Reto
Lippuner

Marcel
Wirth

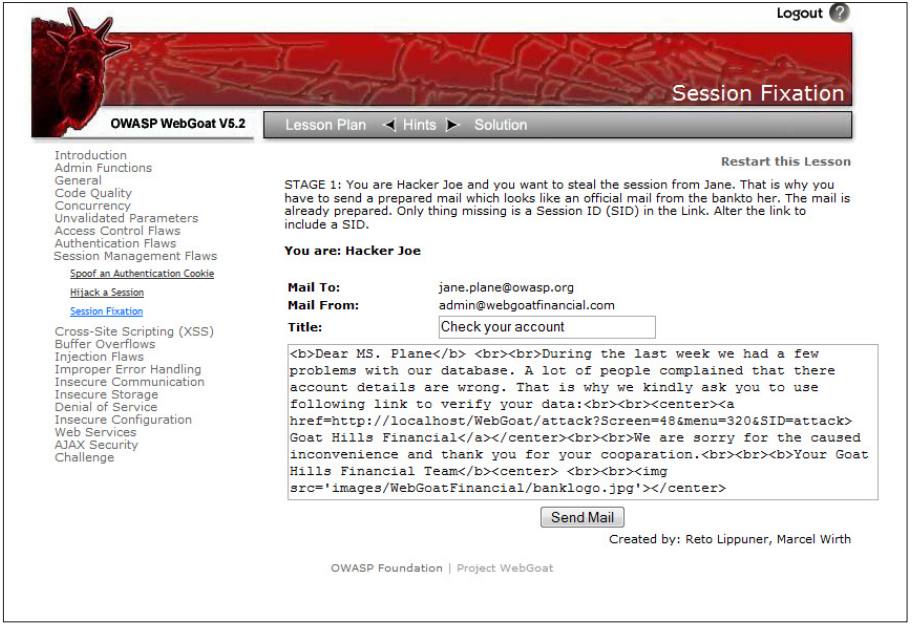
Web Application Security

Diplomanden	Reto Lippuner, Marcel Wirth
Examinator	Prof. Dr. Peter Heinzmann
Experte	Dr. Paul Schöbi, cnlab AG, Rapperswil-Jona SG
Themengebiet	Sicherheit
Projektpartner	cnlab AG, Rapperswil-Jona SG

Auswirkungen von Schwachstellen

Das Open Web Application Security Project (OWASP) hat sich zum Ziel gesetzt, solche Fälle zu vermeiden, indem man Applikationsentwicklern typische Verletzlichkeiten von Webapplikationen näherbringt. Zu diesem Zweck wurde die Lernsoftware WebGoat entwickelt. WebGoat simuliert typische Fehler von Webapplikationen. In über 60 Lektionen kann jedermann Angriffe durchführen und analysieren. So macht man sich mit typischen Angriffen vertraut und lernt Verletzlichkeiten vermeiden. Allerdings wurde die Weiterentwicklung von WebGoat stark vernachlässigt. Unvollständiger oder falscher Inhalt sowie viele Programmierfehler verunmöglichen ein effizientes Abarbeiten der Lektionen.

Ziel dieser Diplomarbeit war es, WebGoat wesentlich zu verbessern und zu erweitern. Dazu galt es zuerst die aktuell relevanten Schwachstellen von Webapplikationen zu identifizieren und die vorhandenen WebGoat-Lektionen im Detail zu studieren und auf Fehler und Unvollständigkeiten zu überprüfen. Im Rahmen der Diplomarbeit musste mehr als die Hälfte der bestehenden WebGoat-Lektionen wesentlich überarbeitet werden. Etwa 40 wesentliche Unzulänglichkeiten



WebGaot in Aktion

von WebGoat wurden behoben. Die vorhandenen Lektionen wurden mit zusätzlichen Erklärungen und Musterlösungen ergänzt. Das Userinterface wurde vereinfacht und intuitiver gestaltet. Die neu erstellte «Introduction Sektion» dürfte dem Neuling den Einstieg in WebGoat wesentlich erleichtern. Zu neu aufgetauchten Verletzlichkeiten bzw. Fehlern von WebApplikationen wurden neue Lektionen erstellt. Es sind dies Lektionen zu den Themen Session Fixation, Multi-Level-Login-Fehler, Insecure Communication und Passwortstärken.

Der WebGoat-Projektleiter Bruce Mayhew hat die im Rahmen dieser Diplomarbeit entstandenen Änderungen in den Hauptentwicklungszweig eingespeist. Somit sollten in der nächsten Version von WebGoat die in dieser Diplomarbeit erarbeiteten Änderungen der gesamten «WebGoat-Community» zur Verfügung stehen.