

# Potentielle Schwachstellen und Risiken von Online-Shops

☒ So unterschiedlich wie die bereits beschriebenen Auswirkungen der Angriffe sind auch die bekannten Schwachstellen charakteristischer Komponenten (Registrierung, Login, Bestellung, Bezahlung etc. ) von Online-Shops. Wir geben Ihnen hier im Blog einen Überblick zu häufigen Fehlern von Shopbetreibern.

## **Authentifizierung**

Eine Kernfunktion von Online-Shops ist die Authentifizierung, also die Anmeldemöglichkeit in einen geschützten Bereich (in der Regel der Verkaufs- oder Transaktionsbereich). Fehler in der Programmierung wie bspw. eine schwache Passwort-Wiederherstellungsfunktion oder aber auch Brute Force-Angriffe können die Übernahme eines Benutzeraccounts ermöglichen.

## **Authorisierung**

Häufig ermöglichen Web-Applikation einem Benutzer das unerlaubte Erlangen höherer Rechte, die einem bspw. das Löschen fremder Benutzeraccounts erlauben. Ursache ist oftmals eine schwache Implementierung des Sessionsmanagements.

## **Gefälschter Inhalt**

Ein Benutzer der einen Online-Shop ansteuert, geht davon aus, dass die Inhalte, die ihm dargestellt werden, tatsächlich vom Shopbetreiber stammen und er diesen vertrauen kann. Cross-Site Scripting Schwachstellen können jedoch das Austauschen des Inhalts oder das Ausführen von schädlichem Programmcode ermöglichen, um den Benutzer zu täuschen und an dessen Zugangsdaten oder Kontoinformationen zu gelangen.

## **Kommando Injektion**

Formularfelder in Webseiten ermöglichen dem Benutzer die Kommunikation mit der Web-Applikation. Bei schlechter Validation der Benutzereingaben können diese jedoch missbraucht werden, um konkrete Systemkommandos auf dem Webserver auszuführen. Ein Beispiel ist das Einschleusen von Datenbank-Kommandos (SQL-Injektion), die eine Modifikation von Datenbankinhalten bewirken kann.

## **Anzeige zusätzlicher Informationen**

Diese Art von Schwachstelle eines Online-Shops ermöglicht einem Angreifer das Auslesen von systemspezifischen Informationen wie beispielsweise Versionsnummern, Software-Distributionen oder die Position von Backup- und Administratoren-Verzeichnissen. Diese zusätzlichen Informationen können einem Angreifer diverse Attacks auf Standardsoftwarelösungen erleichtern.

## **Fehler in der Applikationslogik**

Oftmals gelingt Angreifern das Automatisieren oder Aufbrechen bestimmter logischer Abläufe bei Online-Shops. Beispielsweise erfolgt der Kauf eines Produkts in einem Online-Shop nach einem vorgegebenen sukzessiven Ablauf. In der Regel: Registrierung - Anmeldung - Produktauswahl - Bestellung - Bezahlung - Abmeldung. Gelingt es nun dem Angreifer, den Bezahlungsschritt zu übergehen, oder die Bestellung mehrfach automatisiert auszuführen, kann es zu Problemen für den Online-Shop kommen.

Diese Auflistung soll verdeutlichen, dass gerade für Online-Shops ein hohes Maß an technischer Sicherheit erforderlich ist, da deren charakteristischen Funktionalitäten großes Angriffspotential bieten. Aus diesem Grund erscheint hier in Kürze ein **Selbst-Check für Ihren Online-Shop**.

UPDATE: Im neuen **Trusted Shops Security-Audit** wird in enger Zusammenarbeit mit dem Shopbetreiber eine sicherheitstechnische Untersuchung vorgenommen. Mittels aktueller Prüfungssoftware testen Sicherheitsexperten die Site auf bekannte grundlegende Sicherheitsrisiken. Die Durchführung des Audits gliedert sich in fünf Phasen und wird in enger Zusammenarbeit mit dem Shopbetreiber durchgeführt. Ein detaillierter Audit-Report gibt Auskunft über Verwundbarkeiten und beschreibt erforderliche Gegenmaßnahmen.