

Web Security Check

Das Internet ist öffentlich und somit grundsätzlich unsicher. Das bedeutet eine mögliche Gefährdung Ihrer Webinhalte (Internet, Intranet und Extranet). Auch Kundendaten sind exponiert und manipulierbar. Cross-Side Scripting, SQL Injection, Cookie Poisoning, Session Replay etc. sind keine leeren Schlagworte, sondern relativ einfache Methoden, um an schätzenswerte Informationen zu gelangen, diese zu verändern oder unerlaubte Aktionen auszuführen.

Um Ihr Internetangebot und Ihre Daten abzusichern, gibt es einerseits Regeln bei der Implementierung, Integration und Konfiguration zu beachten. Andererseits kann die Überprüfung der Sicherheit nicht durch die Entwickler selbst durchgeführt werden. Sicherheit ist immer ein Abwägen von Kosten für Massnahmen und Schadenskosten. Der Schaden durch Verlust von Kundendaten oder manipulierte Inhalte ist aber häufig beträchtlich.

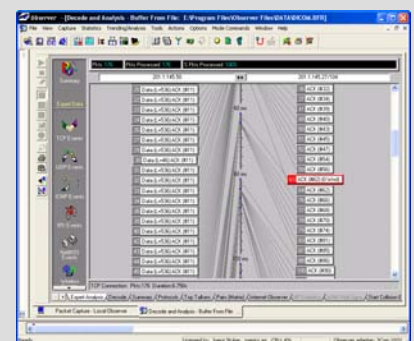
namics hat in verschiedenen Kundenprojekten eine strukturierte Vorgehensweise entwickelt, um die Sicherheit Ihres Angebotes zu überprüfen und Handlungsempfehlungen zu erstellen, die Ihre Anwendungen schützen können.

Ergebnisse

Nach dem namics Web Security Check erhalten Sie diese folgenden Ergebnisse:

- » Ergebnisbericht/Gutachten, das die Ergebnisse der Überprüfung zusammenfasst und dokumentiert
- » Nach Aufwand und Wichtigkeit priorisierte Handlungsempfehlungen für das Beheben der aufgetretenen Schwächen
- » Guidelines für die Entwickler der Website aufgrund der aufgetretenen Schwächen und Handlungsempfehlungen
- » Eine Checkliste für die Qualitätssicherung bei der Weiterentwicklung der Site

- » Sicherheit für Ihre Kundendaten
- » Verhinderung der Manipulation von Inhalten
- » Vermeidung von Imageverlusten und weiteren Schäden



Auswertung des Datenverkehrs zwischen Browser und Server

Vorgehen

1. Auswahl von zehn zu testenden Funktionalitäten und/oder Seiten
2. Testen von Angriffsmöglichkeiten: Eingabevalidierung von Formularen, URL-Encoding, Manipulation von Hidden Fields, Cookies, HTTP-Headers, Cross-Side Scripting, Null Characters, Directory/Path Traversal, SQL Injection, Cookie Poisoning, Session Replay, Mail Spoofing, Brute Force Attacken, unvollständige Authentifizierung, Exposure Web-Application Logic u.a.
3. Testen des Netzwerkzugangs und verfügbarer Dienstmerkmale (sofern durch den Kunden erlaubt)
4. Zusammenfassen der Ergebnisse in einem Ergebnisbericht/ Gutachten und Ableiten von Handlungsempfehlungen
5. Erstellen angepasster Guidelines für Ihre Programmierer
6. (Optional) Optimierung der Site durch namics

Erfahrungen und Referenzen

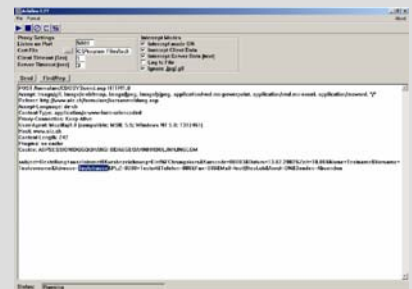
- » namics verfügt über Guidelines und Regeln zur Programmierung von sicheren Web Anwendungen und setzt diese standardmäßig in allen Kundenprojekten ein
- » namics arbeitet für zahlreiche Kunden der Finanzindustrie und der öffentlichen Hand mit hohen Anforderungen an Sicherheit.

Weiterführende Unterlagen

- » namics Einführung zum Thema „Web Application Security“
- » Unterlagen zum namics Fachvortrag “Security-Grundlagen für Entwickler von Internet-Anwendungen“

Preise

	CHF
Überprüfung Ihres Internet-Angebots durch namics	12'000.–
Erstellung von Guidelines für die Entwickler	4'400.–
Optimierung Ihrer Site durch namics	nach Aufwand



Lokaler Proxy, um die zum Server geschickten Daten zu manipulieren

Weitere Informationen

namics ag
Nüscherstrasse 32
CH-8001 Zürich
t +41 44 228 67 77
f +41 44 228 67 88

info@namics.com
www.namics.com