
OPEN WEB APPLICATION SECURITY PROJECT
OWASP TOP 10 VULNERABILITIES

What is the OWASP Top 10?

A list of the top ten web application vulnerabilities

- Determined by OWASP and the security community at large
- Released every few years
- Most recently released in 2017
- First release in 2003

OWASP

Open Web Application Security Project

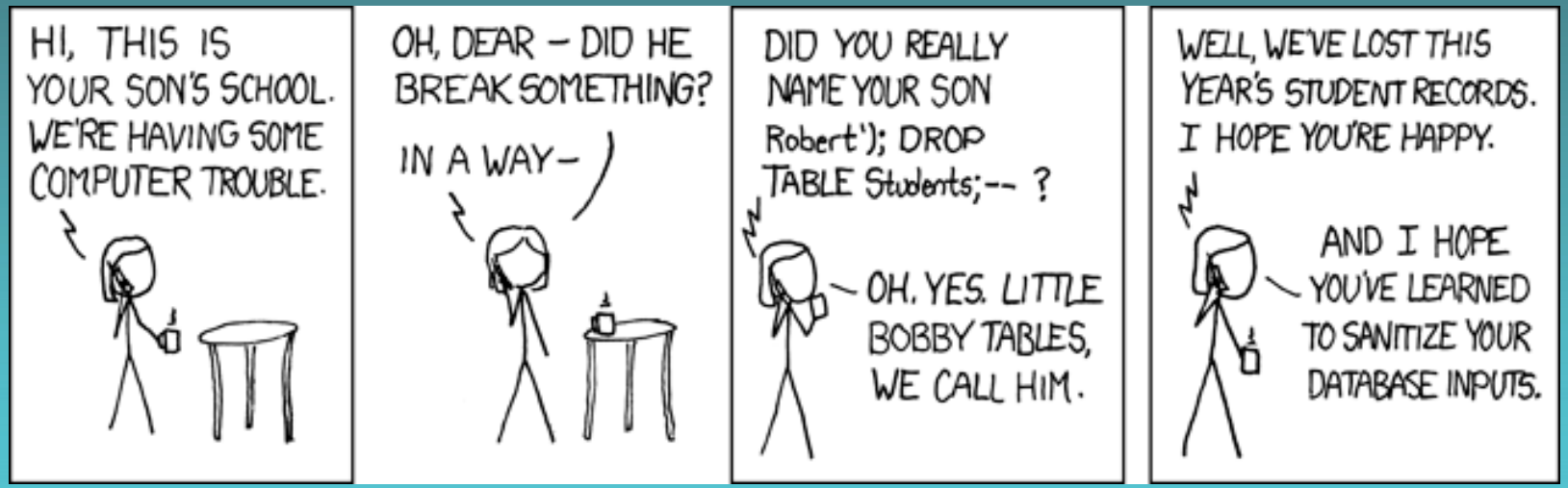
What are the OWASP Top 10 Vulnerabilities for 2017?

A1: Injection
A2: Broken Authentication
A3: Sensitive Data Exposure
A4: XML External Entities (XEE)
A5: Broken Access Control
A6: Security Misconfiguration
A7: Cross-Site Scripting
A8: Insecure Deserialization
A9: Using Components with Known Vulnerabilities
A10: Insufficient Logging and Monitoring

OWASP Top 10 Breakdown – Part 1

A1: Injection

- First placed at A1 in 2010
- Best known for SQL Injection
- Occurs anytime untrusted input is used as an execution command.



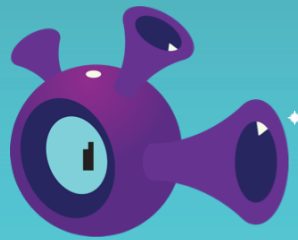
OWASP Top 10 Breakdown – Part 2

A2: Broken Authentication

- Broad category
- Covers issues such as Credential Stuffing, Insecure Password Reset, Session Management Issues, and Insufficient Password Complexity

A3: Sensitive Data Exposure

- Covers the display of data, data at rest, and data in transit
- Sensitive data that does not need to be kept, should not be
- Sensitivity of data should be categorized
- Data should be protected in accordance with how sensitive it is



OWASP Top 10 Breakdown – Part 3

A4: XML External Entities (XEE)

- Occurs when XML parsers allow loading of external entities
- Commonly occurs in older XML processors, as they are configured to allow loading of external entities by default
- Can be used to steal data, perform denial of service attacks, or map out the application and its environment

A5: Broken Access Control

- The other “auth” and just as broad
- Centered around vulnerabilities that allow a user to have access to data and application functionality that the developers did not intend

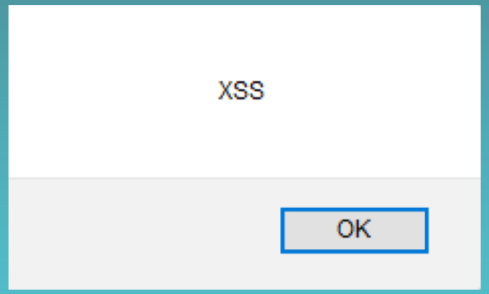
OWASP Top 10 Breakdown – Part 4

A6: Security Misconfiguration

- Occurs anytime an insecure default setting goes ignored or a server or application is configured without security in mind
- Examples include the application returning stack traces or other default messages to the client and vulnerabilities such as Web Cache Deception

A7: Cross-Site Scripting

- Also known as XSS
- Occurs in applications that do not properly handle untrusted input
- Two most common “flavors” are Persisted and Reflected



OWASP Top 10 Breakdown – Part 5

A8: Insecure Deserialization

- Deserialization is a process where structured data is taken and turned into an object
- Applications that use weak deserialization methods are vulnerable to Insecure Deserialization
- Native language serialization formats are often weak
- Makes it possible for data to be interpreted as code, or in a way that an attacker can take advantage of

"Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks."

–OWASP Top 10 - 2017

OWASP Top 10 Breakdown – Part 6

A9: Using Components with Known Vulnerabilities

- Just like in in-house code, vulnerabilities can pop up in 3rd party code and tools
- If the code is still supported, generally a patch can be applied
- If it's no longer supported, a replacement or work-around may be required

A10: Insufficient Monitoring and Logging

- Logging and monitoring is often overlooked
- Proper logging provides valuable information to developers and security teams that can be used to improve weak points
- In the event of a breach, logging and monitoring data can be used to assist with quicker response times, reducing impact

CHANGES IN THE OWASP TOP 10

Notable Changes the OWASP Top 10 from 2013 to 2017

Early versions of the 2017 list were intensely discussed. Over the course of 2017, the list was refined until it became what we have today.

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Breakdown of Changes Between 2013 and 2017 Part 1

A1:

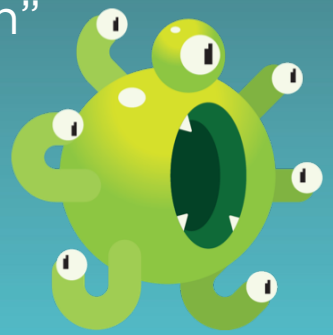
- Unchanged, Injection remains at the top spot

A2:

- Broken Authentication and Session Management remains in the second spot
- Name has been shorted to simply “Broken Authentication”

A3:

- Previously occupied by Cross-Site Scripting (XSS)
- Now Sensitive Data Exposure



A4:

- The previous A4 category was Insecure Direct Object References
- A new category, XML External Entities (XEE) was placed here in 2017

Breakdown of Changes Between 2013 and 2017 Part 2

A5:

- In 2013, A5 went to Security Misconfiguration
- 2013's A4 (Insecure Direct Object Reference) and A7 (Missing Function Level Access Control) categories have combined to become Broken Access Control

A6:

- 2013's A5, Security Misconfiguration has been placed at A6 in 2017

A7:

- Previously, this spot went to Missing Function Level Access Control
- Now occupied by Cross-Site Scripting (XSS)

Breakdown of Changes Between 2013 and 2017 Part 3

A8:

- The now removed category, Cross-Site Request Forgery, sat here in 2013
- Insecure Deserialization (a new category) has been placed at A8

A9:

- Unchanged, remains as Using Components with Known Vulnerabilities

A10:

- 2013's A10, Unvalidated Redirects and Forwards, was removed from the Top 10
- Now occupied by the new category, Insufficient Logging and Monitoring

Summary

- The OWASP Top 10 does not cover every web application security vulnerability
- The Top 10 is a fantastic foundation on which to build an application security plan that also considers the needs of the application and organization

OWASP is a non-profit and is always looking for volunteer assistance for its projects, you can find their website here if you want to learn more

About Cypress Data Defense:

Our goal is to help organizations secure their IT development and operations using a pragmatic, risk-based approach. The diverse background of our founders allows us to apply security controls to governance, networks, and applications across the enterprise.

Contact us to learn more!

https://www.cypressdatadefense.com/contact/

Email: info@cypressdatadefense.com

Phone Number: 720.588.8133

REFERENCES:

"XKCD 'Exploits of a Mom'" https://xkcd.com/327/

"OWASP Top 10 - 2017" https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf