Application Security Verification Standard 4.0

Andrew van der Stock, co-leader ASVS Project

March 2019 - NullCon

Andrew van der Stock

- Senior Principal Consultant, Synopsys
  - Technical Leader of Managed Services

- Joined OWASP late ~2002
  - Lifetime OWASP member
  - Board Member (2015-2018) and Treasurer (2016-2018)

- Selected works:
  - Application Security Verification Standard
  - OWASP Top 10 {2007, 2017}
  - OWASP Developer Guide 2.0

What is the ASVS?

- Started as 80/20 checklist
- Designed to be an actual application security standard
- Set of leading practices – even 2.0 was challenging for many
- Community and Industry Driven

- Completely developed in the open at GitHub
    - Submit issues! Submit PRs! Translate please!

Who is involved?

- You

- Andrew van der Stock, Daniel Cuthbert, Jim Manico
- Josh Grossman, Mark Burnett, Abhay Bhargarv
- Amazing reviewers such as Elar Lang, ossie-git, Ron Perris, Tonimir Kisasondi, Serg Belokamen, Jason Axley, and Adam Caudill

So what’s new?

What’s new

- Now completely written in Markdown
    - Uses MASVS script and CSV generation
    - Easy to translate
    - Easy to determine what changed, when, by whom, and why
- NIST 800-63 compliance
- Data Protection has been upped to be primarily about human sensitive personal identifying information
    - Helps with GDPR and APPs
- IoT ASVS Preview Chapter

Modern web applications

- Full support for server-less, responsive applications
- Containers
- API
- DOM
- Templating

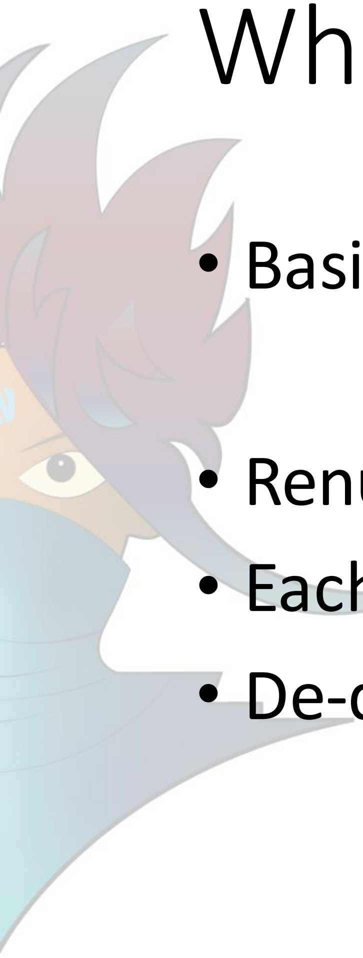
CWE all the things

- Most requested feature for the last decade finally delivered

- Let’s talk about CWE for a minute
  - ASVS is a control based standard
  - Weaknesses are not controls
  - CWE is an imperfect mapping, but it’s the mapping we have

- Not every item ended up with a CWE. CWE needs our help

What’s changed



- Basically everything

- Renumbered completely
- Each section is reorganized and re-ordered
- De-duped. Do not omit any section for your level

L1 is the new minimum

- OWASP Top 10 2017 is simply not sufficient

- Level 1 is now completely testable using pentest techniques
- It’s the only level that is completely penetration testable

- Stop penetration testing. Hybrid reviews at least!

PCI DSS 6.5.x

- Yep

- We even included buffer overflows, integer and safer string operations, as well as ensuring that folks compiled code properly!

What’s gone

- Less impactful controls
- Controls that were implemented by one browser or language
- “Since”

- Mobile Chapter (use MASVS)
- IoT Chapter (use IoT Project)

Detailed Changes

Architecture

- Completely new

- Replaces “dead” section with something that can produce secure by default software
- Design and build security in!

- Level 2 and 3 only

Authentication and NIST 800-63

- Completely aligned with NIST 800-63
  - Except that we had to go to 12 characters for SFA passwords
- Credentials construction and protection (including credential stuffing)
- Credential lifecycle from issuance to retirement
- Multi-factor is now expected, crypto devices, web services
- JWT, Oauth, federated security
- Advanced session management attacks
  - Half open attack

Validation, Sanitization, and Encoding

- Major revamp
- Divided into easy to consume sections
  - Standardized Input and Output Pipelines
  - Input validation for modern applications and APIs
  - Output encoding is the new hotness
  - Injection prevention (including XXE and XML attacks)
  - SSRF
  - Deserialization

Communications Security

- Now DevSecOps friendly
  - No more building a secure chain / path … what does that even mean?

- Easier to comply … automatically
- TLS all the things
- Use modern configuration builders
- Use the verification tools you use today

Malicious Code

- Major update to this section to cover more than just time bombs and Easter eggs
  - Detect malicious code introduction
  - Continuous detection through building
  - Privacy invading libraries (Google’s PUA) mentioned for first time
  - Malicious business logic, such as salami attacks
  - Privacy invading permissions (camera, location, microphone, contacts, etc)

- Mostly Level 3 for apps that can kill you or run the world economy

Business Logic Verification

- Major update
  - Business logic step order
  - Business logic human time
  - Business logic limits
  - Business logic anti-automation
  - Threat model (attack driven design) business logic risks
  - TOCTOU Race conditions that might affect business logic
  - Monitoring, alerting, and detection of unusual business logic events

Files and Resources

- Major revamp
  - Architecture items moved to architecture
  - Configuration items moved to configuration
- Upload - Size and number
- Contents and integrity
- Storage, including malicious file detection
- Execution, including LFI, RFI, and SSRF
- Download

API Security

- Total revamp
- General controls include common sense API controls
  - Must be read in conjunction with authentication, authorization and session management
- RESTful includes schema validation, CORS and origin attacks
- SOAP – fewer more impactful items, far clearer, and not obfuscated
- GraphQL and Web Service Data Layer

Configuration

- Major revamp
- Repeatable, Continuous integration, continuous deployment
- Support for DevSecOps culture and agile practices
- Containers
- Dependency checks mandated
- Sandboxing components including uploaded assets
- Sub-domain takeover

I’m in. How do I use it?

Generally Accepted Security Practices

Secure code review

Security architecture

Integration testing

Peer coding checklists

Developer training

Unit testing

Hybrid reviews

DevSecOps automation

Vulnerability programs

Consultant training

Tool Benchmark

Secure coding checklist

Deployment checklist

Penetration test

Functional constraints

Planning Sprint Assistance

Non-functional and functional features

Supplier Benchmarking

How do I use it?

- Use it as is or fork it

- Level 1 – entry level, penetration testing
- Level 2 – most apps
- Level 3 – apps that can kill you or run the world economy

- Deep standards have no bounds

When can I get it?

- The ASVS 4.0 Final will be released at nullcon on March 1

- GitHub – Development
- OWASP Wiki – Word, PDFs, CSVs, and Hot Linkable markdown

What’s next?

- 4.0 is a complete revamp, so likely to have a few issues at least
  - Minor 0.0.1 updates will address critical issues as necessary
- 4.1 will come in 9-12 months or so to address larger changes
  - OWASP Top 10 2020?
  - OWASP MASVS
  - OWASP IoT
  - OWASP Testing Guide

How to get involved

- Grab a copy today and start to migrate from earlier versions and T10
- If it’s not a good fit for you, fork it, and make it your own
- We need case studies! If you use ASVS, we’d love to hear from you!

- Create issues (4.0.x) or PRs (4.1) if you identify issues
- We need translations. Please join the #asvs channel on OWASP Slack

Thank you

vanderaj@owasp.org (ASVS) | vander@synopsys.com ($dayjob)

@vanderaj