

# Teilautomatisierter Web Application Penetration Test

Gemäss Untersuchungen sind mehr als 50 Prozent der Schwachstellen auf der Applikationsebene zu finden. Die Tendenz ist klar steigend. Auch grössere Anwendungen sind davor nicht gefeit. Die Auswirkungen solcher Schwachstellen können vielfältig sein; Umsatzeinbussen, Verlust der Reputation und Abfluss von kritischen Firmen- oder Kundendaten um nur die wichtigsten zu nennen. Schützen Sie sich rechtzeitig.

Der teilautomatisierte Web-Applikations Penetration Test von Protect7 setzt genau dort an. Dieser überprüft grösstenteils toolbasiert Ihre externen und internen Web-Applikationen auf bekannte Schwachstellen. Protect7 überprüft gefundene Schwachstellen auf False-Positives und bewertet die Risiken im Kontext Ihrer Unternehmung.

## Methode

Die eingesetzte Software untersucht automatisch Ihre Web-Applikation und versucht die gängigsten Angriffsszenarien durchzuführen. Neben Schwachstellen in Ihrer Applikation findet es auch typische Konfigurationsfehler des Webservers und des Applikationsservers.

Mittels verschiedener Methoden wird versucht, die Funktionalitäten der Applikation auszuhebeln oder zu Umgehen. Dadurch wird versucht zu erreichen, dass die Applikation unerlaubte Informationen preisgibt oder die Applikation für andere Zwecke missbraucht werden kann.

Die wichtigsten Punkte bei einem teilautomatisierten Test:

- Informationsbeschaffung durch erzeugte Fehler, Errors oder ungehärtete Applikationen
- Umgehen der Authentifizierung & Autorisierung
- Analyse des Session-Management und Möglichkeiten zum Aushebeln
- Ausprobieren von Injection Angriffen gegen Datenbanken, User Directories oder ähnlichem, um direkt von Eingabefeldern aus auf eigentlich versteckte Daten zuzugreifen (SQL Injection, Code injection etc.)
- Analysieren ob Cross Site Scripting (XSS) möglich ist, wodurch fremder Code auf Ihrer Web-Applikation eingeschleust werden kann, wodurch Ihre Kunden zu Opfern werden könnten
- Überprüfung der Resultate, sowie spezifische manuelle Test durch einen unserer Security Engineers
- Manuell erstellte Risikoeinschätzung und Management Summary

## Hauptziel

Das Hauptziel der teilautomatisierten Überprüfung besteht darin, herauszufinden ob Ihre Applikationen in Bezug auf die bekanntesten Angriffsszenarien anfällig sind. Aktuell vorhandene Risiken werden im Kontext Ihrer Unternehmung aufgezeigt sowie automatisch rapportiert.

## Sie erhalten

- Management Zusammenfassung
- Unsere Einschätzung zu den gefundenen Schwachstellen inkl. Empfehlungen
- Detaillierte automatisierte Reports (Management und Technisch)
- Detaillierte automatisierte Empfehlungen für Verbesserungen
- Report in PDF- und Word-Format

## Ihr Vorteil

- Information zum Sicherheitsniveau Ihrer Web-Applikation
- Minimaler Aufwand
- Finden Sie die Schwachstellen bevor es andere tun
- Überprüfen Sie Ihre Applikationen bevor sie online gehen
- Managen Sie Ihr Risiko
- Treffen Sie geeignete Massnahmen

## Preis

- Der Preis für eine Web-Applikation beträgt CHF 3'450.-
- Zuzüglich administrativer Kosten von CHF 250.-
- Preise exkl. MwSt.

# Teilautomatisierter Web Application Penetration Test



## Benötigte Informationen für den Auftrag

Um einen Teilautomatisierten Penetration Test durchführen zu können, benötigen wir von Ihnen folgende Angaben:

Webseiten-URL:	
IP Adresse(n):	
Applikations-Accounts:	
Ausführungsdatum/-Zeit:	
Kontaktperson (Tel.):	
Weitere Informationen:	

**Hinweis:** Detaillierte Informationen in der Checkliste „Web Application Penetration Test Kunden-Checkliste“

## Bestellung

Wir bitten Sie, die benötigten Informationen auszufüllen, die Lieferadresse sowie Rechnungsadresse einzutragen und uns die Bestellung mit Firmenstempel sowie rechtsgültig unterzeichnet zuzusenden.

per Post: Protect7 GmbH, Schaffhauserstrasse 418, CH-8050 Zürich  
per E-Mail: info@protect7.com  
per Fax: +41 44 515 68 69

Hiermit bestätigen wir:

- Dass wir Eigentümer der oben aufgeführten Webseite sind
- Die Web Application Penetration Test Kunden-Checkliste gelesen und akzeptiert haben
- Protect7 mit dem Penetration Test der aufgeführten Webseite zu beauftragen

Lieferadresse:	Rechnungsadresse
----------------	------------------

Ort:

Datum:

Rechtsverbindliche Unterschrift(en):

