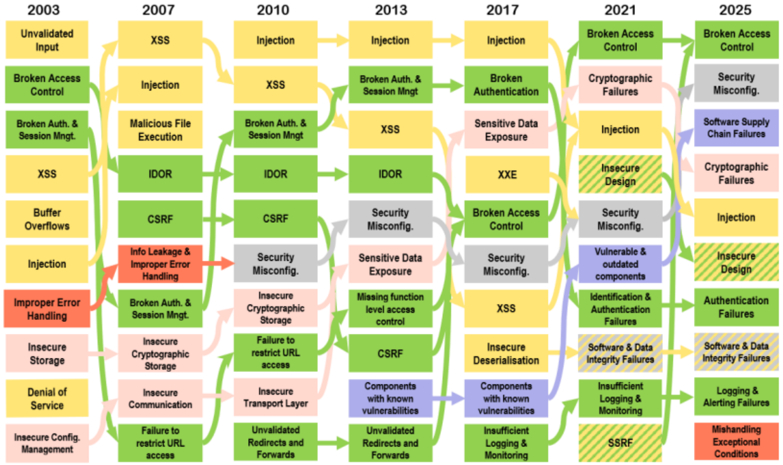
Twenty Years of OWASP Top 10



2003	2007	2010	2013	2017	2021	2025
Unvalidated Input	XSS	Injection	Injection	Injection	Broken Access Control	Broken Access Control
Broken Access Control	Injection	XSS	Broken Auth. & Session Mngt	Broken Authentication	Cryptographic Failures	Security Misconfig.
Broken Auth. & Session Mngt.	Malicious File Execution	Broken Auth. & Session Mngt	XSS	Sensitive Data Exposure	Injection	Software Supply Chain Failures
XSS	IDOR	IDOR	IDOR	XXE	Insecure Design	Cryptographic Failures
Buffer Overflows	CSRF	CSRF	Security Misconfig.	Broken Access Control	Security Misconfig.	Injection
Injection	Info Leakage & Improper Error Handling	Security Misconfig.	Sensitive Data Exposure	Security Misconfig.	Vulnerable & outdated components	Insecure Design
Improper Error Handling	Broken Auth. & Session Mngt.	Insecure Cryptographic Storage	Missing function level access control	XSS	Identification & Authentication Failures	Authentication Failures
Insecure Storage	Insecure Cryptographic Storage	Failure to restrict URL access	CSRF	Insecure Deserialisation	Software & Data Integrity Failures	Software & Data Integrity Failures
Denial of Service	Insecure Communication	Insecure Transport Layer	Components with known vulnerabilities	Components with known vulnerabilities	Insufficient Logging & Monitoring	Logging & Alerting Failures
Insecure Config. Management	Failure to restrict URL access	Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards	Insufficient Logging & Monitoring	SSRF	Mishandling Exceptional Conditions

Open Worldwide Application Security Project
Top 10 of Web Application Risks
2003-2025

Faiz Ilham Muhammad, Erik Poll, Harald Vranken

OWASP Top 10

Open *Worldwide* Application Security Project

founded 2001

name changed from Web to Worldwide in 2024

Best (only?) known for Top 10 of Web Application Risks

The Top 10 is

- great for awareness
- a great first step in improving security

but...

- *only* a first step
- *not* a 'standard' (unlike OWASP ASVS)

Other Top Ns

- OWASP Top 10 for LMM Applications & GenAI
- OWASP Mobile Top 10
- OWASP API Top 10
- OWASP Kubernetes Top 10
- ...

Top Ns by other organisations:

- CWE Top 25 Software Weaknesses, annually since 2019
- CWE Top 25 Hardware Weaknesses, since 2021

2025 edition of OWASP Top 10

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 & Data Integrity Failures
9. Logging & Alerting Failures ⭐
10. Mishandling Exceptional Conditions

8 categories based on data,

2 based on community survey ⭐

Honourable mentions:

- Lack of application resilience
- Memory corruption
- AI-assisted coding

4. Injection Attacks

CWE-89	SQL Injection
CWE-79	Cross-site Scripting (XSS)
CWE-77	Command Injection
CWE-78	OS Command Injection
CWE-90	LDAP Injection
CWE-98	PHP Remote File Inclusion
CWE-91	XML Injection
CWE-88	Argument Injection
CWE-93	CRLF Injection
CWE-643	XPath Injection
CWE-94	Code Injection
CWE-96	Static Code Injection
CWE-95	Eval Injection
CWE-97	Server-Side Includes (SSI)
CWE-99	Resource Injection
CWE-917	Expression Language Injection
CWE-113	HTTP Response Splitting

CWE-20	Improper Input Validation
CWE-116	Improper Encoding or Escaping of Output
CWE-115	Misinterpretation of Output
CWE-112	Missing XML Validation
CWE-129	Improper Validation of Array Index
CWE-470	Unsafe Reflection
CWE-493	Public Variable Without Final Modifier
CWE-500	Public Static Field Not Marked Final
CWE-610	Externally Controlled Reference to a Resource in Another Sphere

…

…

…

Path traversal attacks are included in Broken Access Control

CWE-74	Improper Neutralization of Special Elements Used by a Downstream Component ('Injection')
CWE-76	Improper Neutralization of Equivalent Special Elements
CWE-83	Improper Neutralization of Script in Attributes in a Web Page
CWE-86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages
CWE-644	Improper Neutralization of HTTP Headers for Scripting Syntax
CWE-159	Improper Handling of Invalid Use of Special Elements

6. Insecure Design

Access control

CWE-362	Race Condition
CWE-266	Incorrect Privilege Assignment
CWE-269	Improper Privilege Management
CWE-286	Incorrect User Management

Misc.

CWE-602	Client-Side Enforcement of Security
CWE-501	Trust Boundary Violation
CWE-653	Insufficient Compartmentalization
CWE-656	Reliance on Security Through Obscurity
CWE-657	Violation of Secure Design Principles
CWE-693	Protection Mechanism Failure
CWE-799	Improper Control of Interaction Frequency
CWE-841	Improper Enforcement of Behavioral Workflow
CWE-1125	Excessive Attack Surface

Information leakage

CWE-256	Unprotected Storage of Credentials
CWE-312	Cleartext Storage of Sensitive Info
CWE-313	Cleartext Storage in a File or on Disk
CWE-316	Cleartext Storage of Sensitive Info in Memory
CWE-522	Insufficiently Protected Credentials
CWE-419	Unprotected Primary Channel
CWE-525	Use of Web Browser Cache for Sensitive Info
CWE-311	Missing Encryption of Sensitive Data
CWE-539	Use of Persistent Cookies for Sensitive Info
CWE-598	GET Requests With Sensitive Query Strings

UI

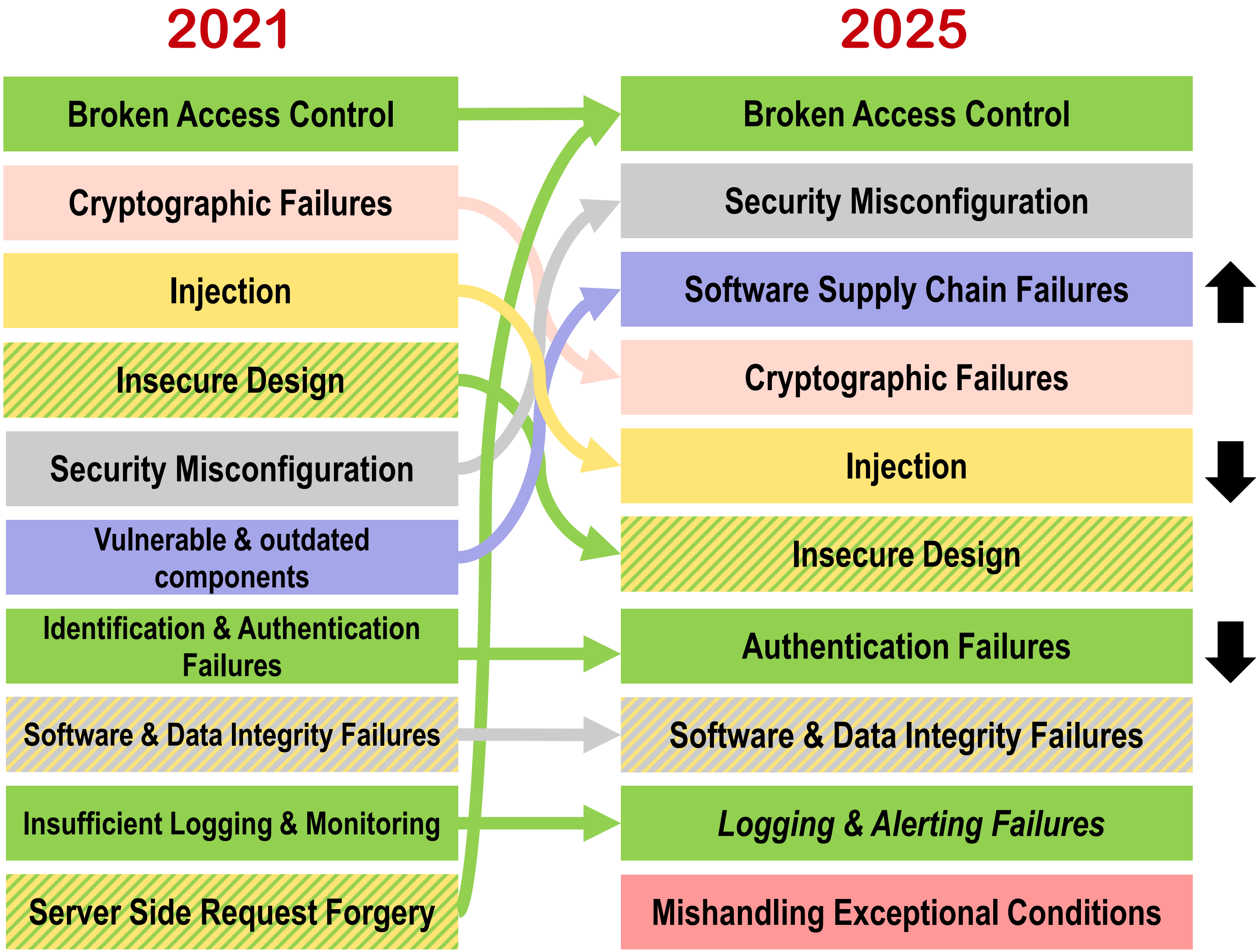
CWE-451	UI Misrepresentation of Critical Information
CWE-1021	Improper Restriction of Rendered UI Layers
CWE-1022	Untrusted Link with window.opener Access

Input handling

CWE-183	Permissive List of Allowed Inputs
CWE-434	Upload of File with Dangerous Type
CWE-436	Interpretation Conflict
CWE-444	HTTP Request Smuggling

CWE-73	External Control of File Name or Path
CWE-642	External Control of Critical State Data
CWE-646	Reliance on File Name or Extension of External File
CWE-807	Reliance on Untrusted Inputs in Security Decision
CWE-454	External Initialization of Trusted Variables or Data Stores
CWE-472	External Control of Assumed-Immutable Web Parameter

CWE-676	Use of Potentially Dangerous Function
CWE-382	J2EE Bad Practices: Use of System.exit()
CWE-628	Function Call with Incorrectly Specified Arguments



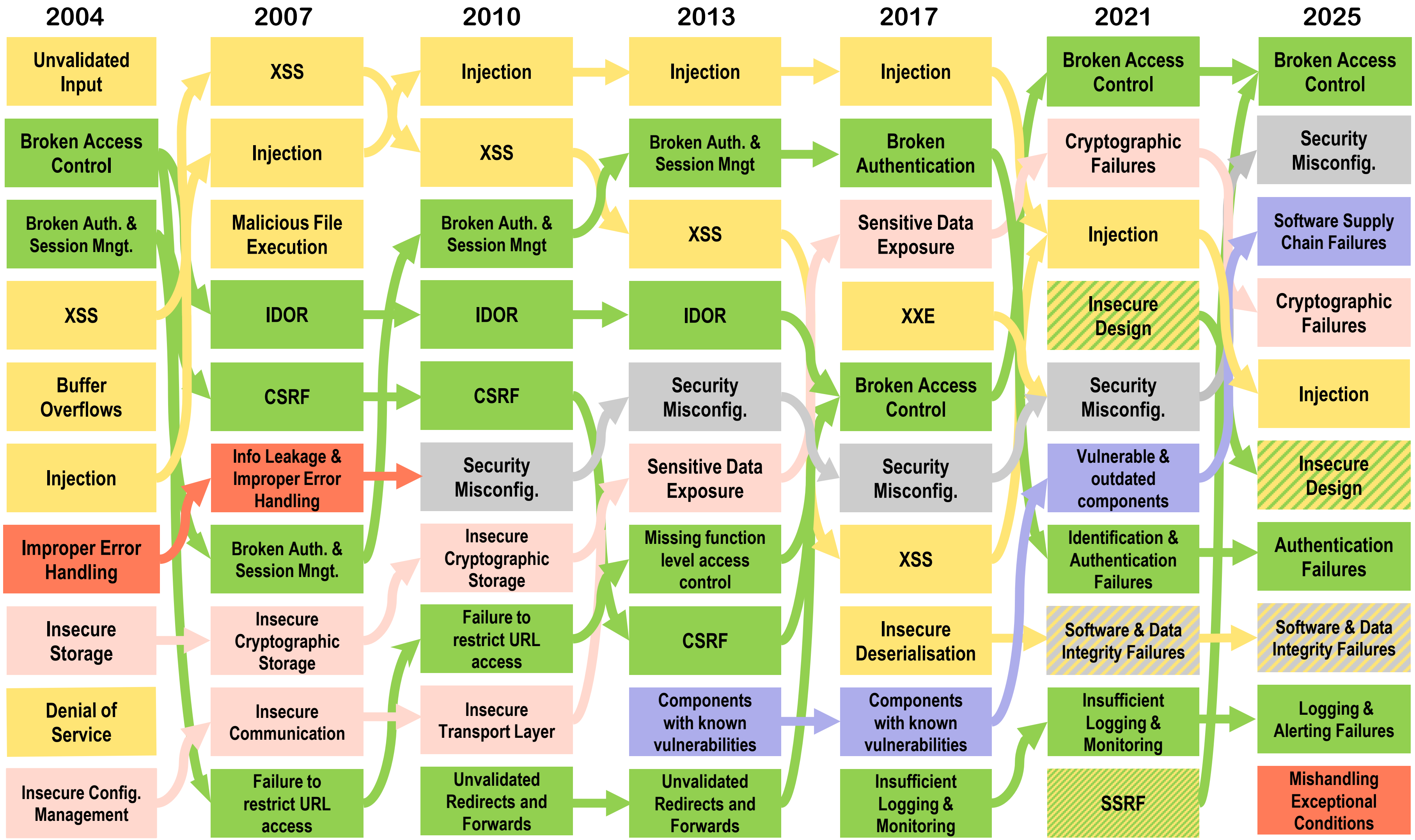
2021

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable & outdated components
- Identification & Authentication Failures
- Software & Data Integrity Failures
- Insufficient Logging & Monitoring
- Server Side Request Forgery

2025

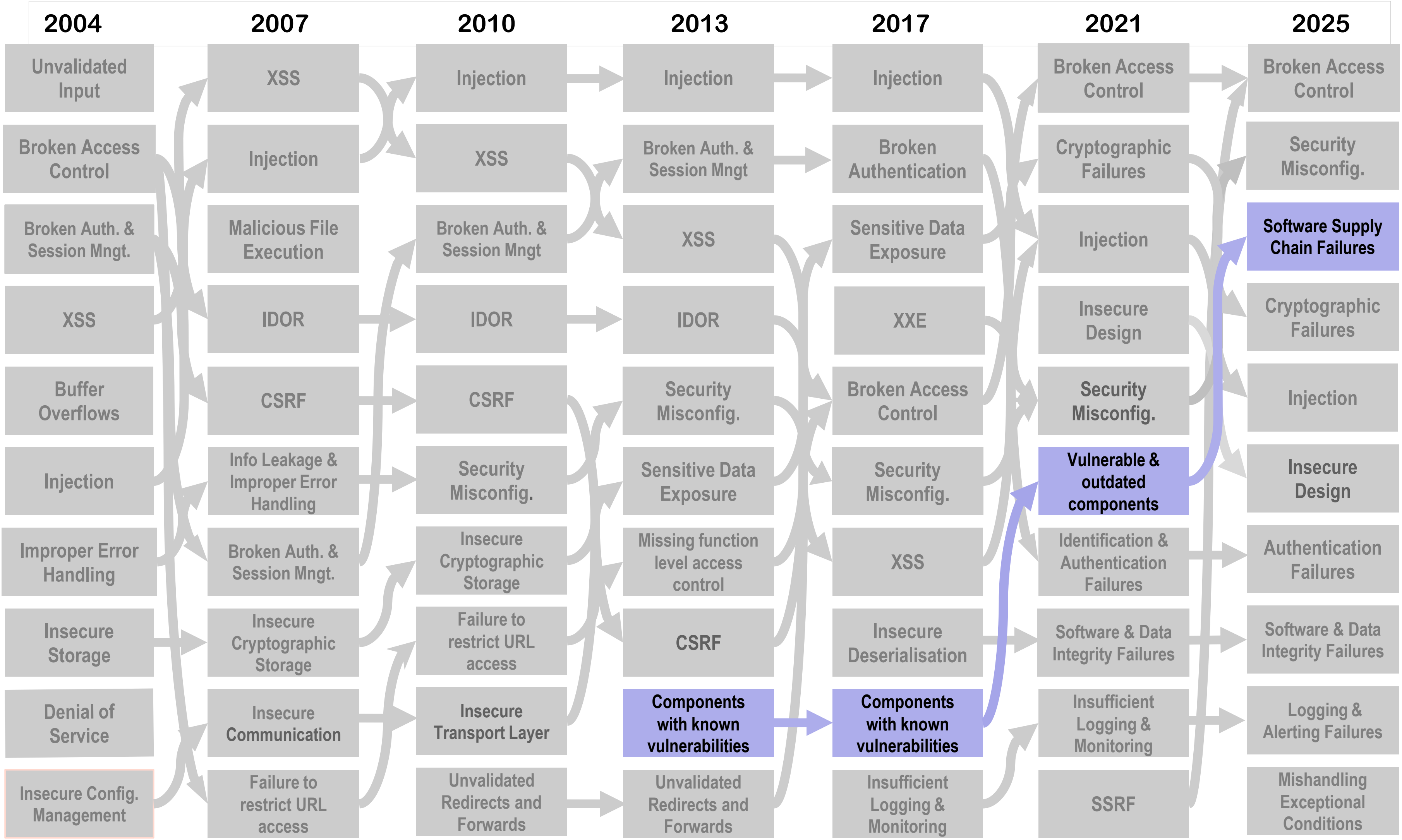
- Broken Access Control
- Security Misconfiguration
- Software Supply Chain Failures ⬆
- Cryptographic Failures
- Injection ⬇
- Insecure Design
- Authentication Failures ⬇
- Software & Data Integrity Failures
- *Logging & Alerting Failures*
- Mishandling Exceptional Conditions

Evolution of the OWASP Top 10



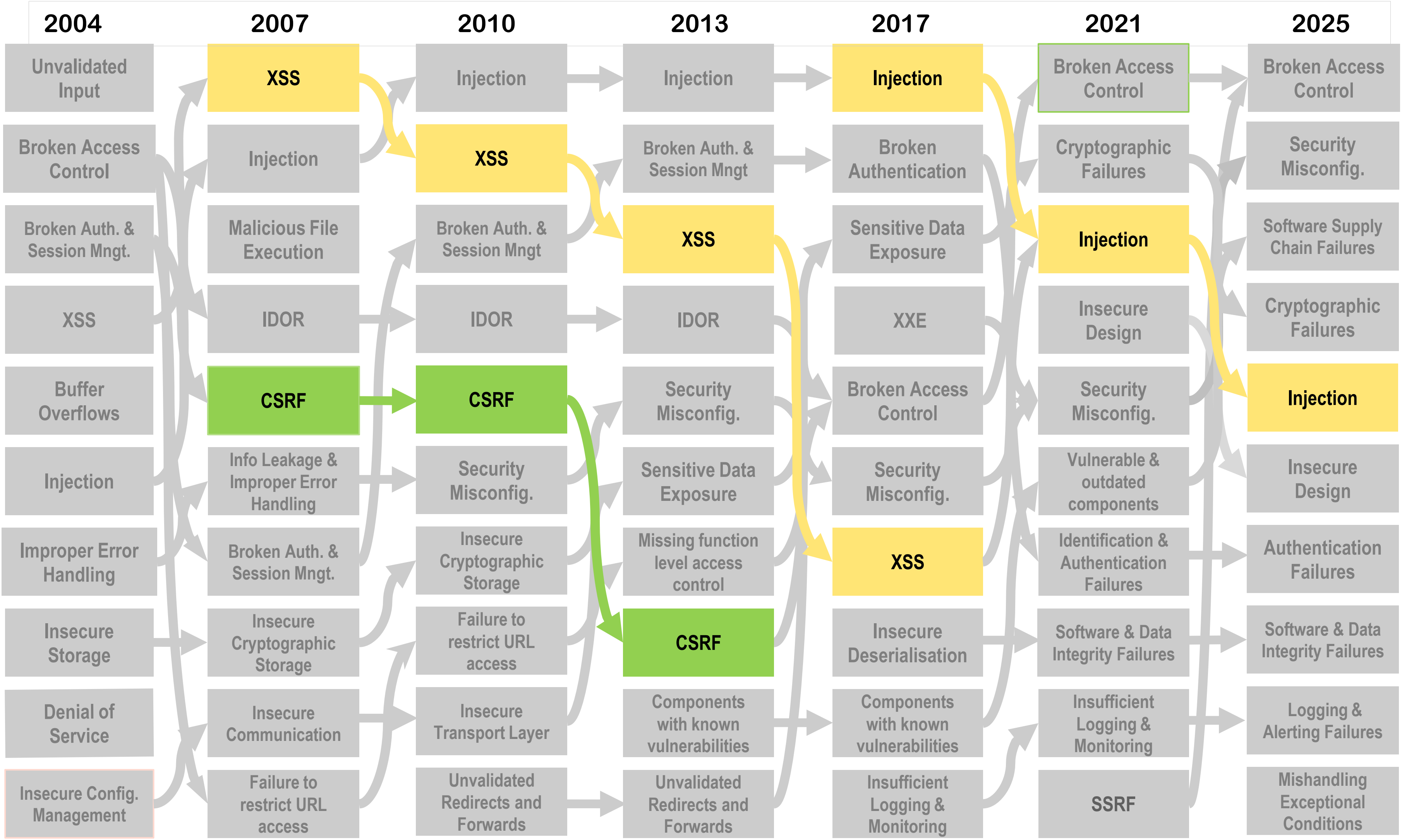
2004	2007	2010	2013	2017	2021	2025
Unvalidated Input	XSS	Injection	Injection	Injection	Broken Access Control	Broken Access Control
Broken Access Control	Injection	XSS	Broken Auth. & Session Mngt	Broken Authentication	Cryptographic Failures	Security Misconfig.
Broken Auth. & Session Mngt.	Malicious File Execution	Broken Auth. & Session Mngt	XSS	Sensitive Data Exposure	Injection	Software Supply Chain Failures
XSS	IDOR	IDOR	IDOR	XXE	Insecure Design	Cryptographic Failures
Buffer Overflows	CSRF	CSRF	Security Misconfig.	Broken Access Control	Security Misconfig.	Injection
Injection	Info Leakage & Improper Error Handling	Security Misconfig.	Sensitive Data Exposure	Security Misconfig.	Vulnerable & outdated components	Insecure Design
Improper Error Handling	Broken Auth. & Session Mngt.	Insecure Cryptographic Storage	Missing function level access control	XSS	Identification & Authentication Failures	Authentication Failures
Insecure Storage	Insecure Cryptographic Storage	Failure to restrict URL access	CSRF	Insecure Deserialisation	Software & Data Integrity Failures	Software & Data Integrity Failures
Denial of Service	Insecure Communication	Insecure Transport Layer	Components with known vulnerabilities	Components with known vulnerabilities	Insufficient Logging & Monitoring	Logging & Alerting Failures
Insecure Config. Management	Failure to restrict URL access	Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards	Insufficient Logging & Monitoring	SSRF	Mishandling Exceptional Conditions

Upwards trends



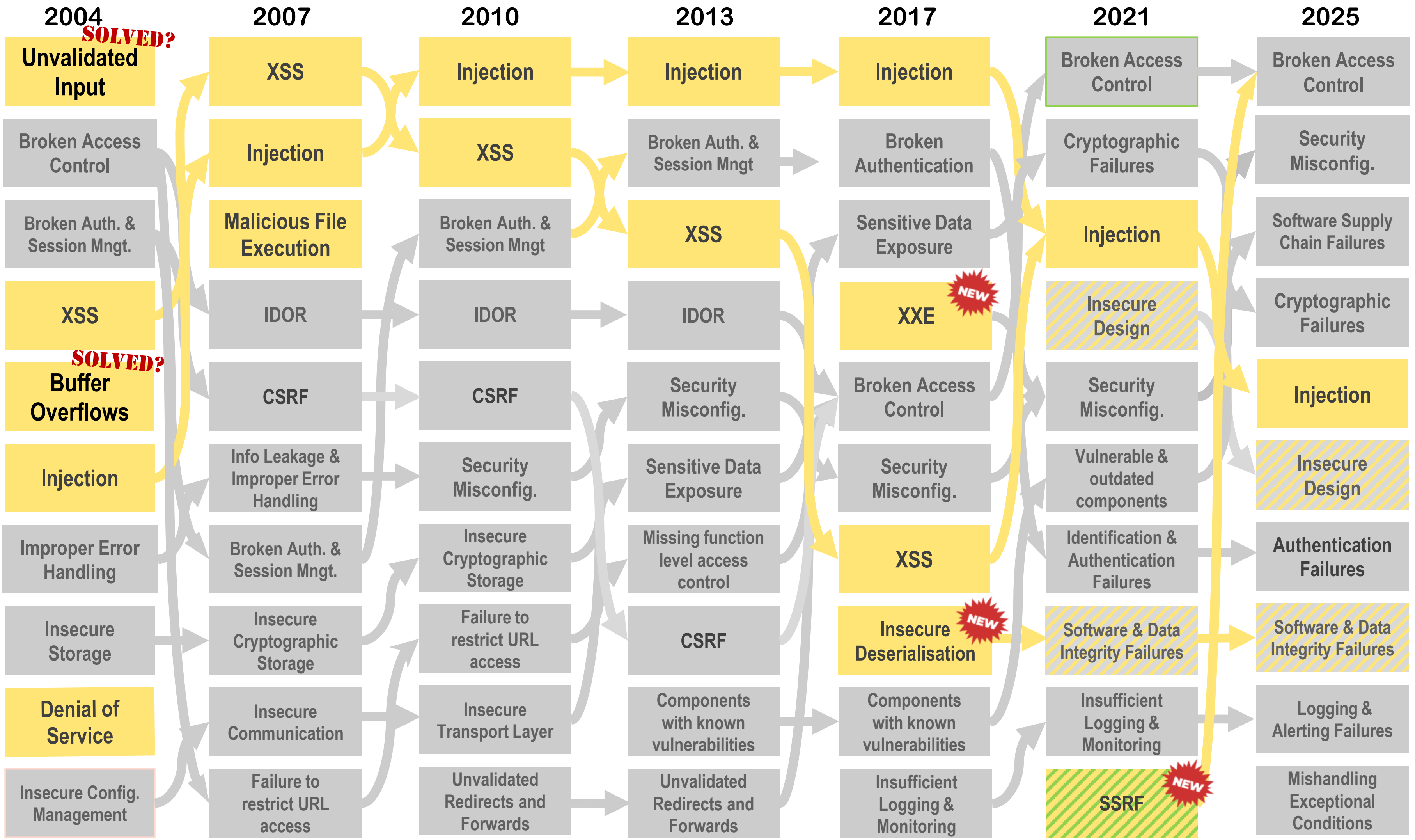
2004	2007	2010	2013	2017	2021	2025
Unvalidated Input	XSS	Injection	Injection	Injection	Broken Access Control	Broken Access Control
Broken Access Control	Injection	XSS	Broken Auth. & Session Mngt	Broken Authentication	Cryptographic Failures	Security Misconfig.
Broken Auth. & Session Mngt.	Malicious File Execution	Broken Auth. & Session Mngt	XSS	Sensitive Data Exposure	Injection	Software Supply Chain Failures
XSS	IDOR	IDOR	IDOR	XXE	Insecure Design	Cryptographic Failures
Buffer Overflows	CSRF	CSRF	Security Misconfig.	Broken Access Control	Security Misconfig.	Injection
Injection	Info Leakage & Improper Error Handling	Security Misconfig.	Sensitive Data Exposure	Security Misconfig.	Vulnerable & outdated components	Insecure Design
Improper Error Handling	Broken Auth. & Session Mngt.	Insecure Cryptographic Storage	Missing function level access control	XSS	Identification & Authentication Failures	Authentication Failures
Insecure Storage	Insecure Cryptographic Storage	Failure to restrict URL access	CSRF	Insecure Deserialisation	Software & Data Integrity Failures	Software & Data Integrity Failures
Denial of Service	Insecure Communication	Insecure Transport Layer	Components with known vulnerabilities	Components with known vulnerabilities	Insufficient Logging & Monitoring	Logging & Alerting Failures
Insecure Config. Management	Failure to restrict URL access	Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards	Insufficient Logging & Monitoring	SSRF	Mishandling Exceptional Conditions

Downward trends



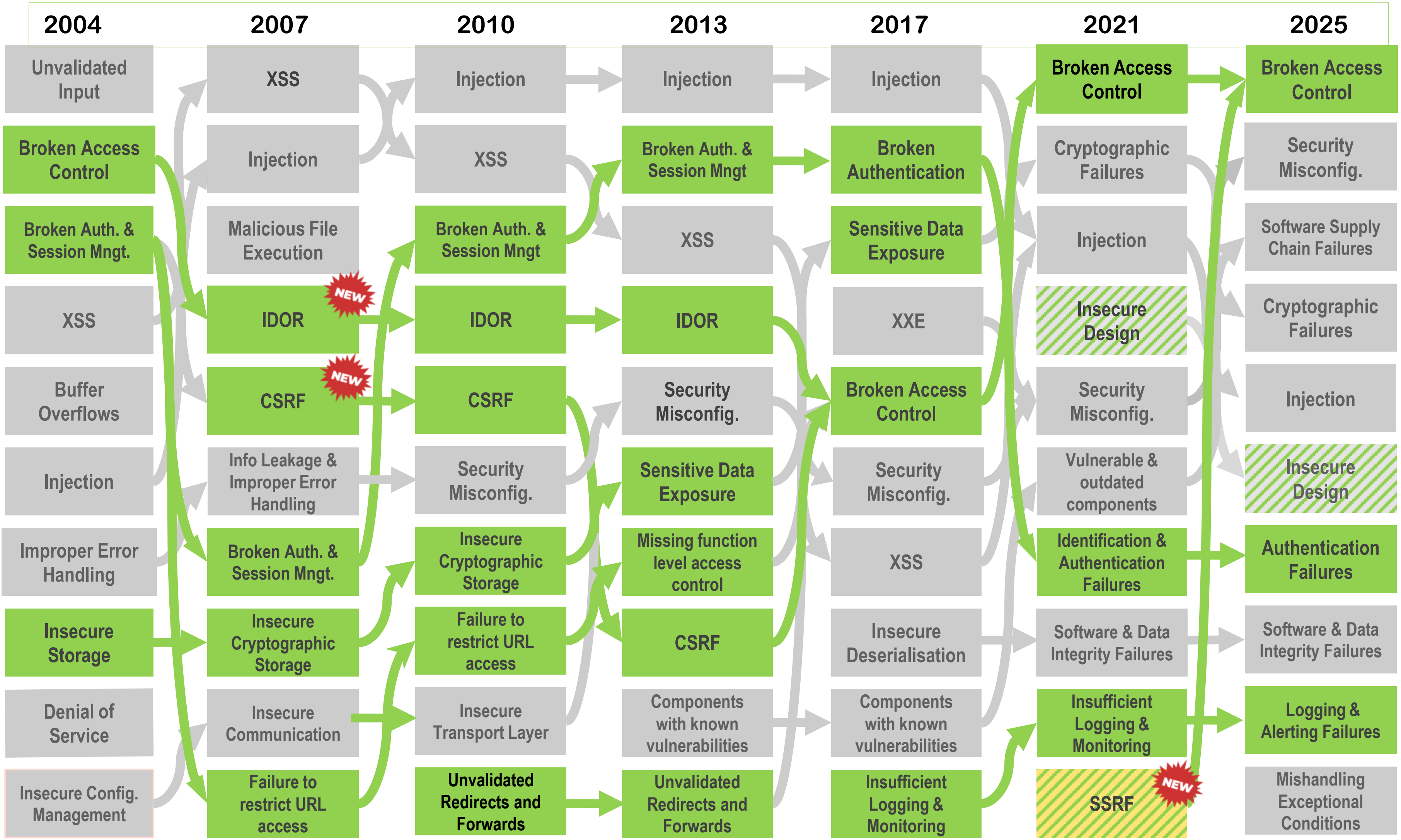
2004	2007	2010	2013	2017	2021	2025
Unvalidated Input	XSS	Injection	Injection	Injection	Broken Access Control	Broken Access Control
Broken Access Control	Injection	XSS	Broken Auth. & Session Mngt	Broken Authentication	Cryptographic Failures	Security Misconfig.
Broken Auth. & Session Mngt.	Malicious File Execution	Broken Auth. & Session Mngt	XSS	Sensitive Data Exposure	Injection	Software Supply Chain Failures
XSS	IDOR	IDOR	IDOR	XXE	Insecure Design	Cryptographic Failures
Buffer Overflows	CSRF	CSRF	Security Misconfig.	Broken Access Control	Security Misconfig.	Injection
Injection	Info Leakage & Improper Error Handling	Security Misconfig.	Sensitive Data Exposure	Security Misconfig.	Vulnerable & outdated components	Insecure Design
Improper Error Handling	Broken Auth. & Session Mngt.	Insecure Cryptographic Storage	Missing function level access control	XSS	Identification & Authentication Failures	Authentication Failures
Insecure Storage	Insecure Cryptographic Storage	Failure to restrict URL access	CSRF	Insecure Deserialisation	Software & Data Integrity Failures	Software & Data Integrity Failures
Denial of Service	Insecure Communication	Insecure Transport Layer	Components with known vulnerabilities	Components with known vulnerabilities	Insufficient Logging & Monitoring	Logging & Alerting Failures
Insecure Config. Management	Failure to restrict URL access	Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards	Insufficient Logging & Monitoring	SSRF	Mishandling Exceptional Conditions

All issues due to input handling



2004	2007	2010	2013	2017	2021	2025
SOLVED? Unvalidated Input	XSS	Injection	Injection	Injection	Broken Access Control	Broken Access Control
Broken Access Control	Injection	XSS	Broken Auth. & Session Mngt	Broken Authentication	Cryptographic Failures	Security Misconfig.
Broken Auth. & Session Mngt.	Malicious File Execution	Broken Auth. & Session Mngt	XSS	Sensitive Data Exposure	Injection	Software Supply Chain Failures
XSS	IDOR	IDOR	IDOR	XXE NEW	Insecure Design	Cryptographic Failures
SOLVED? Buffer Overflows	CSRF	CSRF	Security Misconfig.	Broken Access Control	Security Misconfig.	Injection
Injection	Info Leakage & Improper Error Handling	Security Misconfig.	Sensitive Data Exposure	Security Misconfig.	Vulnerable & outdated components	Insecure Design
Improper Error Handling	Broken Auth. & Session Mngt.	Insecure Cryptographic Storage	Missing function level access control	XSS	Identification & Authentication Failures	Authentication Failures
Insecure Storage	Insecure Cryptographic Storage	Failure to restrict URL access	CSRF	Insecure Deserialisation NEW	Software & Data Integrity Failures	Software & Data Integrity Failures
Denial of Service	Insecure Communication	Insecure Transport Layer	Components with known vulnerabilities	Components with known vulnerabilities	Insufficient Logging & Monitoring	Logging & Alerting Failures
Insecure Config. Management	Failure to restrict URL access	Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards	Insufficient Logging & Monitoring	SSRF NEW	Mishandling Exceptional Conditions

All issues due to access control



2004	2007	2010	2013	2017	2021	2025
Unvalidated Input	XSS	Injection	Injection	Injection	Broken Access Control	Broken Access Control
Broken Access Control	Injection	XSS	Broken Auth. & Session Mngt	Broken Authentication	Cryptographic Failures	Security Misconfig.
Broken Auth. & Session Mngt.	Malicious File Execution	Broken Auth. & Session Mngt	XSS	Sensitive Data Exposure	Injection	Software Supply Chain Failures
XSS	IDOR NEW	IDOR	IDOR	XXE	Insecure Design	Cryptographic Failures
Buffer Overflows	CSRF NEW	CSRF	Security Misconfig.	Broken Access Control	Security Misconfig.	Injection
Injection	Info Leakage & Improper Error Handling	Security Misconfig.	Sensitive Data Exposure	Security Misconfig.	Vulnerable & outdated components	Insecure Design
Improper Error Handling	Broken Auth. & Session Mngt.	Insecure Cryptographic Storage	Missing function level access control	XSS	Identification & Authentication Failures	Authentication Failures
Insecure Storage	Insecure Cryptographic Storage	Failure to restrict URL access	CSRF	Insecure Deserialisation	Software & Data Integrity Failures	Software & Data Integrity Failures
Denial of Service	Insecure Communication	Insecure Transport Layer	Components with known vulnerabilities	Components with known vulnerabilities	Insufficient Logging & Monitoring	Logging & Alerting Failures
Insecure Config. Management	Failure to restrict URL access	Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards	Insufficient Logging & Monitoring	SSRF NEW	Mishandling Exceptional Conditions

2025 CWE Top 25 – based on CVE data

1 Cross-Site Scripting
2 SQL Injection
3 Client-side Request Forgery (CSRF)
4 Missing Authorization
5 Out-of-bounds Write
6 Path Traversal
7 Use After Free
8 Out-of-bounds Read
9 OS Command Injection
10 Code Injection
11 Classic Buffer Overflow
12 Upload of Dangerous File
13 NULL pointer deference
14 Stack-based Buffer overflow
15 Deserialization of Untrusted Data
16 Heap-based Buffer Overflow
17 Incorrect Authorization
18 Improper Input Validation
19 Improper Access Control
20 Exposing Info to Unauthorized User
21 Missing Authentication
22 Server-Side Request Forgery (SSRF)
23 Command Injection
24 Authorization Bypass with User-Controlled Key
25 Allocation of Resources without Throttling

This ranking is based on frequency (# CVEs)
The OWASP Top 10 is based on incidence (# applications) & impact

OWASP Top 10 vs 2025 CWE Top 25

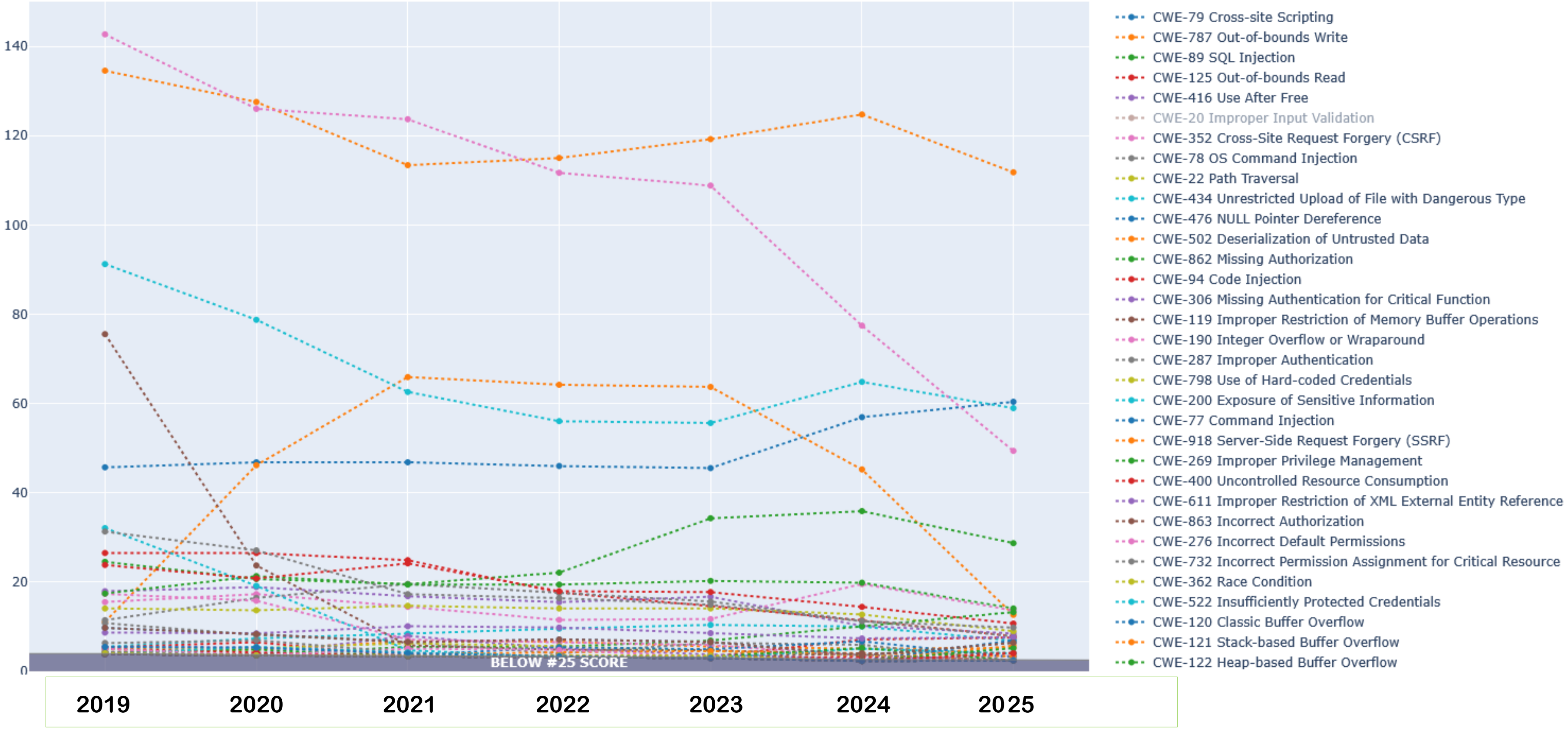
- Broken Access Control
- Security Misconfiguration
- Software Supply Chain Failures
- Cryptographic Failures
- Injection
- Insecure Design
- Authentication Failures
- Software & Data Integrity Failures
- Logging & Alerting Failures
- Mishandling Exceptional Conditions

1 Cross-site Scripting
2 SQL Injection
3 Cross-Site Request Forgery (CSRF)
4 Missing Authorization
5 Out-of-bounds Write
6 Path Traversal
7 Use After Free
8 Out-of-bounds Read
9 OS Command Injection
10 Code Injection
11 Classic Buffer Overflow
12 Upload of Dangerous File
13 NULL pointer deference
14 Stack-based Buffer overflow
15 Deserialization of Untrusted Data
16 Heap-based Buffer Overflow
17 Incorrect Authorization
18 Improper Input Validation
19 Improper Access Control
20 Exposing Info to Unauthorized User
21 Missing Authentication
22 Server-Side Request Forgery (SSRF)
23 Command Injection
24 Authorization Bypass with User-Controlled Key
25 Allocation of Resources Without Throttling

Big difference, due to

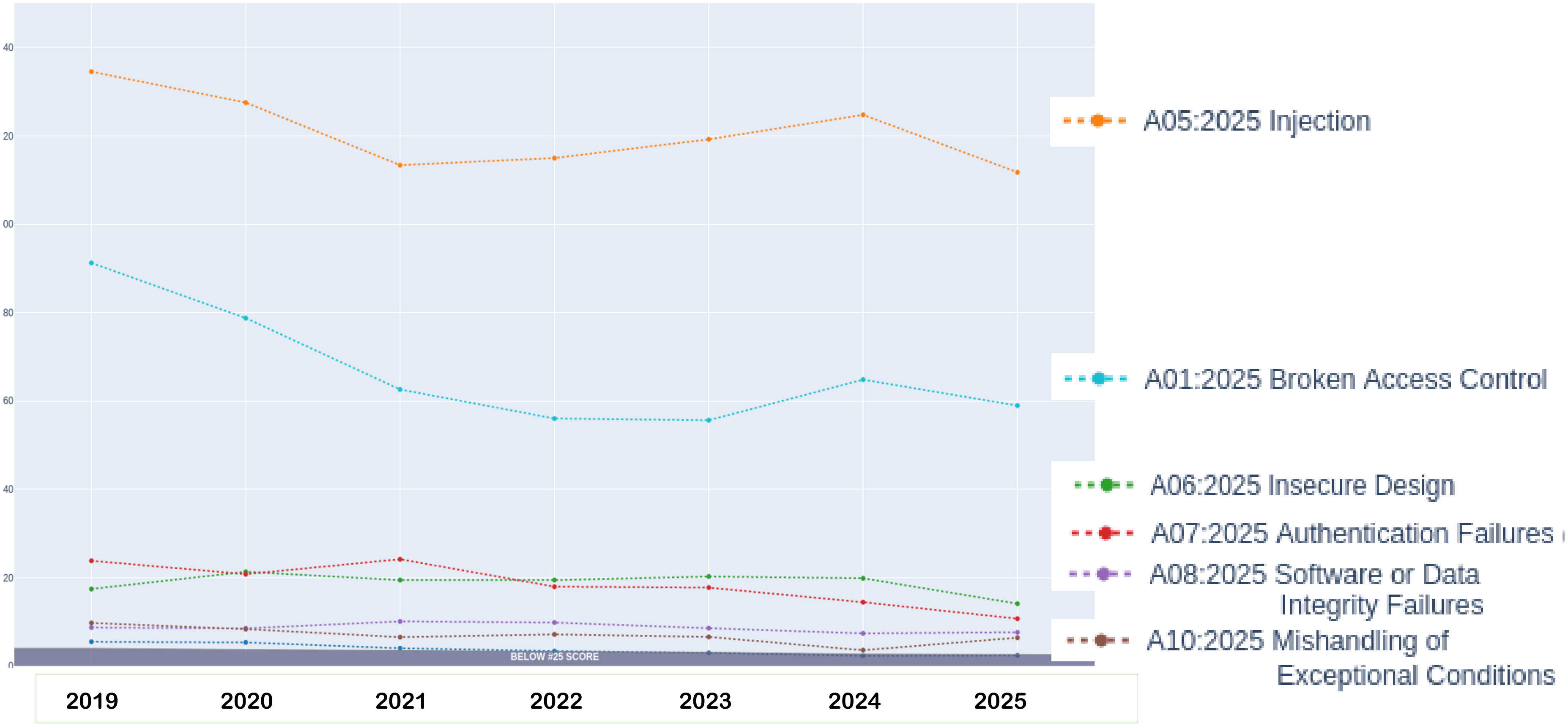
1. looking at incidence vs frequency
2. some flaws not showing up as CVEs

CWE Top 25 trends (i.e. CVE trends)

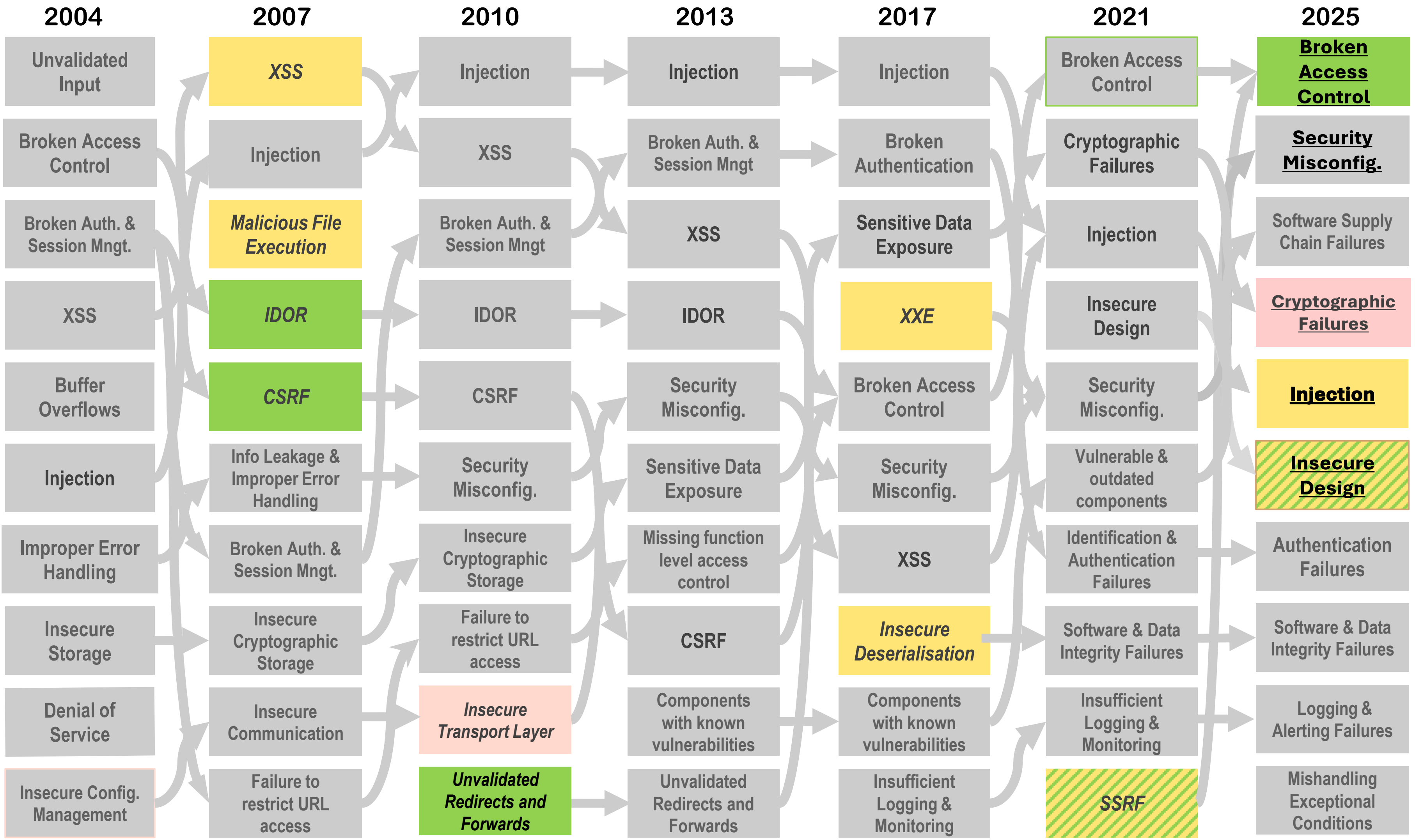


faizilham.com/lab/cwe-owasp/ranks.html

CVE trends – aggregated in the OWASP Top 10 categories



OWASP Trend: *specific* → **generic** Bad for awareness/actionability?



2004	2007	2010	2013	2017	2021	2025
Unvalidated Input	*XSS*	Injection	Injection	Injection	Broken Access Control	**Broken Access Control**
Broken Access Control	Injection	XSS	Broken Auth. & Session Mngt	Broken Authentication	Cryptographic Failures	**Security Misconfig.**
Broken Auth. & Session Mngt.	*Malicious File Execution*	Broken Auth. & Session Mngt	XSS	Sensitive Data Exposure	Injection	Software Supply Chain Failures
XSS	*IDOR*	IDOR	IDOR	*XXE*	Insecure Design	**Cryptographic Failures**
Buffer Overflows	*CSRF*	CSRF	Security Misconfig.	Broken Access Control	Security Misconfig.	**Injection**
Injection	Info Leakage & Improper Error Handling	Security Misconfig.	Sensitive Data Exposure	Security Misconfig.	Vulnerable & outdated components	**Insecure Design**
Improper Error Handling	Broken Auth. & Session Mngt.	Insecure Cryptographic Storage	Missing function level access control	XSS	Identification & Authentication Failures	Authentication Failures
Insecure Storage	Insecure Cryptographic Storage	Failure to restrict URL access	CSRF	*Insecure Deserialisation*	Software & Data Integrity Failures	Software & Data Integrity Failures
Denial of Service	Insecure Communication	*Insecure Transport Layer*	Components with known vulnerabilities	Components with known vulnerabilities	Insufficient Logging & Monitoring	Logging & Alerting Failures
Insecure Config. Management	Failure to restrict URL access	*Unvalidated Redirects and Forwards*	Unvalidated Redirects and Forwards	Insufficient Logging & Monitoring	*SSRF*	Mishandling Exceptional Conditions

4. Cryptographic Failures

(Password) Hashing

CWE-261	Weak Encoding for Password
CWE-328	Reversible One-Way Hash
CWE-759	One-Way Hash without a Salt
CWE-760	One-Way Hash with a Predictable Salt
CWE-916	Password Hash With Insufficient Computational Effort

Key management

CWE-321	Use of Hard-coded Cryptographic Key
CWE-320	Key Management Errors (Prohibited)

Not using crypto

CWE-523	Unprotected Transport of Credentials
CWE-319	Cleartext Transmission of Sensitive Info

Logic Flaws

CWE-296	Improper Following of a Certificate Chain
CWE-324	Use of a Key Past its Expiration Data
CWE-347	Improper Verification of Crypt. Signature
CWE-322	Key Exchange without Entity Authentication
CWE-323	Reusing a Nonce, Key Pair in Encryption
CWE-325	Missing Required Cryptographic Step
CWE-757	Algorithm Downgrade

Insecure crypto – i.e. real crypto failures?

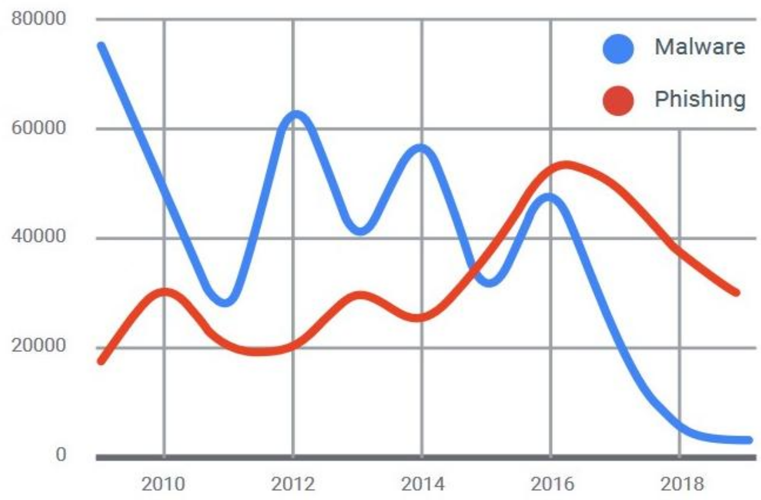
CWE-326	Inadequate Encryption Strength
CWE-327	Broken or Risky Cryptographic Algorithm
CWE-780	RSA Algorithm without OAEP
CWE-1240	Crypto Primitive with Risky Implementation

Randomness

CWE-329	Not Using a Random IV with CBC Mode
CWE-330	Use of Insufficiently Random Values
CWE-331	Insufficient Entropy
CWE-332	Insufficient Entropy in PRNG
CWE-334	Small Space of Random Values
CWE-335	Incorrect Usage of Seeds in PRNG
CWE-336	Same Seed in PRNG
CWE-337	Predictable Seed in PRNG
CWE-338	Use of Cryptographically Weak PRNG
CWE-1241	Use of Predictable Algorithm in RNG
CWE-340	Generation of Predictable Numbers or Identifiers
CWE-342	Predictable Exact Value from Previous Values

Bigger trend: software vs wetware flaws

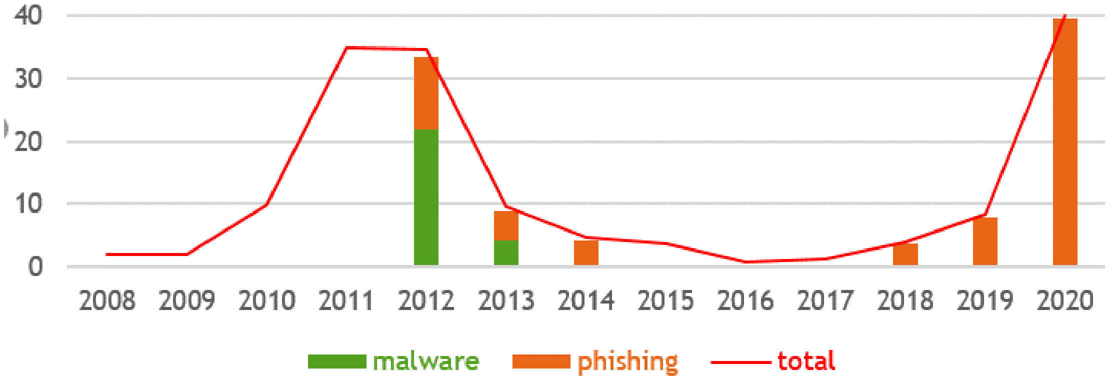
Exploit malware vs phishing detected by Google



[Source: Safe Browsing/

Google Transparency Report]

Internet banking losses in the Netherlands



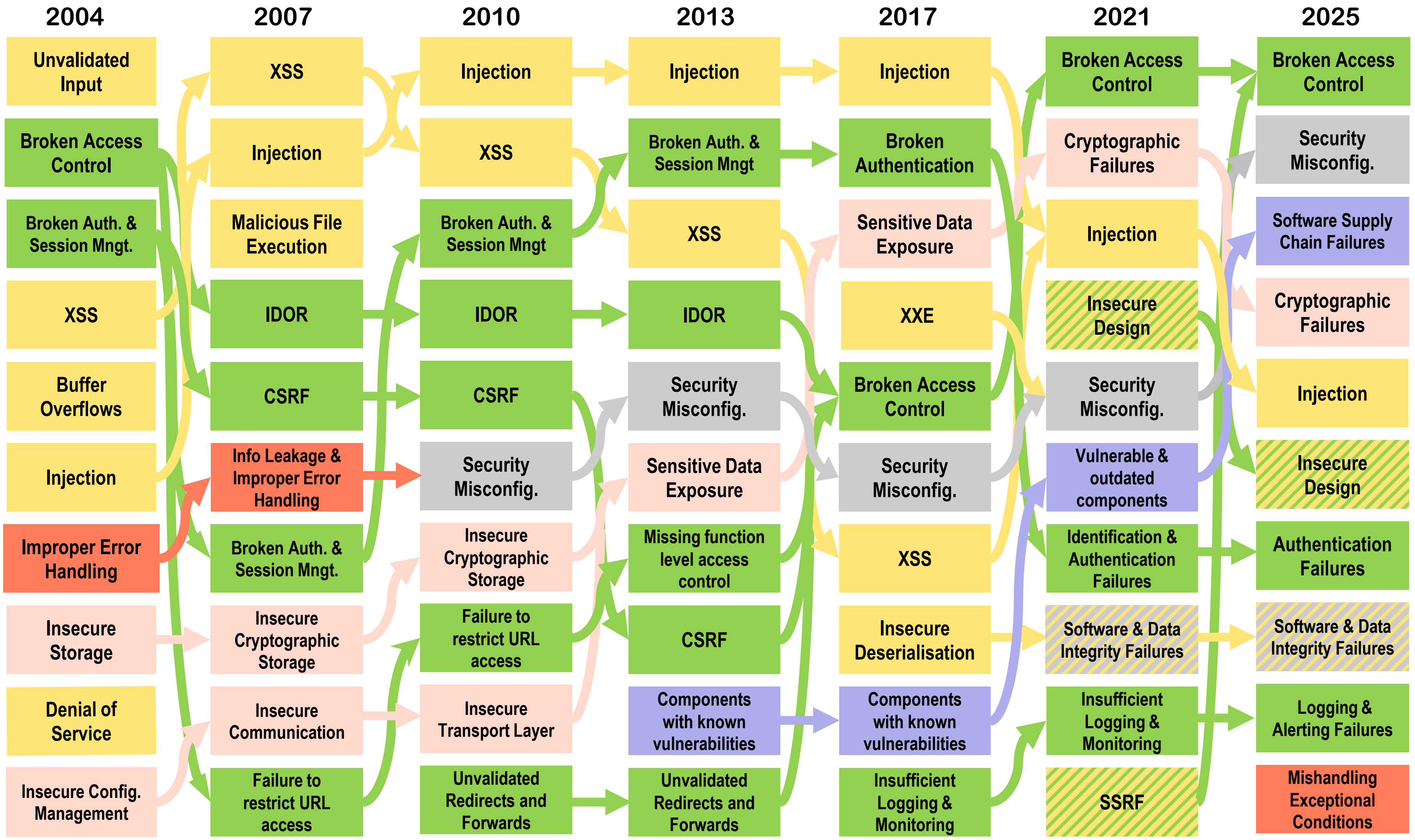
[Source: Betaalvereniging]

Conclusions

- Classification and ranking security vulnerabilities is a messy business
- Trends are hard to spot, but
  - *Supply chain issues* on the rise
  - *Injection problems* on decline (thanks to better platforms & APIs?) but not if you look at frequency instead of incidence
  - *Misconfiguration* on the rise, due to *more* platforms & APIs?
- How to maximise awareness and actionability?

faizilham.com/lab/cwe-owasp/ranks.html

Evolution of the OWASP Top 10



2004	2007	2010	2013	2017	2021	2025
Unvalidated Input	XSS	Injection	Injection	Injection	Broken Access Control	Broken Access Control
Broken Access Control	Injection	XSS	Broken Auth. & Session Mngt	Broken Authentication	Cryptographic Failures	Security Misconfig.
Broken Auth. & Session Mngt.	Malicious File Execution	Broken Auth. & Session Mngt	XSS	Sensitive Data Exposure	Injection	Software Supply Chain Failures
XSS	IDOR	IDOR	IDOR	XXE	Insecure Design	Cryptographic Failures
Buffer Overflows	CSRF	CSRF	Security Misconfig.	Broken Access Control	Security Misconfig.	Injection
Injection	Info Leakage & Improper Error Handling	Security Misconfig.	Sensitive Data Exposure	Security Misconfig.	Vulnerable & outdated components	Insecure Design
Improper Error Handling	Broken Auth. & Session Mngt.	Insecure Cryptographic Storage	Missing function level access control	XSS	Identification & Authentication Failures	Authentication Failures
Insecure Storage	Insecure Cryptographic Storage	Failure to restrict URL access	CSRF	Insecure Deserialisation	Software & Data Integrity Failures	Software & Data Integrity Failures
Denial of Service	Insecure Communication	Insecure Transport Layer	Components with known vulnerabilities	Components with known vulnerabilities	Insufficient Logging & Monitoring	Logging & Alerting Failures
Insecure Config. Management	Failure to restrict URL access	Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards	Insufficient Logging & Monitoring	SSRF	Mishandling Exceptional Conditions

8. Software & Data Integrity Failures

Input handling

CWE-345	Insufficient Verification of Data Authenticity
CWE-353	Missing Support for Integrity Check
CWE-426	Untrusted Search Path
CWE-427	Uncontrolled Search Path Element
CWE-502	Deserialization of Untrusted Data
CWE-565	Reliance on Cookies without Validation and Integrity Checking
CWE-784	Reliance on Cookies without Validation and Integrity Checking in Security Decision
CWE-915	Improperly Controlled Modification of Dynamically-Determined Object Attributes

Code handling/software supply chain issues

CWE-494	Download of Code Without Integrity Check
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-830	Inclusion of Web Functionality from an Untrusted Source
CWE-926	Improper Export of Android Application Components
CWE-506	Embedded Malicious Code
CWE-509	Replicating Malicious Code (Virus or Worm)

2. Security Misconfiguration

CWE-15	External Control of System or Configuration Setting
CWE-16	Configuration
CWE-260	Password in Configuration File
CWE-547	Use of Hard-coded, Security-relevant Constants
CWE-489	Active Debug Code
CWE-5	J2EE Misconfiguration: Data Transmission Without Encryption
CWE-11	ASP.NET Misconfiguration: Creating Debug Binary
CWE-13	ASP.NET Misconfiguration: Password in Configuration File
CWE-1174	ASP.NET Misconfiguration: Improper Model Validation

Cookies & CORS

CWE-315	Cleartext Storage of Sensitive Information in a Cookie
CWE-614	Sensitive Cookie in HTTPS Session Without 'Secure' Flag
CWE-1004	Sensitive Cookie Without 'HttpOnly' Flag
CWE-526	Exposure of Sensitive Information Through Environment Variables
CWE-942	Permissive Cross-domain Policy with Untrusted Domains

Injection attacks

CWE-611	Improper Restriction of XML External Entity Reference
CWE-776	XML Entity Expansion