INTEGRAÇÃO DE MODELOS OWASP: UMA ABORDAGEM COMPLEMENTAR PARA SEGURANÇA NO DESENVOLVIMENTO DE SOFTWARE

Sara Rayna Gibmaier Scheffer[1], Fabiano de Oliveira Wonzoski[2]

1. Discente do curso de gradução Bacharelado em Ciência da Computação, Unoesc, Videira, SC
2. Docente do curso de gradução Bacharelado em Ciência da Computação, Unoesc, Videira, SC

Autor correspondente: Sara Rayna Gibmaier Scheffer, saragibmaier@gmail.com

Área: Ciências Exatas e Tecnológicas

Introdução: A segurança no desenvolvimento de software consolidou-se como uma preocupação central diante da crescente sofisticação das vulnerabilidades exploradas em ambientes corporativos. Nesse contexto, três frameworks da OWASP apresentam abordagens complementares. O OWASP Top 10 (2021) atua como guia normativo e de conscientização, classificando riscos críticos, mas carece de direcionamentos técnicos de mitigação. O ASVS 4.0.3 (2021), por sua vez, fornece requisitos verificáveis organizados por níveis de criticidade, permitindo validações técnicas detalhadas. Já o SAMM 2.0 (2020) estrutura a maturidade organizacional em domínios como governança, verificação e construção, orientando a evolução de processos. A integração dessas três perspectivas oferece um caminho mais abrangente para institucionalizar a segurança no ciclo de vida do software. **Objetivo:** O estudo buscou comprovar a eficácia da utilização combinada dos frameworks OWASP Top 10, ASVS e SAMM, como estratégia de fortalecimento da segurança em todas as etapas de desenvolvimento. **Método:** Foi conduzida pesquisa qualitativa, exploratória e descritiva, com base em análise documental comparativa. Foram examinadas versões oficiais dos três frameworks, analisando quatro critérios principais: foco, estrutura, aplicabilidade e desafios. A metodologia envolveu catalogação das características centrais de cada modelo e posterior cruzamento dos dados em matriz comparativa, permitindo identificar sobreposições, lacunas e complementaridades. **Resultados:** A análise revelou que o OWASP Top 10 desempenha papel de sensibilização inicial, mas apresenta limitações técnicas. O ASVS, em contrapartida, detalha requisitos robustos de segurança, ainda que demande maior esforço de implementação. O SAMM atua em nível organizacional, oferecendo orientações para melhoria contínua, mas requer maturidade processual prévia. Verificou-se que, isoladamente, cada modelo deixa lacunas: o Top 10 não traz requisitos verificáveis, o ASVS não cobre gestão de processos e o SAMM não detalha vulnerabilidades técnicas. Entretanto, a integração entre eles cobre essas deficiências, resultando em um ciclo completo: diagnóstico, verificação técnica e evolução organizacional. A análise estatística demonstrou que cerca de 70% das vulnerabilidades do OWASP Top 10 possuem cobertura direta por requisitos do ASVS, evidenciando alinhamento técnico significativo. Identificou-se ainda que a implementação dos níveis básicos do ASVS pode aumentar em 10% a 15% o tempo dedicado à fase de QA, enquanto os níveis avançados elevam esse esforço entre 25% e 40%. No caso do SAMM, a busca por maturidade organizacional mais elevada implica em overhead inicial de aproximadamente 20% no tempo de projeto, compensado posteriormente pela redução de retrabalho em segurança. **Conclusão:** O estudo demonstrou que a integração entre OWASP Top 10, ASVS e SAMM configura uma abordagem progressiva e complementar, capaz de fortalecer a segurança desde a conscientização até a gestão da maturidade organizacional. A análise confirmou que a combinação promove não apenas cobertura técnica das vulnerabilidades, mas também sustentação processual contínua, especialmente relevante para organizações que desejam institucionalizar práticas de desenvolvimento seguro. Recomenda-se que pesquisas futuras explorem estudos de caso práticos e ferramentas de automação que apoiem essa integração.

Palavras-chave: OWASP; Desenvolvimento de software; Segurança; Integração.