VALIDAÇÃO E ESCALABILIDADE DE METODOLOGIA PARA ANÁLISE DE VULNERABILIDADES EM APLICAÇÕES *WEB*

Autor: Guilherme Castillo Quattrer
Orientadora: Regina L. O. Moraes
Faculdade de Tecnologia - FT/UNICAMP

INTRODUÇÃO

A grande da maioria das atividades modernas utiliza aplicações computacionais, tais como, atividades comerciais e sistemas bancários. Algumas destas aplicações não podem apresentar resultados divergentes dos esperados, ou seja, defeitos, pois podem acarretar grandes perdas financeiras, materiais e humanas.

Uma abordagem que tem se mostrado bastante eficiente para validar sistemas que exigem segurança no funcionamento (*dependability* em inglês) é o uso de Injeção de Falhas. Injeção de Falhas é uma técnica de validação de sistemas, em que se procura produzir ou emular a presença de falhas e se observa o sistema sob teste para se verificar qual será sua resposta nessas condições.

OBJETIVO

O objetivo deste projeto é complementar e validar as ferramentas J-SWFIT [1] e J-ATTACK [2], que são, respectivamente, uma ferramenta de injeção de falhas e uma ferramenta de injeção de ataques para aplicações *Web*. A J-ATTACK injeta os ataques que estão entre os 10 mais frequentes, segundo a OWASP [3]. Além disso, foi avaliada a eficácia de scanners comerciais quando falhas foram injetadas e vulnerabilidades foram abertas em função das falhas injetadas. Verificou-se que os scanners apresentaram baixa cobertura e alta taxa de falsos positivos.

ABORDAGEM

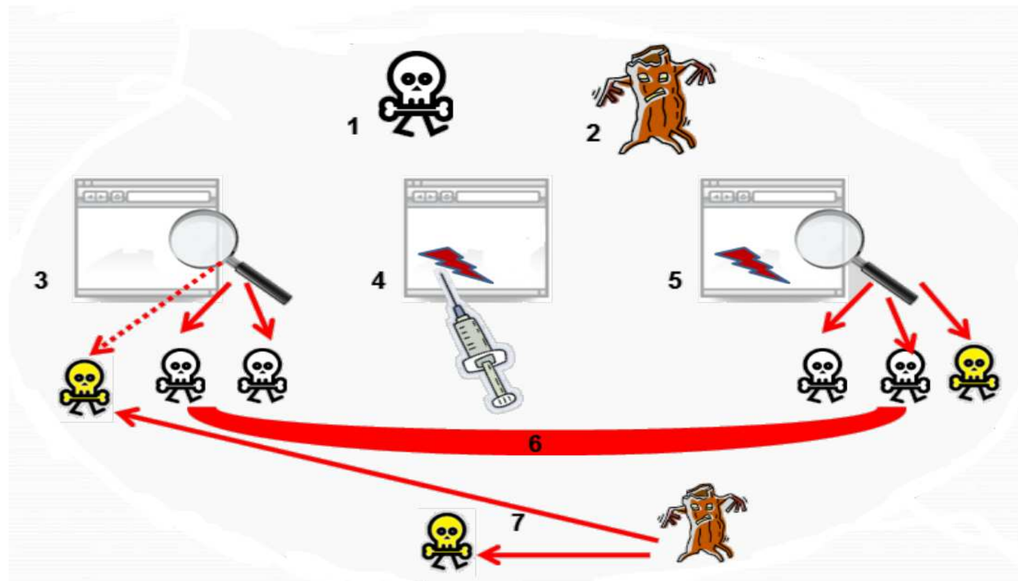

Figura 1: Abordagem para Análise de *Scanners* de Vulnerabilidade[4]

Primeiramente, é feito um *scan* para localizar as vulnerabilidades existentes na aplicação. Uma falha é injetada na aplicação, utilizando-se a J-SWFIT e um novo *scan* é realizado. Caso novas vulnerabilidades sejam detectadas, um ataque é emulado com base nas árvores de ataque e injetado na aplicação utilizando-se a J-ATTACK. Se o ataque tiver sucesso, a nova vulnerabilidade é confirmada e o ataque é repetido sobre a aplicação original. Se o ataque for confirmado também na aplicação original, uma falha de cobertura é registrada.

BIBLIOGRAFIA

[1] SANCHES B., BASSO, T., MORAES, R. “J-SWFIT: A Software Fault Injection Tool”. IN: Proc. of The Fifth Latin-American Symposium on Dependable Computing – LADC, 2011.

[2] FERNANDES, P.C.S. ; BASSO, T. ; MORAES, R. . J-Attack - Injetor de Ataques para Avaliação de Segurança de Aplicações Web. In: Workshop de Testes e Tolerância a Falhas, 2011, Campo Grande - MT. Proceedings of WTF 2011, 2011.

[3] OWASP – “The Free and Open Application Security Community”. Disponível em http://www.owasp.org/index.php/Main_Page. Ultimo acesso, Setembro/2012.

[4] BASSO, T :Uma abordagem para avaliação da eficácia de *scanners* de vulnerabilidades em aplicações web. Dissertação e Apresentação de Mestrado, 2010.