025

A01:2025 Broken Access Control

A02:2025 Security Misconfiguration

A03:2025 Software Supply Chain Failures  Greatly Expanded!

A04:2025 Cryptographic Failures

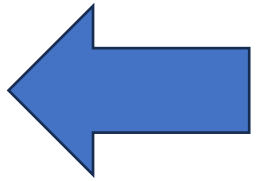
A05:2025 Injection

A06:2025 Insecure Design

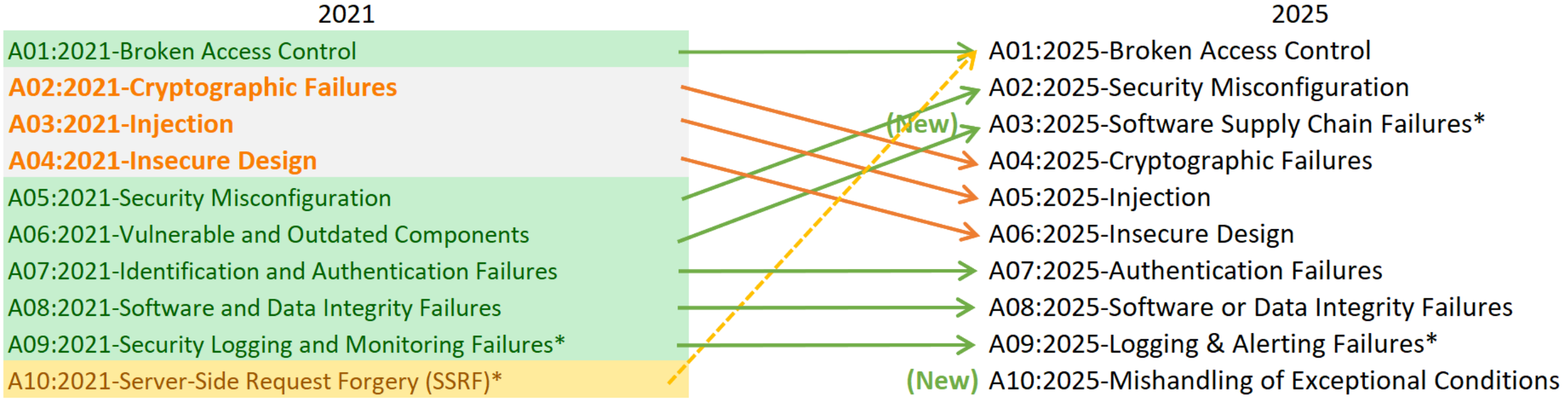
A07:2025 Authentication Failures

A08:2025 Software or Data Integrity Failures

A09:2025 Logging & Alerting Failures

A10:2025 Mishandling of Exceptional Conditions  Brand New!

The Changes



- Green – Stayed the same rank or went up
- Orange – Dropped in rank
- Yellow – Merged into another category

Agenda

1. Housekeeping
2. What is OWASP & The Top Ten
3. How the 2025 List Was Built
4. Overview of the New Top Ten
5. The Familiar Eight
6. New! #3 Software Supply Chain Failures
7. New! #10 Mishandling of Exceptional Conditions
8. Honorable Mentions
9. How to Use the Top Ten in Your Organization
10. Community & Next Steps

TOP 10

A01:2025 Broken Access Control

- Hands down the #1 category for web apps, APIs, and many other digital systems
- Failures in authorization (AuthZ), giving access where/when you should not
- Prevention: deny by default, test thoroughly, perform this action in a centralized function, add rate limiting and other limits at every opportunity, perform logging and alerting, etc.
- This covers 4 items for the current OWASP API Top Ten
- This item now includes SSRF

A02:2025 Security Misconfiguration

- A strong second, configuration mistakes that lead to security weaknesses and vulnerabilities
- Leaked credentials fall into this category, which are the top security misconfiguration
- This category is #1 for cloud and infrastructure security, hands down, specifically due to leaked credentials
- Prevention: Regular hardening, checking configurations semi-regularly, using credential scanners, disabling unnecessary features, etc.

A04:2025 Cryptographic Failures

- Yes, we skipped 3. That's after. More later!
- Often this is caused by encryption that is missing altogether (cleartext) but also misconfigurations in cryptographic features
- Data should be encrypted in transit and at rest for all systems, and in memory for more sensitive systems
- The result of this vulnerability is often sensitive data exposure
- Prevention: classify and label all data, minimize data storage requirements, protect your keys, use up-to-date and strong standard algorithms, implementations, protocols, and keys, etc.

A05:2025 Injection 

- Tricking an application into executing an attacker's code
- Generally, the malicious code is inserted where data should be, and the application mistakes it for its own code
- Good news: It was #1 from 2003-2017, #3 in 2021, #5 in 2025!
- Bad news: Prompt injection is #1 in the OWASP Top 10 for LLM Applications 😟
- Prevention: thorough and proper input validation, then escaping or sanitization of special and powerful characters, parameterized queries, code review, testing/fuzzing, using frameworks that support prevention

A06:2025 Insecure Design

- It doesn’t matter if we implement a poor design perfectly, we will still have problems
- Insecure design can lead to catastrophic consequences, and is often only found with manual testing (automated tooling is weak in this area)
- Prevention: threat modelling, secure design patterns and concepts, architecture review processes, design white boarding, security user stories, etc.

A07:2025 Authentication Failures

- When an attacker tricks a system into recognizing an invalid or incorrect user as legitimate
- Credential stuffing and brute force attacks are part of this category
- The risk for the user whose account is taken over is critical, but if the account itself is privileged, it can pose critical risk for the entire application
- Prevention: Implement mechanisms to prevent weak passwords, breached passwords, credential stuffing, brute force, etc. Enable use of password managers, passkeys, MFA, and/or passwordless. Segregate admin accounts

A08:2025 Software or Data Integrity Failures

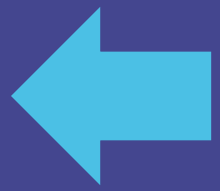
- Systems that incorrectly trust data, critical components, infrastructure, and/or updates
- Fetching resources from untrusted sources, without validating their integrity, can have dire results
- Malicious actors are attacking from this vector more often now, with threat actors posing as open-source maintainers and other positions of trust
- Prevention: use digital signatures, encryption or other methods to verify integrity, implement change review processes, etc.

A09:2025 Logging & Alerting Failures

- Without logging and monitoring, attacks and breaches cannot be detected, and without alerting it is very difficult to respond quickly and effectively during a security incident
- Insufficient, incomplete, or logs that have been tampered with are all potentially equally damaging
- Prevention: Every security control (auditable event) must be logged (success or failure), error messages and logs do not contain sensitive data, logs are protected against tampering. Establish effective monitoring and alerting use cases incl. playbooks such that suspicious activities are detected and responded to quickly.

Agenda

1. Housekeeping
2. What is OWASP & The Top Ten
3. How the 2025 List Was Built
4. Overview of the New Top Ten
5. The Familiar Eight
6. New! #3 Software Supply Chain Failures
7. New! #10 Mishandling of Exceptional Conditions
8. Honorable Mentions
9. How to Use the Top Ten in Your Organization
10. Community & Next Steps



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
  - These attacks are growing in frequency
  - They can be very costly

A03:2025 Software Supply Chain Failures

- This includes
  - CI/CD and build servers
  - Your code repository and code
  - APIs / external services that are integral to your application
  - Configuration files, secrets, infrastructure as code (IaC)
  - Developer workstation, IDE, and development environment
  - Artifacts and dependencies
  - Etc.

A03:2025 Software Supply Chain Failures

- Examples: SolarWinds, Log4J, PhantomRaven, $1.5B Bybit crypto attack
- Prevention:
  - Use a software composition analysis (SCA) or software supply chain tool or SBOM to know your dependencies **and** monitor them for vulnerabilities that pose business risk
  - Perform regular hardening across your entire supply chain, be extremely careful with access control and auditing
  - Protect developer access, train them, monitor suspicious behavior, enforce MFA, apply least privilege

Agenda

1. Housekeeping
2. What is OWASP & The Top Ten
3. How the 2025 List Was Built
4. Overview of the New Top Ten
5. The Familiar Eight
6. New! #3 Software Supply Chain Failures
7. New! #10 Mishandling of Exceptional Conditions
8. Honorable Mentions
9. How to Use the Top Ten in Your Organization
10. Community & Next Steps

A10:2025 Mishandling of Exceptional Conditions

- When programs fail to prevent, detect, and respond to unusual and unpredictable situations, which leads to crashes, unexpected behavior, and sometimes vulnerabilities
- 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
- If you solve this item, it also addresses most of Lack of Application Resilience, but the reverse is not true

A10:2025 Mishandling of Exceptional Conditions

- This can involve one or more of the following 3 failings;
  - the application doesn't prevent an unusual situation from happening,
  - it doesn't identify the situation as it is happening, and/or it
  - responds poorly or not at all to the situation afterwards
- Attacks:
  - Using sensitive info in error messages to attack more effectively
  - Race conditions, replay attacks, any attack on a partially completed transaction that was not rolled back/failed closed
  - Denial of service

A10:2025 Mishandling of Exceptional Conditions

- Prevention:
  - Catch and properly handle errors (throw error, log, then alert)
  - Implement a global exception handler
  - Functionality or tooling that watches for repeated errors or patterns that indicate an on-going attack, then blocks
  - Fail closed, roll back any incomplete transaction if error occurs
  - Add limits at every opportunity, rate limiting ,resource quotas…
  - Perform strict input validation, then escaping or sanitization
  - Perform error handling in a centralized manner

Agenda

1. Housekeeping
2. What is OWASP & The Top Ten
3. How the 2025 List Was Built
4. Overview of the New Top Ten
5. The Familiar Eight
6. New! #3 Software Supply Chain Failures
7. New! #10 Mishandling of Exceptional Conditions
8. Honorable Mentions
9. How to Use the Top Ten in Your Organization
10. Community & Next Steps

TOP 10

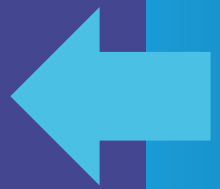
Honorable Mentions

Three categories that didn't make the final ten but should be on your radar:

1. Lack of Application Resilience (#11, was quite close to #10)
2. Memory Mismanagement Issues (#12 - far from the top in data and community feedback)
3. AI Assisted Coding (no data to support this, because of the way the data is gathered, from tools and pentests, not from incident responders, manual code review, and postmortem findings)

Agenda

1. Housekeeping
2. What is OWASP & The Top Ten
3. How the 2025 List Was Built
4. Overview of the New Top Ten
5. The Familiar Eight
6. New! #3 Software Supply Chain Failures
7. New! #10 Mishandling of Exceptional Conditions
8. Honorable Mentions
9. How to Use the Top Ten in Your Organization
10. Community & Next Steps



TOP 10

How to Use the Top Ten in Your Organization

- Integrating it into SDLC / AppSec programs
- Awareness vs. compliance
- Training and prioritization tips
- Don’t stop at 10!

Agenda

1. Housekeeping
2. What is OWASP & The Top Ten
3. How the 2025 List Was Built
4. Overview of the New Top Ten
5. The Familiar Eight
6. New! #3 Software Supply Chain Failures
7. New! #10 Mishandling of Exceptional Conditions
8. Honorable Mentions
9. How to Use the Top Ten in Your Organization
10. Community & Next Steps

TOP 10

Status

Data Collection

Industry Survey

Data Analysis

Write Up

Write Up Review and Editing

Translations

Responsive Web and Mobile Version

PDF and Developer Poster

https://www.owasptopten.org/

Community & Next Steps

- Draft writing is open for comment.
- How to provide feedback.
- Head over to #project-top-10 on OWASP Slack and say hi
- Looking for translators - #top-10-translations
- Log issues at https://github.com/OWASP/Top10
  - Suggest improvements by logging issues
  - We work in GitHub in Markdown
  - Fork and branch to create PRs

Resources

- The OWASP Top Ten site: https://owasp.org/Top10/

Slides

QR Code here for slides

Tanya Janca
And
Neil Smithline

OWASP 2025 GLOBAL AppSec | USA

THANK YOU!

Slides: https://links.shehackspurple.ca/slidelinkgoeshere