ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

TIK Institut für Technische Informatik und Kommunikationsnetze

Sommersemester 2005

Semesterarbeit

von

Matthias Keller

Tutor: Stefan Frei
Co-Tutor: Thomas Dübendorfer

Ausgabe: April 2005
Abgabe: November 2005

# Beurteilung: Web Attack Showcases for the Security Demo Lab

## 1 Kenntnisse und Fähigkeiten

Der Student hat seine PHP- und SQL-Kenntnisse zur Web- und Datenbank-Programmierung unter Linux und Windows gefestigt und vertieft.

Die Arbeit sowie zwei Laboraufgaben zu SQL-Injection und Crosssite-Scripting (XSS) wurden mit WinWord auf Englisch dokumentiert.

## 2 Systematik und Wissenschaftlichkeit

Die Herangehensweise des Studenten war so, dass die Implementierung stets im Zentrum stand. Verwandte Arbeiten wurden wenig beachtet und wenn, dann nur sehr oberflächlich analysiert. Beispielsweise wurden nur je eine stattgefundene Attacke zu SQL-injection bzw. XSS erwähnt, obwohl beim CERT Dutzende betroffene Programme aufgelistet sind.

Ein Design wurde erst auf Nachdruck der Betreuer erstellt und auch erst nachdem wesentliche Teile bereits implementiert waren. Auf das Erreichen bzw. eine Validierung der gesetzten Designziele (in der Aufgabenstellung aufgeführt) wurde nicht eingegangen. Alternative Lösungswege oder -ansätze (wie z.B. eine online Bank statt einem Message Board) wurden keine aufgezeigt oder diskutiert in der Dokumentation.

Wissenschaftlich brachte die Arbeit keine neuen Erkenntnisse, da sie sich auf Software Engineering Beiträge beschränkte.

## 3 Eigeninitiative und Einsatz

Der Student programmierte sehr selbständig, da er viel Erfahrung in der Webprogrammierung bereits mitbrachte. Die Kommunikation und Arbeit der Betreuer mit dem Studenten gestaltete sich schwierig. Zum einen wurden vom

Studenten gesetzte Milestones mehrfach kurzfristig eigenmächtig verschoben durch ihn und zum anderen waren teilweise die Antwortzeiten mehrmals ungwewöhnlich lange.

Da es keine eigentliche Designphase gab, konnten die Betreuer auch erst relativ spät in der Impementierungsphase noch Design-Ideen anbringen.

Der Student brachte eigene Ideen ein bezüglich einer eleganten Log-Einblendung und dem einfachem Setzen von Programm-Optionen im laufenden Betrieb.

# 4 Qualität der Ergebnisse

Die angestrebten Kernziele eines Web Attack Showcases wurden erreicht. Eine Validierung des Codes und der Installations- und User Manual-Dokumentation im praktischen Einsatz oder mit Testbenutzern wäre sinnvoll gewesen. Die Beschreibung der Showcases *Cross-Site Scripting* und *SQL-Injection* beschränkt sich auf die trivialsten Beispiele dieser Angriffe. Hinweise zu vortgeschritteneren Techniken dieser Angriffsklassen wäre angebracht gewesen da man gerade diese in einem Testbed wie dem MSDL effektiv behandeln könnte.

Die Implementierung der Applikation (PHP Scripts, Database Scripts, Installationsscript) ist unvollständig und ungetestet abgegeben worden. Die Datenbankscripts, Installscripts und -hinweise waren bei Abgabe unvollständig und mussten nachgebessert werden. Die Dokumentation zur Installation war ungenügend (keine System-Requirements/Voraussetzungen deklariert, verwirrender oder kein logische Aufbau) und wurde durch Beigabe einer *readme*-Datei nachgebessert. Die Unterstützung von MS SQL (statt nur MySQL) wurden zwar umgesetzt, aber nicht getestet.
Der geschriebene PHP-Programmcode ist klar strukturiert und angemessen kommentiert. Die Codequalität ist als gut einzustufen. Der Student entwickelte und realisierte einen guten Ansatz zur Integration von eigenem Validierungscode durch die Teilnehmer an einem Praktikum. Auf Ideen zur konsequenten Trennung von Code und Layout wurde nicht eingegangen. Der Aufbau der Datenbank ist einfach und klar (zwei Tabellen).
Das Design der generischen Input-Validierung, das zentral ist für die zwei untersuchten Attack-Typen, ist zu wenig mächtig und eher praxisfremd gewählt. So kann in einer *Validation class* nur nach den Typen *int*, *string* und *double* validiert werden. Es ist zu erwarten, dass dies für die meisten gängigen Web-Applikatoinen nicht reichen würde. Eine praxixnahe Input-Validierung müsste z.b. auch Formularfeld-spezifische Validierungen wie z.B. Email-Addresse, Telefon-Nummer, Passwort etc. erlauben.

# 5 Vortrag

Der auf englisch gehaltene Vortrag war klar und verständlich. Der Student war gut vorbereitet auf den Vortrag und hielt sich an die zeitlichen Vorgaben. Architektur, Performance oder Evaluation wurden nicht angesprochen. Die Conclusions (preventing attacks is not easy") sind etwas gar knapp ausgefallen.

Der Student beantwortete die Fragen im Anschluss kompetent.

# 6 Bericht

Die Ausarbeitung stellt die Aufgabenstellung sowie die entwickelte Applikation dar. Zudem wird die Installation erklärt. Es wurden auch zwei User Manuals (zu SQL injection bzw. XSS) sowie Musterlösungen erarbeitet.

Die Dokumentation zur Applikation ist etwas knapp ausgefallen, insbesondere was das Design, evaluation von related work und die getroffenen Entscheide betrifft. Oft werden sofort Details erklärt (z.B. GUI-Elemente), ohne den Kontext (z.B. fehlender Screenshot der Applikation) vorher klar zu machen, was den Leser leicht überfordern kann. Die trifft insbesondere auf das concept chapter 3ßu.

Es gibt nur kleine Inkonsistenzen (z.B. Seite 23: Datenbank MSS QL nicht erwähnt, obwohl auch dafür angepasst. Dafür wird DB2 (nicht getestet) erwähnt.).

Der in Englisch verfasste Text hat mehrere sehr verwirrende Schreibfehler, z.B. thread statt threat, fehlende Apostrophe bei vielen Genitiven, tough statt though, relay statt rely. Ein Korrekturlesen vor Abgabe war durch die Betreuer aufgrund der starken ungeplanten Verzögerungen der Arbeitsabgabe nicht möglich.

Die User Manuals mit ihren Aufgaben sind sehr offen gehalten. Es bleibt unklar, ob Studenten in einem Praktikum damit klar kommen, da es bisher nie getestet wurde. Mit vielen mögliche Antworten muss gerechnet werden, was ein solches Praktikum eher betreuungsintensiv gestalten wird. Die Musterlösungen geben nachvollziehbare und präzise Antworten.

Mehrere für das Nachschlagen praktische Tabellen stellen die Implementierungsdetails bzw. -parameter übersichtlich dar.

# 7 Zusammenfassung

Insgesamt wurden die Ziele der Arbeit erreicht. Die Gesamtqualität ist mit eher gut zu beurteilen. Die Resultate dieser Arbeit können nach kleineren Anpassungen und Ergänzungen für einen Praktikumsnachmittag oder im Unterricht verwendet werden.

## Note:

Zürich, den 18. November 2006