T1309

VALIDAÇÃO DE INJETOR DE FALHAS E DE METODOLOGIA PARA ANÁLISE DE VULNERABILIDADES EM APLICAÇÕES WEB

Felipe Favaro Müller (Bolsista PIBIC/CNPq) e Profa. Dra. Regina Lúcia de Oliveira Moraes (Orientadora), Faculdade de Tecnologia - FT, UNICAMP

Falhas nas aplicações de software podem ser a causa de vulnerabilidades de segurança que podem ser exploradas por usuários externos para invadir o sistema. Se o invasor tiver sucesso, a organização responsável poderá ser exposta a danos econômicos e de credibilidade. O objetivo deste trabalho é complementar uma ferramenta injetora de falhas de software, a JSWFIT, resultado de um projeto prévio desenvolvido pelo grupo de teste da FT. A ferramenta altera o *bytecode* java para emular falhas realistas de software. Um novo operador de falhas foi integrado à ferramenta e a validação da nova versão foi feita através de teste por injeção de falhas. Um scanner de vulnerabilidade foi utilizado e três aplicações *Web* foram escolhidas para os testes. Primeiramente, as aplicações originais (sem falhas artificiais) foram submetidas ao scanner e as vulnerabilidades existentes foram registradas. Depois, falhas foram injetadas utilizando a JSWFIT e as aplicações foram novamente submetidas ao scanner. Se uma nova vulnerabilidade foi acusada, um mapeamento dessa falha e do contexto da aplicação aos tipos de vulnerabilidades observadas foi registrado. Também o scanner foi avaliado. Os resultados mostraram que a JSWFIT foi eficaz na injeção das falhas e que o scanner apresentou baixa cobertura e alta taxa de falsos positivos.

Metodologia - Análise - Vulnerabilidades