



OWASP

Open Web Application
Security Project

OWASP ASVS

Hector Espinoza

hectorjonathanespinoza@gmail.com

Agenda

- Intro
- What is ASVS 3.0?
- Verification Levels
- PCI DSS mapping
- The “Framework”

Me

- 10+ years of experience in AppSec, Dev
- Application Security Engineer at USAA
- Freelance Pentester at ClickIT
- Chapter member Aguascalientes, Ags and San Antonio, Tx
- Favorite vulnerability: Remote Cmd Execution
- I love source code analysis 😊 AKA (LOC poisoning)



What is ASVS 3.0?

- Application Security Verification Standard
- A community-effort to establish a **framework** of **security requirements** and **controls** that focus on normalizing the functional and non-functional security controls required when designing, developing and testing modern web applications.

So?

Requirement #	Control	What defect does it prevent?	Verification Level
5.15	V5: Malicious input handling verification requirements	PXSS, RXSS, DXSS, JSONXSS, AXSS, etc	1, 2, 3
5.12	V5: Malicious input handling verification requirements	OS Command Injection	1, 2, 3
9.1	V9: Data protection verification requirements	Sensitive information stored in Local Cache	1, 2, 3



Verification Levels

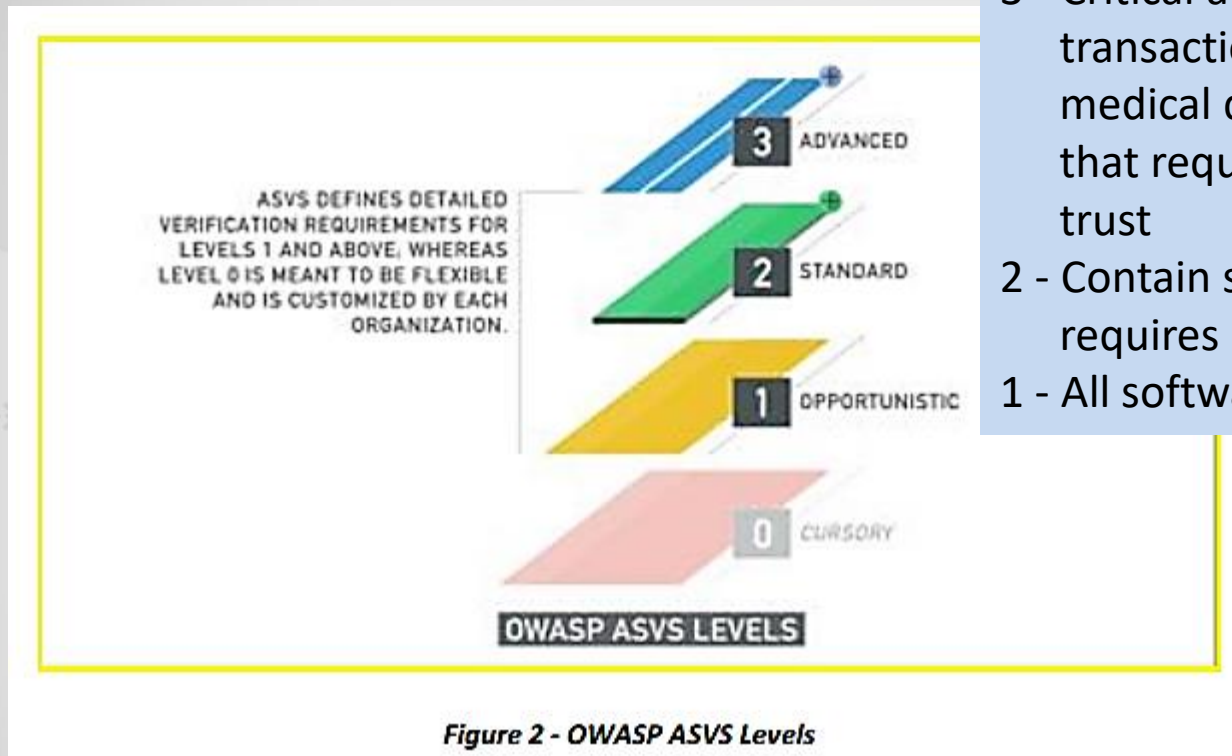


Figure 2 - OWASP ASVS Levels

- 3 - Critical applications, high value transactions, contain sensitive medical data, or any application that requires the highest level of trust
- 2 - Contain sensitive data, which requires protection
- 1 - All software

PCI DSS mapping

- PCI DSS 6.5 is derived from the OWASP Top 10 2004/2007 (with some recent process extensions).
- The ASVS is a strict superset of the OWASP Top 10 2013 (154 items to 10 items), so all of the issues covered by OWASP Top 10 and PCI DSS 6.5.x are handled by more fine grained ASVS control requirements.

The “Framework”

ASVS Home

https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Home

PDF Standard

https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf

Framework Spreadsheet

<https://www.owasp.org/images/b/b2/ASVS-excel.xlsx>



Questions?

CONNECT.

LEARN.

GROW.

Thank you!

hectorjonathanespinoza@gmail.com



OWASP
Open Web Application
Security Project