Stefan Waidele
Ensisheimer Straße 2
79395 Neuenburg am Rhein
Stefan.Waidele@AKAD.de

AKAD University
Immatrikulationsnummer: 102 81 71

Modul SWE02 — Softentwicklung
Assignment

Sicherheit bei Web–Anwendungen

Betreuer: Prof. Paul Kirchberg

29. April 2014

AKAD University

Inhaltsverzeichnis

Abkürzungsverzeichnis

CSS	Cascading Style Sheets
DOS	Denial of Service
DDOS	Distributed Denial of Service
SQL	Structured Query Language
WWW	World Wide Web
XSS	Cross Site Scripting

1 Einleitung

1.1 Ziele dieser Arbeit

In dierser Artbeit sollten mögliche Angriffstechniken auf Webanwendungen sowie geeignete Gegenmaßnahmen dargestellt werden.

Auch wenn eine Internetanwendung wie etwa ein Web–Shop nur einem beschränkten Personenkreis zur Verfügung stehen soll, so ist zumindest das Anmeldeformular[1] aufgrund der Struktur des World Wide Web (WWW) doch für Angriffe beliebiger Personen erreichbar. Daher sind schon bei der Implementierung eine Reihe von Sicherheitsaspekten zu beachten, um dieser umfangreichen Bedrohung entgegen zu wirken.

1.2 Aufbau der Arbeit

Zunächst werden im Kapitel 2 erörtert, warum der Sicherheitsaspekt bei der Erstellung eines Web–Shops ein wichtig ist. Es werden Angriffsziele, Szenarien genannt, sowie die möglichen wirtschaftlichen Konsequenzen eines erfolgreichen Angriffs aufgezeigt. Außerdem wird als ein einfaches HTML–Formular skizziert anhand dessen die unterschiedlichen Angriffsmöglichkeiten gezeigt werden können.

Im Kapitel 3 wird gezeigt, wie Angriffe mit dem Methoden Cross Site Scripting (XSS), SQL–Injection sowie Brute Force durchgeführt und abgewehrt werden können.

[1] Zumeist gilt dies für noch mehr Seiten mit Benutzerinteraktion, wie z.B. die Grundfunktionalität des Warenkorbs, Suchfunktione, etc.

1.3 Abgrenzung

Angriffe im Internet können an vielen Punkten der Datenübertragung statt finden. Diese Arbeit beschäftigt sich hauptsächlich mit den Methoden, auf die schon bei der Softwareentwicklung geachtet werden sollte. Risiken, die in den Verantwortungsbereich des Serverbetreibers oder WLAN–Anbieters (wie z.B. Man in the Middle), oder gar des Kunden (Datendiebstahl bzw. Keylogger auf dem Kunden–PC) liegen, werden hier nicht weiter behandelt, auch wenn sie im Grundlagenteil der Vollständigkeit halber erwähnt werden.

2 Grundlagen

2.1 Schützenswerte Güter

Vertraulichkeit, Integrität, Verbindlichkeit, Verfügbarkeit

2.2 Angriffsziele

Webshop, unsere Daten, die Daten unserer Kunden

2.3 Angriffsarten

Denial of Service (DOS) bzw. Distributed Denial of Service (DDOS), Man in the Middle, Cross Site Scripting XSS[2], SQL–Injection Structured Query Language (SQL), Brute Force

[2] X für „Cross“, um Verwechslungen mit Cascading Style Sheets (CSS) zu vermeiden.

3 Hauptteil

3.1 Bewertung der Kostenarten

3.1.1 Variable Kosten

3.1.2 Fixkosten

3.2 Bewertung der Zuschlagskalkulation

3.3 Vorstellung der Kostenstruktur im betrachteten Unternehmen

3.3.1 Ausgangslage

3.3.2 Entwicklung im Verlauf der Simulation

3.4 Bewertung der Kostenstruktur

3.4.1 Erklärung der Entwicklung

3.4.2 Bewertung

4 Bewertung & Ausblick

Literatur

[Friedl, 2007] Friedl (2007). SQL Injection Attacks by Example, Abruf am 25.10.2013. http://www.unixwiz.net/techtips/sql-injection.html.

[Fuest, 2013] Fuest (2013). Fall Vodafone zeigt die wahren Sicherheitslücken, Abruf am 25.10.2013. http://www.welt.de/wirtschaft/webwelt/article119967954/Fall-Vodafone-zeigt-die-wahren-Sicherheitsluecken.html.

[Hauer, 2010] Hauer (2010). Das Singleton Design Pattern, Abruf am 11.10.2013. http://www.philipphauer.de/study/se/design-pattern/singleton.php#nachteile.

[Olson (Hrsg.), 2013] Olson (Hrsg.) (2013). PHP Manual: Safe Password Hashing, Abruf am 25.10.2013. http://www.php.net/manual/de/faq.passwords.php#faq.passwords.fasthash.

[Oracle, 2013] Oracle (2013). MySQL 5.5 Manual: Encryption and Compression Functions, Abruf am 25.10.2013. https://dev.mysql.com/doc/refman/5.5/en/encryption-functions.html#function_md5.

[Schmalenbach, 1963] Schmalenbach (1963). *Kostenrechnung und Preispolitik*. Westdeutscher Verlag, Köln/Opladen, 8. auflage edition.

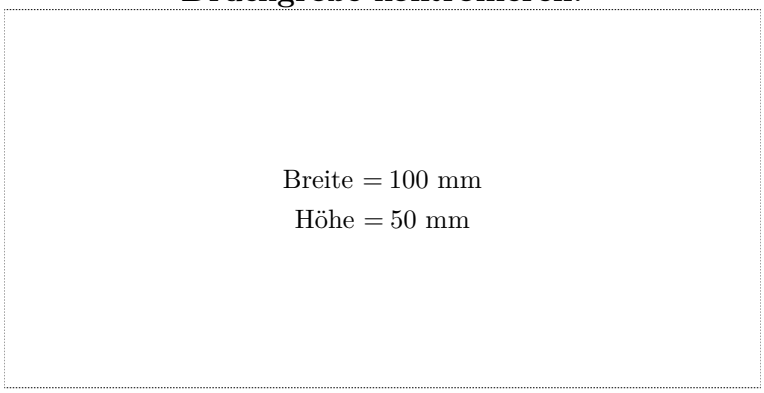
[Wöhe, 2010] Wöhe (2010). *Einführung in die Allgemeine Betriebswirtschaftslehre*. Verlag Franz Vahlen, München, 24. auflage edition.

Eidesstattliche Erklärung

Ich versichere, dass ich das beiliegende Assignment selbstständig verfasst, keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie alle wörtlich oder sinngemäß übernommenen Stellen in der Arbeit gekennzeichnet habe.

(Datum, Ort) (Unterschrift)

— Druckgröße kontrollieren! —



— Diese Seite nach dem Druck entfernen! —