OWASP Top Ten 2021

Where we've been and where we are

Who We Be

Nathan Larson wrote vulnerable software for two decades before wandering into an appsec class about 10 years ago and catching the security bug. His favorite security defect is *H. sapiens*.

Alex Bauert has worked in software and software security for over 2 decades. He has contributed to and led app sec efforts at a number of companies.

What we'll touch on tonight

- A little review
- The OWASP Top Ten 2021
- What's changed over the years
- What hasn't changed
- The New Items
- What's the Value of the Top Ten?
- Open Discussion

Gotta start somewhere...

- Initially ad-hoc
- Later editions used surveys
- 2021 edition uses data and survey feedback
  - Data → 8 categories
  - Surveys → 2 categories
- Why not just rely on data?
  - When vulns show up in data they've been exploited for years

Quantifying the mess

- Finding frequency does not factor in
  - Tools will find many instances of a defect
- Incidence rate more useful
  - What pct of apps had a given defect?
  - Gives a better view of risk (attacker needs one instance of defect)

Growing pains

- Analyzing a lot of CWE categories
  - About 30 CWEs before
  - Nearly 400 CWEs now (didn’t restrict)
- Changes to the structure needed
  - Allow for better training alignment

A little History

Comparison of 2003, 2004, 2007, 2010 and 2013 Releases

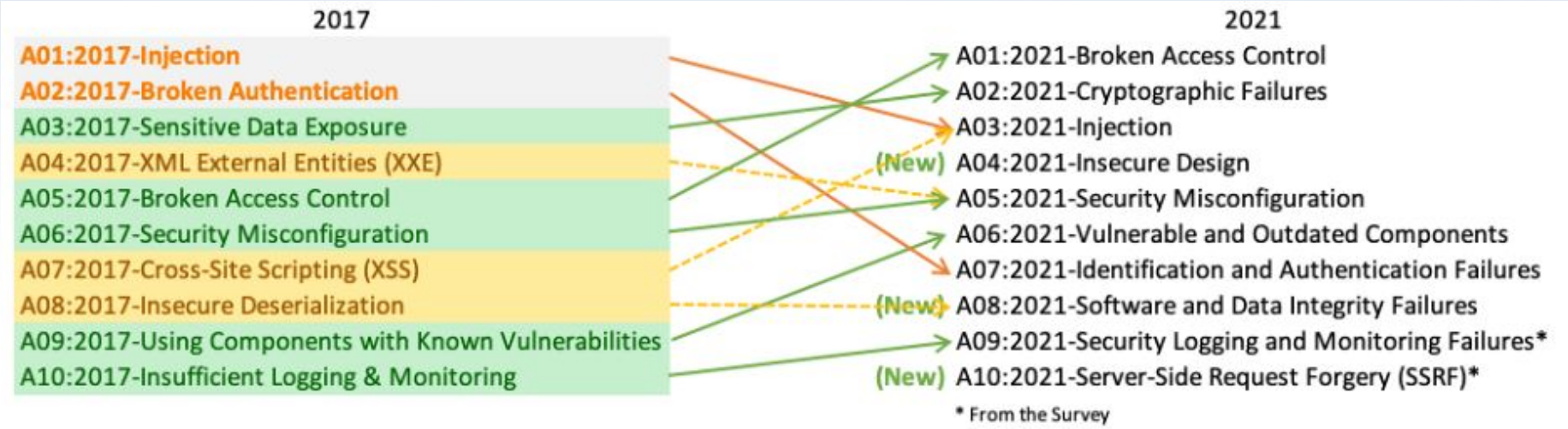
OWASP Top Ten Entries (Unordered)	Releases				
	2003	2004	2007	2010	2013
Unvalidated Input	A1	A1[9]	×	×	×
Buffer Overflows	A5	A5	×	×	×
Denial of Service	×	A9[2]	×	×	×
Injection	A6	A6[3]	A2	A1[10]	A1
Cross Site Scripting (XSS)	A4	A4	A1	A2	A3
Broken Authentication and Session Management	A3	A3	A7	A3	A2
Insecure Direct Object Reference	×	A2	A4[11]	A4	A4
Cross Site Request Forgery (CSRF)	×	×	A5	A5	A8
Security Misconfiguration	A10	A10[3][5]	×	A6	A5
Missing Functional Level Access Control	A2	A2[1]	A10[13]	A8	A7[16]
Unvalidated Redirects and Forwards	×	×	×	A10	A10
Information Leakage and Improper Error Handling	A7	A7[14][4]	A6	A6[8]	×
Malicious File Execution	×	×	A3	A6[8]	×
Sensitive Data Exposure	A8	A8[6][5]	A8	A7	A6[17]
Insecure Communications	×	A10	A9[7]	A9	×
Remote Administration Flaws	A9	×	×	×	×
Using Known Vulnerable Components	×	×	×	×	A9 [18][19]

Another Transition

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.]

OWASP Top 10 2017 to 2021

- Rank updates
- New categories
- Expanded categories
- Focuses on root causes when possible



New to the Top Ten

- Insecure Design
- Software & Data Integrity Failures
- Server Side Request Forgery

A04: Insecure Design

You didn’t Shift-Left far enough

Secure Design and Secure Patterns

Threat Modeling

But we already do SAST/DAST

Before the code

Context is Everything

A08: Software & Data Integrity Failures

“Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs).” *from the OWASP Top Ten page

Sounds like Software Supply Chain but really isn’t
Difference is that these vulnerabilities leverage execution within.
This groups vulnerabilities injected into the payloads of otherwise benign artifacts before endpoint delivery - for example

Insecure Deserialization - the log4j vulnerability this week

A10: Server Side Request Forgery

- App fetches remote resource without validating URL supplied by user
- Survey-generated entry
  - Data not supporting – yet
- So what? Attackers can use SSRF to:
  - Scan for open ports on the network
  - Access files local to the server
  - Read metadata of cloud services
  - Abuse internal services for further mischief
- Plan is to roll into a category eventually – where would it make sense?

Subsumed 2017 categories

Cross-Site Scripting – now in Injection

Insecure Deserialization – Software and Data Integrity Failures

XML External Entities – now in Security Misconfiguration

Use Case	OWASP Top 10 2021	OWASP Application Security Verification Standard
Awareness	Yes	
Training	Entry level	Comprehensive
Design and architecture	Occasionally	Yes
Coding standard	Bare minimum	Yes
Secure Code review	Bare minimum	Yes
Peer review checklist	Bare minimum	Yes
Unit testing	Occasionally	Yes
Integration testing	Occasionally	Yes
Penetration testing	Bare minimum	Yes
Tool support	Bare minimum	Yes
Secure Supply Chain	Occasionally	Yes

How to use the list?

- Evolution of the list has changed. How should we use it?
  - Less specific over time
  - OWASP Top Ten Vulnerabilities doesn't mean the same any more
    - SAST/DAST Filters and how many results does this mean
    - Standards or Frameworks that say no OWASP Top Ten

What is the value of a top 10 list?

- Origin subjective; enough evidence now?
- Specific enough to be useful to most?
- Does this kind of tool help make risk decisions?
- How has the battle gone over 20 years?
- Line in the Sand
  - Back to context and which risks matter

Discussion

- How do you use the Top 10?

What's next?

- Research something you want to share?
- Have lots of knowledge about a topic?
- Just love appsec so much, you can't help it?

OWASP chapters always need speakers!
See the Meetup group for info
Contact Alex or Nate with ideas

References

- https://owasp.org/Top10