Testes de Segurança Estáticos na Esteira de Desenvolvimento de Aplicações: Um Estudo de Caso na SEPLAG-CE

Francisco R. M. Campos[1], Leonardo O. Silva[1], João G. L. O. Batista[1], Igor M. Benevides[1], Rafael L. Gomes[2], Emanuel B. Rodrigues[1], Rossana M. C. Andrade[1], Daniel C. Bentes[3], Alexandre S. Cialdini[3]

[1]Universidade Federal do Ceará (UFC), Fortaleza, Ceará, Brasil.

{ramonmartins,leonardosilva_99,joaoguibatista,igormbenevides}@alu.ufc.br

{emanuel,rossana}@dc.ufc.br

[2]Universidade Estadual do Ceará (UECE), Fortaleza, Ceará, Brasil.

rafa.lopes@uece.br

[3]Secretaria do Planejamento e Gestão do Ceará (SEPLAG), Fortaleza, Ceará, Brasil.

{daniel.bentes,alexandre.cialdini}@seplag.ce.gov.br

1. Introdução

Nas instituições públicas, tais como a Secretaria do Planejamento e Gestão do Ceará (SEPLAG)[1], o uso de técnicas de *Static Application Security Testing* (SAST) desempenham um papel estratégico, pois os sistemas governamentais costumam armazenar informações críticas da população (tais como dados pessoais, fiscais, judiciais e de saúde), cuja exposição indevida pode gerar consequências graves para a sociedade e para a administração pública. Diante deste contexto, este trabalho apresenta uma análise de segurança de aplicações utilizando técnicas SAST na infraestrutura da SEPLAG, com o objetivo de identificar vulnerabilidades no código-fonte de sistemas prioritários indicados pela equipe da instituição, possibilitando uma análise abrangente dos riscos de segurança cibernética que poderiam ser explorados por agentes mal-intencionados.

2. Metodologia

Para classificação das vulnerabilidades encontradas, foram utilizadas duas listas: *Common Vulnerabilities and Exposures* (CVE)[2] e *Common Weakness Enumeration* (CWE)[3]. Cada vulnerabilidade tem uma pontuação de severidade calculada pelo *Common Vulnerability Scoring System* (CVSS), que varia de 0,1 a 10,0 [FIRST 2019]. As seguintes ferramentas SAST foram usadas: (1) Dependency Check[4], que detecta vulnerabilidades divulgadas publicamente em dependências de projetos; (2) Trivy[5], um scanner para vulnerabilidades em contêineres, repositórios de código e pacotes; (3) Semgrep[6], uma ferramenta de análise estática e personalizável para várias linguagens. Estas ferramentas exibem resultados de

[1]https://www.seplag.ce.gov.br
[2]https://cve.mitre.org
[3]https://cwe.mitre.org
[4]https://github.com/dependency-check/DependencyCheck
[5]https://github.com/aquasecurity/trivy
[6]https://github.com/semgrep/semgrep

CVEs e CWEs detalhados e padronizados, possuindo a capacidade de integração com esteiras de *Continuous Integration and Continuous Delivery/Deployment* (CI/CD).

3. Resultados e Discussão

Como pode ser visto na Tabela 1, foi encontrado um total de 8 vulnerabilidades durante a análise SAST realizada no repositório de código, com a seguinte distribuição de severidades (calculadas usando o CVSS): 1 alta (CVSS entre 7, 0 e 8, 9), 6 moderadas (entre 4, 0 e 6, 9) e 1 baixa (entre 0, 1 e 3, 9). Nota-se que a maioria das vulnerabilidades encontradas possuem um grau de explorabilidade menor do que 5,0, evidenciando uma pequena probabilidade de um ataque malicioso. Entretanto, metade das vulnerabilidades possuem impacto maior do que 6,0, com destaque para a vulnerabilidade CWE-200 que tem impacto máximo na aplicação, pois está relacionada à exposição de informações confidenciais a um ator não autorizado. Esses resultados demonstram a importância da esteira de CI/CD com SAST aplicado, possibilitando a descoberta e correção de vulnerabilidades.

Tabela 1. Níveis de severidade, explorabilidade e impacto das vulnerabilidades

Common Weakness Enumeration (CWE)	Severidade	Explorabilidade	Impacto
CWE-200: Exposição de informações confidenciais a um ator não autorizado	7,5	5,0	10,0
CWE-863: Autorização incorreta	6,8	6,7	6,9
CWE-321: Uso de chave criptográfica no código-fonte	6,4	4,8	8,0
CWE-35: Path traversal	6,3	5,6	7,0
CWE-732: Atribuição incorreta de permissão para recurso crítico (2 vulnerabilidades encontradas)	4,2	3,4	5,0
CWE-209: Geração de mensagem de erro contendo informações sensíveis	4,2	3,4	5,0
CWE-358: Verificação de segurança mal implementada para padrão estabelecido	2,0	2,0	2,0

A partir dos resultados apresentados, percebe-se que a aplicação das técnicas SAST na esteira de CI/CD possibilitou uma automatização da análise de segurança de forma viável (~4 minutos) e a identificação de vulnerabilidades concretas, reforçando a importância da adoção de práticas contínuas de segurança no SSDLC, promovendo uma cultura preventiva e sustentável de proteção dos ativos digitais do setor público. Além disso, a aplicação da esteira de CI/CD com SAST se alinha diretamente às boas práticas internacionais de segurança ao incorporar mecanismos automatizados e contínuos de identificação e mitigação de vulnerabilidades ao longo do ciclo de desenvolvimento.

Agradecimentos

Os autores agradecem ao CNPq (Processos 306362/2021-0 e 303877/2021-9) e à FUNCAP/SEPLAG, através do programa Cientista Chefe no projeto ”Testes de Vulnerabilidades e Monitoramento de Segurança Cibernética nos Sistemas Computacionais e Redes de Computadores da SEPLAG”, pelo apoio financeiro.

Referências

FIRST (2019). Forum of Incident Response and Security Teams - Common Vulnerability Scoring System v3.1: Specification Document. Acessado em: 14 de agosto de 2025.