OWASP ASVS (APPLICATION SECURITY VERIFICATION STANDARD) TRAINING

Level - OWASP

Email – contact@DevOpsSchool.com

TRAINING AGENDA

DAY 1

Introduction to OWASP ASVS

- Overview of OWASP and the ASVS project
- Why ASVS matters in modern application security
- ASVS vs OWASP Top 10 vs SAMM
- Real-world use cases of ASVS in SDLC

Understanding ASVS Structure & Verification Levels

- ASVS architecture and control categories
- Verification Levels:
    - Level 1 (Basic Security)
    - Level 2 (Standard Security)
    - Level 3 (Advanced / High-Risk Applications)

- Mapping ASVS levels to application risk profiles

Secure Architecture & Design (V1)

- Secure design principles
- Threat modeling and trust boundaries
- Secure component and dependency selection
- Security requirements in design reviews

Authentication, Identity & Session Management (V2 & V3)

- Secure authentication mechanisms
- Password policies and MFA requirements
- Session handling, cookies, and token security
- Common implementation mistakes

Access Control & Authorization (V4)

- Role-based and attribute-based access control
- Preventing broken access control
- Server-side enforcement best practices
- Testing authorization logic

DAY 2

Input Validation, Output Encoding & Injection Prevention (V5)

- Preventing SQL, NoSQL, OS command injection
- Secure input handling strategies
- Output encoding and escaping techniques

- Validation patterns and anti-patterns

Cryptography, Data Protection & Privacy (V6)

- Secure storage of sensitive data
- Encryption at rest and in transit
- Key management best practices
- Common cryptographic failures

Error Handling, Logging & Monitoring (V7)

- Secure error handling techniques
- Logging security events correctly
- Avoiding sensitive data leakage in logs
- Monitoring and alerting integration

API & Web Services Security (V8 & V9)

- Applying ASVS to REST & GraphQL APIs
- Secure API authentication & authorization
- Rate limiting and abuse prevention
- Mapping ASVS to OWASP API Security Top 10

Security Configuration, Files & Business Logic (V10–V14)

- Secure configuration management
- File upload/download security
- Business logic abuse prevention
- Protecting against misconfiguration

ASVS Testing, Compliance & Automation

- How to use ASVS as a testing checklist

- Manual vs automated ASVS verification
- Mapping ASVS to SAST, DAST, and IAST tools
- Security testing workflows

ASVS in DevSecOps & Real-World Implementation

- Integrating ASVS into CI/CD pipelines
- Using ASVS for secure SDLC governance
- ASVS compliance reporting
- Case studies and implementation roadmap

Final Wrap-Up & Next Steps

- Key takeaways and best practices
- ASVS adoption checklist
- Recommended tools and references
- Q&A and discussion