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

1. Mai 2014

AKAD University

Inhaltsverzeichnis

Abkürzungsverzeichnis **ii**

1 Einleitung **1**
1.1 Ziele dieser Arbeit 1
1.2 Aufbau der Arbeit 1
1.3 Abgrenzung 2

2 Grundlagen **3**
2.1 Schützenswerte Güter 3
2.2 Angriffsziele 3

3 Angriffsarten und Gegenmaßnahmen **5**
3.1 Denial of Service 5
3.2 Man in the Middle 6
3.3 Brute Force 6
3.4 SQL–Injection 6
3.5 Cross Site Scripting 6

4 Bewertung & Ausblick **7**

Literatur **iii**

Abkürzungsverzeichnis

CSS	Cascading Style Sheets
DoS	Denial of Service
DDoS	Distributed Denial of Service
ERP	Enterprise Resource Planning
HTTP	Hypertext Tranfsfer Protocol
HTTPS	Hypertext Tranfsfer Protocol Secure
OWASP	Open Web Application Security Project
SCM	Supply Chain Management
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

Bei der Sicherheit eines Webshops bestehen die gleichen Grundbedrohunge wie bei der der Informationssicherheit im allgemeinn. Diese sind Vertraulichkeit, Verläßlichkeit, Verbindlichkeit, Verfügbarkeit.[2]

- **Vertraulichkeit:** Die Daten sollen nicht in die Hände von Unbefugten geraten bzw. unberechtigt gelesen werden.
- **Verläßlichkeit** (Integrität): Die Daten sollen nicht verändert werden.
- **Verbindlichkeit** (Authentizität): Die Herkunft der Daten bzw. die Identität des Urheber ist zweifelsfrei zu ermitteln.
- **Verfügbarkeit:** Die Daten bzw. Programmfunktionen sind jederzeit (bzw. immer wenn benötigt) verfügbar.

2.2 Angriffsziele

Ein Webshop bildet den Verkaufsprozess zwischen Händler und Kunde ab. Auch wenn die Angriffe an diesem Bindeglied stattfinden, können sich die oben genannten Grundbedrohungen auf unterschiedliche Ziele richten:

- **Der Webshop selbst:** Hier wird direkt auf die Verfügbarkeit bzw. Zuverlässigkeit der Shopsoftware gezielt
- **Die Unternehmensdaten:** Auch wenn bei oberflächlicher Betrachtung ein Webshop nur Produktdaten und Preislisten enthält, so sind hier durch die Kaufabwicklung weitere, durchaus sensible Daten wie z.B. Verkaufsstatistiken oder Rabattstaffeln gespeichert. Wird keine Stand–Alone Shoplösung

[2] Aufzählung und Erklärungen vgl. [Dix (Hrsg.), 2008]

sondern eine in das Supply Chain Management (SCM) bzw. Enterprise Resource Planning (ERP) integrierte Lösung verwendet, so können erfolgreiche Angreifer noch weitere Daten des Unternehmens erlangen.

- **Die Kundendaten:** Kundenadressen und vergangene Bestellungen können für gezieltes und effektives Direktmarketing genutzt werden. Kreditkarten– oder Kontodaten, Benutzernamen und Passwörter bieten ebenfalls eine Grundlage für weitergehende Angriffe auf die Benutzerkonten des Kunden bei anderen Anbietern und Diensten, bis hin zum Identitätsdiebstahl.[3]

[3] vgl. [Fuest, 2013]

3 Angriffsarten und Gegenmaßnahmen

Je nach Angriffsziel und Absicht des Angreifers kommen unterschiedlichen Angriffsmethoden zum Einsatz. Das Open Web Application Security Project (OWASP) erstellt regelmäßig eine Liste der der wichtigsten Angriffsarten auf Internetapplikationen. Die in dieser Arbeit untersuchten Risiken Injection (Am Beispiel Structured Query Language (SQL)) und XSS[4] belegen auf dieser Liste für 2013 die Plätze eins und drei[5]. Die beiden weiteren hier besprochenen Angriffsmethoden Denial of Service (DoS) bzw. Distributed Denial of Service (DDoS), Man in the Middle und Brute Force können als zumindest als Teilsspekte der ebenfalls in der Liste vorkommenden Punkte „Broken Authentication and Session Management“ (Platz 2) und „Security Misconfiguration“ (Platz 5) betrachtet werden.

3.1 Denial of Service

Unter einem DoS versteht man einen Angriff auf die Verfügbarkeit eines Angebots. Im Kontext dieser Arbeit verfolgt der Angreifer somit das Ziel, den Webshop für die Kunden unbenutzbar zu machen. Dies kann aufgrund der öffentlichen Erreichbarkeit mit legitim erscheinenden Anfragen an den Webserver geschehen. Aufgrund der Leistungsfähigkeit moderner Webserver ist dies aber i.d.R. nicht mit einzelnen Rechnern zu leisten. Daher werden meist große Netzwerke von Rechnern[6] für einen gemeinsamen, dann DDoS gennanten Angriff verwendet.[7]

Oft sind DoS–Angriffe nicht zweifelsfrei nachweisen, da Server auch durch eine entsprechende Menge von legitimen Zugriffen[8] überlastet werden können. Mögliche Gegenmaßnahmen sind die Nutzung einer skalierbaren Infrastruktur, die

[4] X für „Cross“, um Verwechslungen mit Cascading Style Sheets (CSS) zu vermeiden.
[5] vgl. [OWASP.org (Hrsg.), 2013]
[6] Die Besitzer dieser Rechner wissen i.d.R. nichts von diesen Angriffen, da die Schadsoftware unbemerkt über Computerviren eingeschleust wurde.
[7] vgl. [Carr, 2011], Kapitel 5
[8] z.B. durch Berichterstattung in populären Medien bzw. auf reichweitenstarken Webseiten („Slashdot–Effekt“)

allgeimein effektive Implementierung der Shopsoftware sowie eine entsprechende Konfiguration der Serversoftware (z.B. Caching).

Da DoS–Angriffe nicht nur per Hypertext Tranfsfer Protocol (HTTP) auf die Shopsoftware selbst sondern auch auf Firewalls oder Router zielen können[9] sind die Abwehrmöglichkeiten für den Entwickler der Shopsoftware sehr beschränkt.

3.2 Man in the Middle

Beim Man in the Middle Angriff versucht der Angreifer sich unbemerkt als Mittelsmann in die Kommunikation zwischen Kunde und Webshop einzuklinken. Obwohl der Kunde denkt, direkt mit der Anwendung zu kommunizieren, kann jeglicher Datenfluss vom Angreifer mitgelesen, protokolliert und in schlimsten Fall manipuliert werden. Der Angreifer benötigt daher Zugriff auf die Infrastruktur. Dieser kann im tatsächlichen Zwischenschalten von Abhörhardware[10] oder im virtuellen Zwischenschalten auf den unteren Protokollebenen der Netzwerkkommunikation erfolgen.[11]

Da der Applikationsentwickler keinen Einfluss auf die Infrastruktur des Internets hat, bleibt hier als Gegenmaßnahme lediglich die Wahl von verschlüsselten Kommunikaitonswegen, z.B. per Hypertext Tranfsfer Protocol Secure (HTTPS).

3.3 Brute Force

3.4 SQL–Injection

3.5 Cross Site Scripting

[9] vgl. [Amoroso, 2011], S. 60ff
[10] vgl. [Stoll, 1998], S. 28
[11] vgl. [Pritchett et al., 2013], Kapitel 7.8

4 Bewertung & Ausblick

Literatur

[Amoroso, 2011] Amoroso (2011). *Cyber Attacks – Protecting National Infrastructure*. Butterworth-Heinemann, USA.

[Carr, 2011] Carr (2011). *Inside Cyber Warfare*. O'Reilly Media, USA, 2nd. edition edition.

[Dix (Hrsg.), 2008] Dix (Hrsg.) (2008). Begriffsbestimmung: Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität, Abruf am 01.05.2014. `http://www.datenschutz-berlin.de/content/technik/begriffsbestimmungen/verfuegbarkeit-integritaet-vertraulichkeit-authentizitaet`.

[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 01.05.2014. `http://www.welt.de/wirtschaft/webwelt/article119967954/Fall-Vodafone-zeigt-die-wahren-Sicherheitsluecken.html`.

[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`.

[OWASP.org (Hrsg.), 2013] OWASP.org (Hrsg.) (2013). Top 10 – 2013, The Most Critical Web Application Security Risks, Abruf am 01.05.2014. `http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf`.

[Pritchett et al., 2013] Pritchett et al. (2013). *Kali Linux Cookbook*. Packt Publishing, USA.

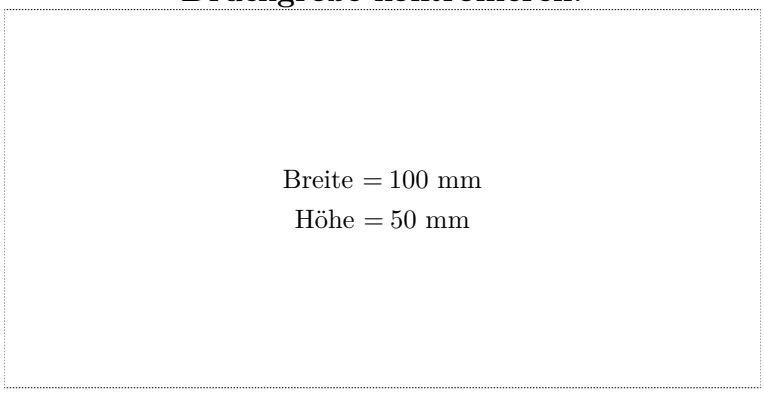
[Stoll, 1998] Stoll (1998). *Das Kuckucksei*. Fischer Taschenbuch Verlag, Frankfurt am Main, 6. auflage edition.

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! —