OWASP
Open Web Application Security Project

OWASP TOP 10

VS

OWASP ASVS

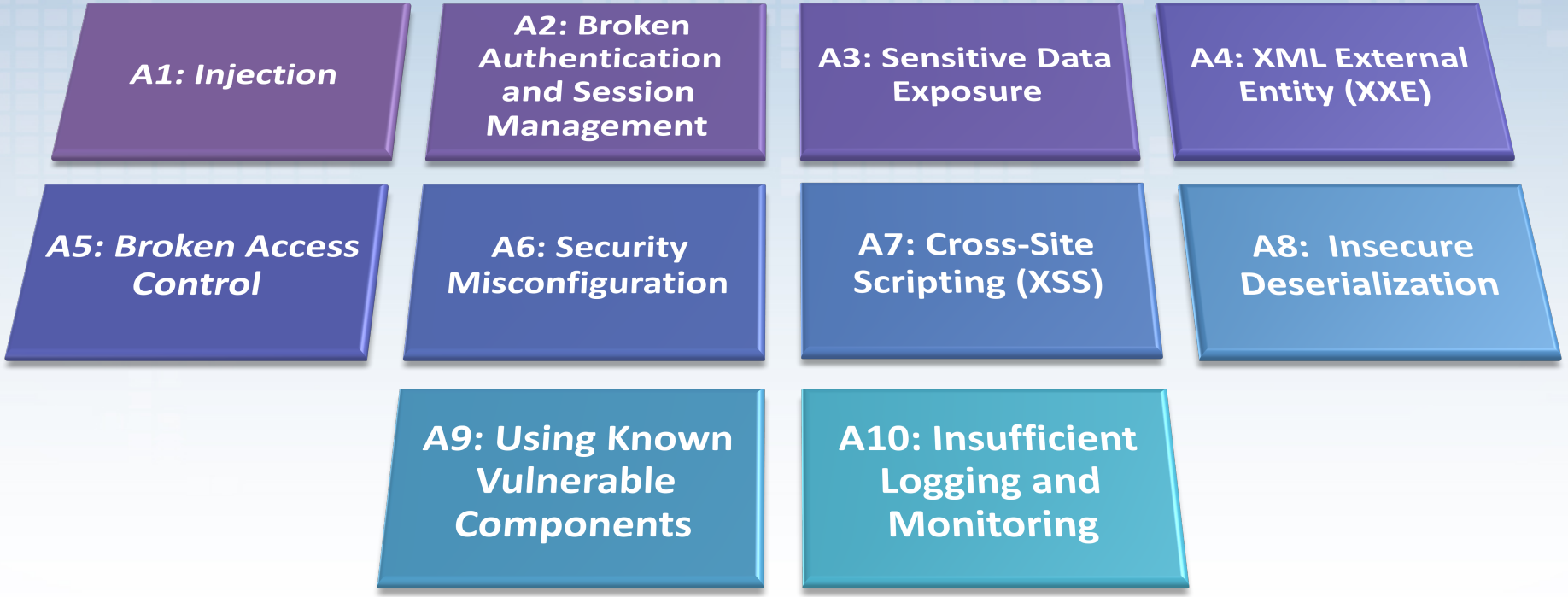
Joe Blanchard | St. Louis OWASP Chapter

The OWASP Top Ten

- The OWASP Top 10 provides a list of the **10 Most Critical Web Application Security Risks.** **(since 2004)**
- Project members include a **variety of security experts from around the world** who have shared their expertise to produce this list.
- This list is meant to **spread awareness** regarding Web Security issues. *It is not a standard.*
- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

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 Ten (2017)



OWASP
Open Web Application Security Project

Web Application Technical Security Controls, Unleashed!

OWASP Application Security Verification Standard 3.0

The OWASP Application Security Verification Standard (ASVS) Project provides a basis for testing web application technical security controls and also provides developers with a list of requirements for secure development.

The primary aim of the **OWASP Application Security Verification Standard (ASVS) Project** is to normalize the range in the coverage and level of rigor available in the market when it comes to performing Web application security verification using a commercially-workable open standard.

Use as a metric - Provide application developers and application owners with a yardstick with which to assess the degree of trust that can be placed in their Web applications.

Use as guidance - Provide guidance to security control developers as to what to build into security controls in order to satisfy application security requirements, and

Use during procurement - Provide a basis for specifying application security verification requirements in contracts.

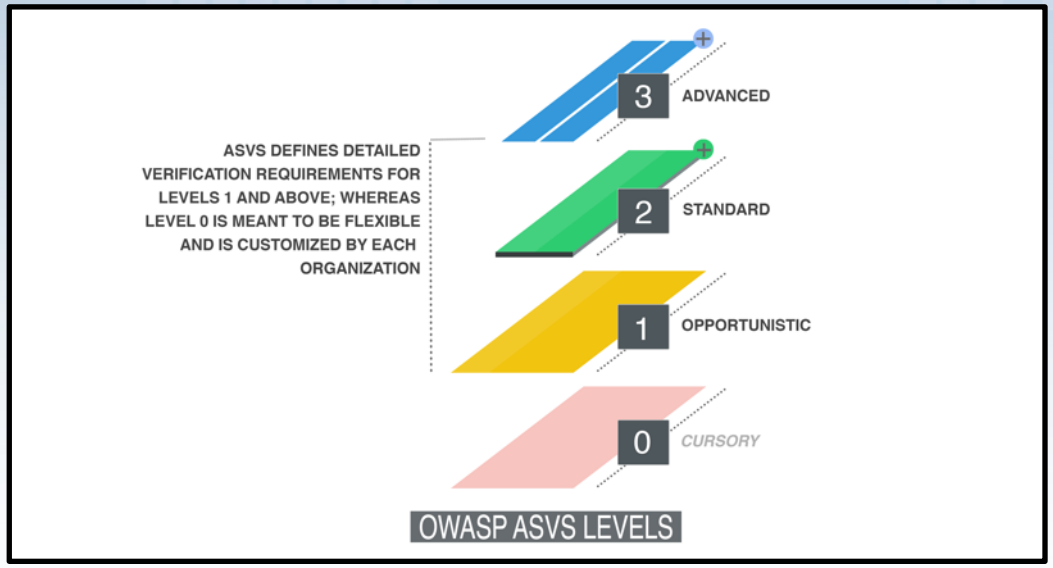
ASVS MAIN GOALS

- to help organizations develop and maintain secure applications
- to allow security service, security tools vendors, and consumers to align their requirements and offerings

The Application Security Verification Standard defines three security verification levels, with each level increasing in depth.

- ASVS Level 1 is meant for all software.
- ASVS Level 2 is for applications that contain sensitive data, which requires protection.
- ASVS Level 3 is for the most critical applications - applications that perform high value transactions, contain sensitive medical data, or any application that requires the highest level of trust.

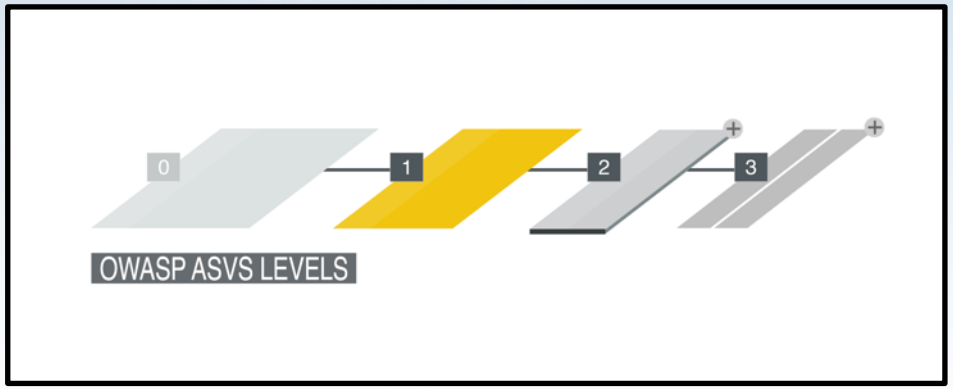
Application Security Verification Standard 3.0



- First application security standard by developers, for developers
- Defines three risk levels with around 150 controls
- Similar but not the same: ISO 27034

OWASP
Open Web Application Security Project

Application Security Verification Standard 3.0



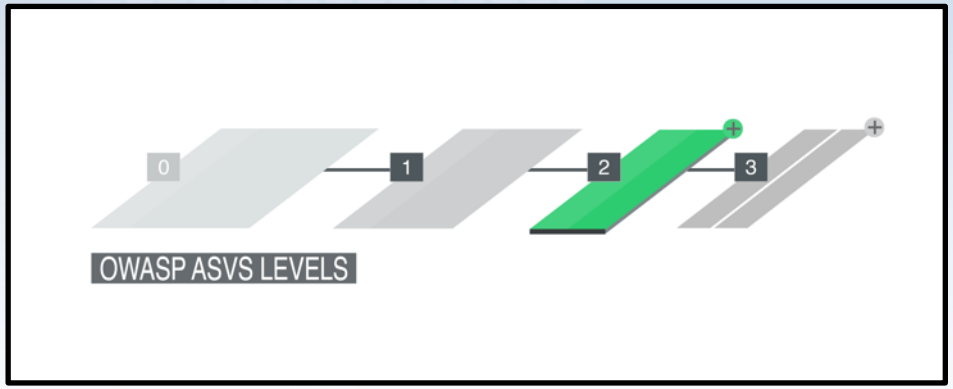
- Level 1: Baseline

- Minimum required for all apps
- Mostly fully testable
- Mostly automatable

- 82 Controls

OWASP
Open Web Application Security Project

Application Security Verification Standard 3.0



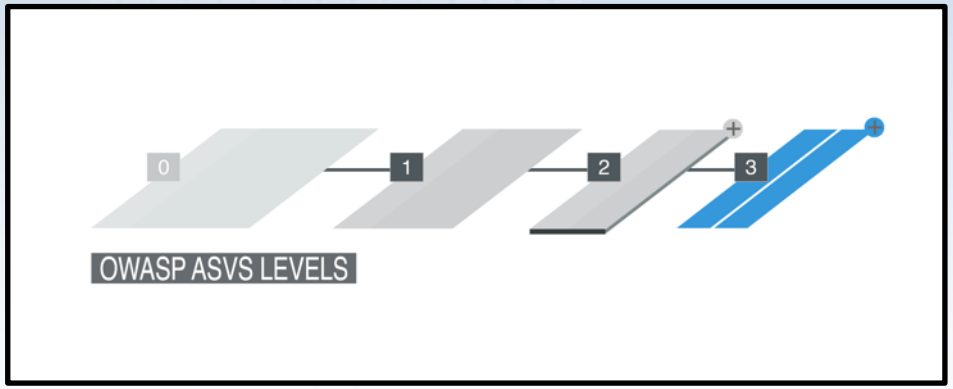
- Level 2: Standard

- Suitable for sensitive data
- About 75% testable
- Somewhat automatable

- 139 Controls

OWASP
Open Web Application Security Project

Application Security Verification Standard 3.0



- Level 3: Comprehensive

- Suitable for critical apps
- Mostly testable, but many more manual verifications required
- Not amenable to automation

- 154 Controls

OWASP
Open Web Application Security Project

- ASVS V1 Architecture
- ASVS V2 Authentication
- ASVS V3 Session Management
- ASVS V4 Access Control
- ASVS V5 Input validation and output encoding
- ASVS V7 Cryptography
- ASVS V8 Error Handling
- ASVS V9 Data Protection
- ASVS V10 Communications
- ASVS V13 Malicious Code
- ASVS V15 Business Logic Flaws
- ASVS V16 Files and Resources
- ASVS V17 Mobile
- ASVS V18 API
- ASVS V19 Configuration
- ASVS V20 Internet of Things

Security Verification Requirements

#	Description	L1	L2	L3	Since
1.1	All app components are identified and known to be needed.	✓	✓	✓	1.0
1.2	Security controls are never enforced only on the client side, but on the respective remote endpoints.		✓	✓	1.0
1.3	A high-level architecture for the application and all connected remote services has been defined and security has been addressed in that architecture.		✓	✓	1.0
1.4	Data considered sensitive in the context of the application is clearly identified.			✓	1.0
1.5	All app components are defined in terms of the business functions and/or security functions they provide.			✓	1.0
1.6	A threat model for the application and the associated remote services has been produced that identifies potential threats and countermeasures.			✓	1.0
1.7	All security controls have a centralized implementation.		✓	✓	3.0
1.8	Components are segregated from each other via a defined security control, such as network segmentation, firewall rules, or cloud based security groups.		✓	✓	3.0
1.9	A mechanism for enforcing updates of the application exists.		✓	✓	3.0
1.10	Security is addressed within all parts of the software development lifecycle.		✓	✓	3.0
1.11	all application components, libraries, modules, frameworks, platform, and operating systems are free from known vulnerabilities		✓	✓	3.0.1
1.12	There is an explicit policy for how cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced. Ideally, follow a key management standard such as NIST SP 800-57.		✓	✓	3.1

Threat Profile by Industry

Industry	Threat Profile	L1 Recommendation	L2 Recommendation	L3 Recommendation
Finance and Insurance	Although this segment will experience attempts from opportunistic attackers, it is often viewed as a high value target by motivated attackers and attacks are often financially motivated. Commonly, attackers are looking for sensitive data or account credentials that can be used to commit fraud or to benefit directly by leveraging money movement functionality built into applications. Techniques often include stolen credentials, application-level attacks, and social engineering. Some major compliance considerations include Payment Card Industry Data Security Standard (PCI DSS),Gramm Leech Bliley Act and Sarbanes-Oxley Act (SOX).	All network accessible applications.	Applications that contain sensitive information like credit card numbers, personal information, that can move limited amounts of money in limited ways. Examples include: (i) transfer money between accounts at the same institution or (ii) a slower form of money movement (e.g. ACH) with transaction limits or (iii) wire transfers with hard transfer limits within a period of time.	Applications that contain large amounts of sensitive information or that allow either rapid transfer of large sums of money (e.g. wire transfers) and/or transfer of large sums of money in the form of individual transactions or as a batch of smaller transfers.

Where can I get a copy of ASVS, and talk to people using ASVS?

- You can download a copy from the ASVS Project page:
  - http://www.owasp.org/index.php/ASVS
- You can send comments and suggestions for improvement using the project mailing list:
  - See "Mailing List/Subscribe" link on project web page.
  - Tell us how your organization is using the OWASP ASVS. Include your name, organization's name, and brief description of how you are using the ASVS

THANK YOU!

Joe Blanchard
Cyber & Application Security Lead
Allstate
joe.blanchard@allstate.com
joe.blanchard@owasp.org
Office: 618-409-8535

LinkedIn: https://www.linkedin.com/in/joe-blanchard-499bb918/
Twitter: xmoxxen

Take 10.

Grab a drink!

OWASP Chapter – St. Louis

Chapter Goals

- Commit to at least quarterly meetings
- Find stable locations for meetings
- Find great speakers!
- Publicize the chapter and recruit new members
- Keep the chapter non-commercial

Frequency & Type of Meetups

- Quarterly or Bi-Monthly
- Night of the Week (Mon, Tue, Thur)

- Speakers (Full Length, Mini Talks?)
- In Depth or High Overview
- CTF & Labs

- Study Groups/Sessions

Enhancing the committee!

- Leadership Roles
  - Chapter Lead x2
  - Venue Chair & Assistant
  - Speaker Chair & Assistant
  - Sponsor Chair & Assistant
  - Communications Chair

Appsec: Midwest 2019

- St. Louis Chapter has been invited to participate
- Seeking a volunteer(s) to service on committees
- Will receive a portion of the proceeds
- Looking to be May/June of 2019