



OWASP 2022
GLOBAL
AppSec

SAN
FRANCISCO
NOV 14-18



Josh Grossman

**ASVS 5.0 – The rise of the
Security Verification Standard**

Bounce Security and ASVS project co-leader



OWASP 2022
GLOBAL
AppSec

SAN
FRANCISCO
NOV 14-18



Josh Grossman

**ASVS 5.0 - The rise of the
Security Verification Standard**

Bounce Security and ASVS project co-leader



Josh Grossman



- Over 15 years of IT and Application Security, IT Risk and development experience
- CTO for Bounce Security, value-driven Application Security support
- Consulting and training for clients internationally and locally
- Contact:



[@JoshCGrossman](https://twitter.com/JoshCGrossman)



josh@bouncesecurity.com



<https://joshcgrossman.com/>



<https://appsecg.host>

—

- OWASP Israel Chapter Board
- Co-leader of the OWASP ASVS Project
- Major Contributor to the OWASP Top Ten Proactive Controls project
- Contributor to:
 - OWASP Top 10 Risks
 - OWASP JuiceShop



Today, I will be mostly discussing...

Background to the ASVS

01

What is the OWASP ASVS?

02

What is the plan for version 5.0?

03

How are we seeing it used in industry?

04

How you can you use it and get involved?

05





SO, WHAT IS THE ASVS?

BACKGROUND

Quiz time! You tell me! (Vote with your hands)

- Who has heard of the ASVS?
- Who has used the ASVS?
- Who uses it on an ongoing basis?
- Who knows by heart what section V2 is called?
 - Authentication 😊
- Who can tell me by heart what v4.0.3–2.5.2 says?

2.5.2

Verify password hints or knowledge-based authentication (so-called "secret questions") are not present.



SO, WHAT IS THE ASVS?

BACKGROUND



~~SO, WHAT IS THE ASVS?~~

WELL FIRST, WHAT ISN'T THE ASVS

The OWASP Top 10 Risks – The Good

- Released every 3-4 years
- Led by security experts from around the world
 - Andrew van der Stock, Neil Smithline, Torsten Gigler, Brian Glas
- Public comments and conversation on 2017/2021 choices
- Frequently cited
- Application security awareness document

TOP10

The OWASP Top 10 Risks – The Less Good

- Spread awareness regarding Web Security issues.
- It is not a standard.
 - Take note, PCI-DSS and others who incorrectly list it as one.
- Not a comprehensive list
- Bringing problems, not solutions



OWASP Top Ten Proactive Controls

- Guidance document
- Developer/builder focused



Define Security Requirements

01

Leverage Security Frameworks
and Libraries

02

Secure Database Access

03

Encode and Escape Data

04

Validate All Inputs

05

Implement Digital Identity

06

Enforce Access Controls

07

Protect Data Everywhere

08

Implement Security Logging
and Monitoring

09

Handle All Errors and
Exceptions

10

Top Ten Proactive Controls – The Good

- A great starting point
- Gives practical prevention details
- Also a great team:
 - Katy Anton, Jim Manico, Jim Bird



Top Ten Proactive Controls – The Less Good

- Still not comprehensive
- Again, more for awareness
- Not organized as a standard



So, watcha gonna do?



The OWASP ASVS!





SO, WHAT IS THE ASVS?

WHAT IS THE ASVS

What is the ASVS?

- Requirements for a secure application
- Designed to be an actual standard
- Set of leading practices
- Community and practitioner driven
- Developed in the open
- Split into 3 levels of requirement



More about ASVS 4.0.3

- Not going to cover today
- See my previous talk 😊

<https://appsecg.host/asvs>





Use of the ASVS in industry

INDUSTRY

Use of the ASVS in industry

- Develop Secure Requirements
- Design Security Checklist
- Guidelines for Implementation
- Map security properties of a security mechanism
- ...
- Verification Standard

Not this verification!





Verifying the security of an App

VERIFICATION

What about our usual AppSec verification?

Penetration Testing Considered Harmful

(haroon@thinkst.com)

Penetration Testing Considered Harmful, Haroon Meer – 44CON 2011

<https://www.youtube.com/watch?v=GvX52HPAfBk>
<https://thinkst.com/resources/slides/44con-final.pdf>

What about our usual AppSec verification?



Penetration Testing Considered Harmful, Haroon Meer – 44CON 2011

<https://www.youtube.com/watch?v=GvX52HPAfBk>
<https://thinkst.com/resources/slides/44con-final.pdf>

We can do better....can we?



OWASP
AppSec USA
San Jose, CA
October 6-12, 2018

How to get the best AppSec test of your life

Josh Grossman
Comsec Global

@JoshCGrossman

ASVS 5.0 – The rise of the Security Verification Standard

Various suggestions, including:



Q: What is this "Penetration Testing Execution Standard"?

A: It is a new standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing (i.e. Security evaluations).

http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

44CON

thinkst
applied research

So, what about AppSec?



Challenges for OWASP

1. How can OWASP remain neutral?
2. How can we drive adoption of standard?
3. How do we know the tester is competent?

Case Study 1 - CREST OVS

- Defines a standard for performing application security assessments
- Based around Levels 1 and 2 of ASVS and MASVS
- Intended to result in standardized and comparable reports
- % of revenue will be donated back to OWASP
- Announced in Summer 2022



CREST OVS – Response to challenges

1. How can OWASP remain neutral?
 - OWASP defines the standards, CREST does the rest (in consultation with OWASP).
 - No exclusivity
2. How can we drive adoption of standard?
 - CREST have experience in getting assessment standards adopted in industry
3. How do we know the tester is competent?
 - CREST have experience in accrediting testers

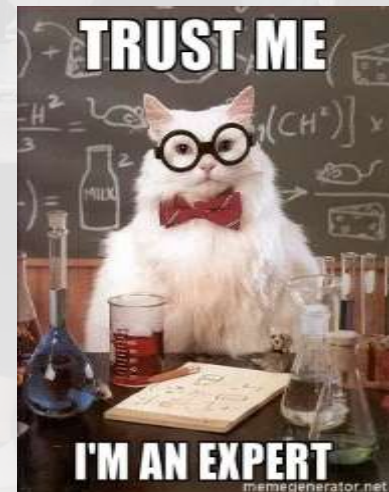


Case Study 2 – Other industry group

- Oversee a large ecosystem of applications
- Applications go through some form of ASVS/MASVS based assessment
- Type depends on application “impact”
- Needs to be scalable

Large tech company - Other industry group

1. How can OWASP remain neutral?
 - OWASP defines the standards, Industry group does the rest (in consultation with OWASP).
 - No exclusivity
2. How can we drive adoption of standard?
 - Industry members control the ecosystem
3. How do we know the tester is competent?
 - Open problem...



Other outstanding challenges

- 4. Usability of standard
- 5. Scope of standard
- 6. Scalability of standard



Other outstanding challenges

4. Usability of standard
 - We are planning release 5.0
5. Scope of standard
 - Let us know in the issues!
6. Scalability of standard
 - Open problem...



[PROJECTS](#) [CHAPTERS](#) [EVENTS](#) [ABOUT](#)

Roadmap to version 5.0 of the OWASP ASVS project

Josh Grossman

Sunday, May 15, 2022

On behalf of the [OWASP ASVS](#) leadership team, we are excited to publicise the objectives and roadmap for the upcoming version 5.0 of the flagship OWASP Application Security Project. We are hoping to be able to release a final



Key principles for 5.0

Making it easier to use by:

- Clarifying existing requirements and adding new ones based on community feedback
- Enhance explanations on the levels and reduce the barrier to entry
- Clean up mappings
- Streamline the main document



Calls to action

ACTION

1) Get ready for Verification!

- Expect ASVS/MASVS assessments based in the future
- Application Penetration Testers: Can you start structuring your testing around the *SVS?
- Application Developers: Can you structure your control documentation based on *SVS?

2) Help with version 5.0



Josh Grossman



Jim Manico



Elar Lang



Daniel Cuthbert



**Andrew Van
der Stock**

But we need you too!!!

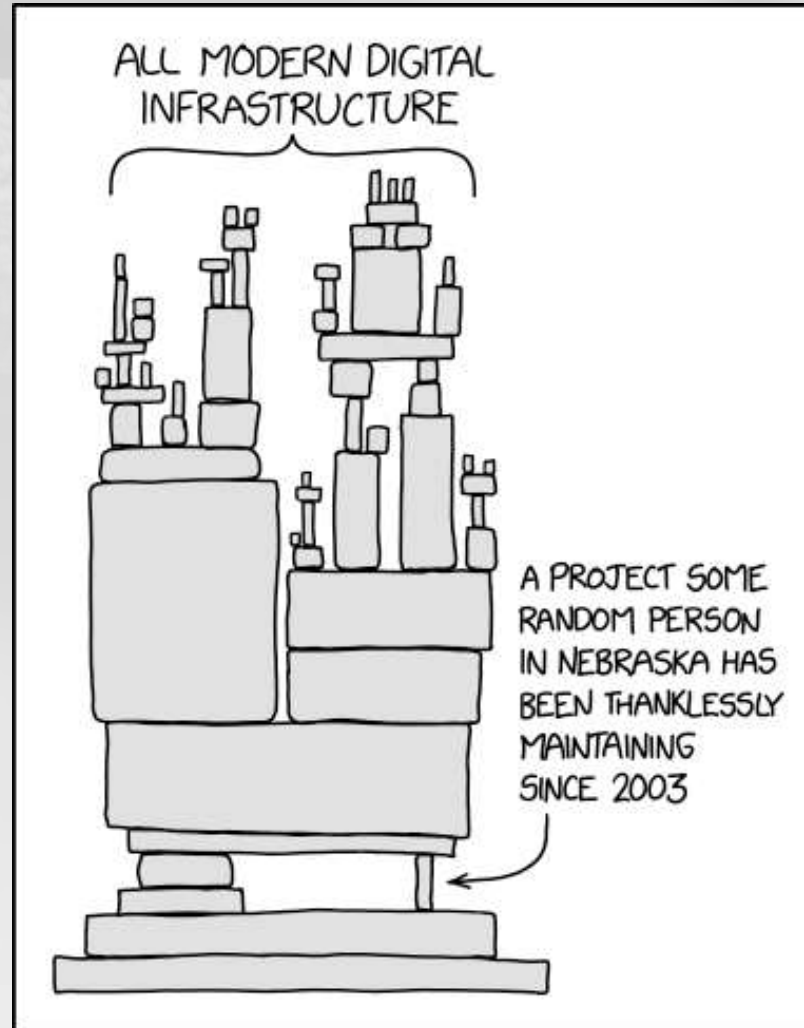
2) Help with version 5.0

- Submit issues/change suggestions
- Submit general feedback
- Comment on other people's issues

<https://github.com/OWASP/ASVS/issues>

<https://github.com/OWASP/ASVS/blob/master/CONTRIBUTING.md>

3) Support the standard



3) Support the standard

Thanks to our supporters!

Maintaining Supporters (through time provision)


Organizations who have allowed contributors to spend significant time working on the standard as part of their working day with the organization. This will be evaluated at the sole discretion of the project leaders. Supporter will be listed 2 years from the end of the time provision.





Primary supporters

Organizations who have donated \$7,000 or more to the project via OWASP. Supporter will be listed in this section for 3 years from the date of the donation.




Secondary supporters

Organizations who have donated \$3,000 or more to the project via OWASP. Supporter will be listed in this section for 2 years from the date of the donation.



Tertiary supporters

Organizations who have donated \$500 or more to the project via OWASP. Supporter will be listed in this section for 1 year from the date of the donation.



Associate supporters

Organizations who have donated another amount to the project via OWASP. Supporter will be listed in this section for 1 year from the date of the donation.

3) Support the standard

**GIVING
TUESDAY**

Donate to the OWASP Foundation

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects and hundreds of local chapters worldwide, your gift* will support the Foundation and its many activities around the world to secure the web. Existing donors can [Modify Recurring Gifts](#).

Amount of your Gift

USD \$

EUR €

GBP £

\$10

\$25

\$50

\$100

\$500

\$ 10,000

Summary

- Get ready for Verification!
- Help with version 5.0
- Support the standard

Whilst I have you...

Whilst I have you...



OWASP
AppSec Israel 2023

We're Back!

Tel Aviv, May 2023

Tell your friends! Tell your employers!

<https://appsecil.org/> @OWASP_IL



THANK YOU!

Any Questions?

Thanks to Michal Kamensky for help with the slides

Josh Grossman

✉ josh.grossman@owasp.org

✉ josh@bouncesecurity.com

🐦 [@JoshCGrossman](https://twitter.com/JoshCGrossman)



ASVS Project

🐦 [@OWASP_ASVS](https://twitter.com/OWASP_ASVS)

🐱 <https://github.com/OWASP/ASVS>

🌈 <https://owasp.slack.com, #project-asvs>

🌐 <https://owasp.org/asvs>

