Ist mein Online-Shop wirklich sicher? Der Schnell-Check

In diesem Beitrag wird ein dreistufiger Test erläutert, anhand dessen Sie Ihren eigenen Online-Shop auf die Existenz bekannter Sicherheitsschwachstellen prüfen können. Ist wenigstens ein Ergebnis der Prüfungen positiv, hat Ihr Online-Shop eine bekannte Schwachstelle, die unverzüglich behoben werden sollte.

Nutzen Sie diese einfach Möglichkeit, Ihre Sicherheit zu verbessern.

Die hier vorgestellten Methoden sind nicht destruktiv und eignen sich in dieser Form nicht für einen wirklichen Angriff. Sie verdeutlichen aber die Systematik der so genannten „Low-Hanging-Fruits"-Schwachstellen. Das Verständnis hierüber ermöglicht Ihnen den Blick von außen auf die Sicherheit Ihres Shops und liefert mögliche Optimierungspotentiale.

Sicherheitslücke	Potentielle Gefahr
1. Eingabefeld (z.B. Suchformular)	Cross-Site Scripting (XSS) Schwachstellen ermöglichen das Austauschen des Inhalts oder das Ausführen von schädlichem Programmcode, um den Benutzer zu täuschen und bspw. an dessen Zugangsdaten oder Kontoinformationen zu gelangen.
2. Login-Formular	Mit „Brute Force" Angriffen können Angreifer Benutzernamen und Passwörter herausfinden und damit im Namen eines Benutzers einkaufen.
3. Befehlsausführung	Mit „SQL Injection" Angriffen können Angreifer sich unerlaubten Zugang zu Ihrer Datenbank verschaffen.

Prüfung 1: Eingabefeld / Cross-Site-Scripting (XSS)
Folgen Sie diesem Link XSS, klicken anschließend in das Eingabefeld und kopieren die Zeichenfolge in die Zwischenablage (STRG+A und STRG+C). Anschließend surfen Sie Ihren Online-Shop an und fügen die Zeichenfolge aus der Zwischenablage (STRG+V) in das Suchformular Ihres Shops ein.

> *Erscheint nach dem Absenden des Formulars ein Pop-Up Fenster mit dem Inhalt ‚XSS', sind sie soeben Opfer eines erfolgreichen (aber natürlich harmlosen) Cross-Site-Scripting Angriffs geworden.*
>
> *Erscheint kein Pop-Up Fenster mit dem Inhalt ‚XSS', sondern die Webseite reagiert wie gewohnt auf diese Suchanfrage, ist zumindest Ihr Suchformular gegen gängige Cross-Site-Scripting Angriffe geschützt.*

Prüfung 2: Login-Formular
Ist die Anzahl falscher Eingaben beim Login begrenzt?

> *Um Brute-Force Attacken auf das Login-Formular zu vermeiden, sollten Benutzer nach dem fünften nicht erfolgreichen Login automatisch für bspw. 20 Minuten ausgesperrt werden.*
>
> *Ist das nicht der Fall sollten zumindest folgende bekannte Standardpasswörter bei der Registrierung unterdrückt werden (Passwort; 12345678; ‚Benutzername' ; ‚Shopname')*

Prüfung 3: Befehlsausführung
Dieser Test wird ebenfalls auf das Login-Formular angewandt. Es handelt sich um eine so genannte SQL-Injection. Führen Sie einen Login-Versuch mit der Zeichenfolge "`admin' --` " (ohne Anführungszeichen) als Benutzernamen und einem beliebigen Passwort durch.

Reagiert das System ungewöhnlich, beispielsweise durch die Ausgabe einer Systemfehlermeldung (SQL Error) bietet die Datenbankschnittstelle einen potentiellen Angriffspunkt, indem sie unnötig Informationen preisgibt.

Loggt das System sogar erfolgreich ein ist es Ihnen gelungen sich ohne die Eingabe eines Passwortes als Administrator für das System zu authentifizieren. In diesem Fall sollten Sie unbedingt die Validierung Ihres Login-Formulars überprüfen.

Erscheint jedoch die gewohnte Fehlermeldung, dass Benutzername und/oder Passwort nicht korrekt eingegeben wurden, ist zumindest Ihr Login-Formular gegen diesen speziellen Angriff geschützt.

Um das vom Benutzer entgegengebrachte Vertrauen bestätigen zu können und sich sowie seine Benutzer nicht zu gefährden, sollte ein Online-Shop frei von bekannten Schwachstellen sein. Wie unser kurzer Selbsttest zeigt, bedarf das Ausnutzen dieser Schwachstellen heute keines großen Vorwissens oder gar besonderer Tools.

Übrigens: Im **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.