**Web Application Security Assessment**

Das Assessment beinhaltet eine umfassende technische Überprüfung der Webanwendung, um potenzielle Schwachstellen aufzudecken, die die Sicherheit und Integrität der Anwendung beeinträchtigen könnten. Die Methodologie stützt sich auf dem OWASP Web Security Testing Guides (WSTG) [[1]](#footnote-1) sowie den OWASP Top 10 Web Application Security Risks[[2]](#footnote-2). Dabei werden verschiedene Angriffsszenarien analysiert, um die Webanwendung umfassend zu bewerten.

**Methodologie**

Die Penetrationstests umfassen sowohl automatisierte als auch manuelle Prüfungen, um ein breites Spektrum an potenziellen Angriffsszenarien zu berücksichtigen:

* **Serverscans und Infrastrukturtests**: Die Tests beinhalten Port- und Service-Scans auf den zugrunde liegenden Servern, um Schwachstellen zu identifizieren und die Integrität der zugrunde liegenden Komponenten zu überprüfen. Gefundene Schwachstellen werden manuell validiert, um False Positives auszuschliessen und die tatsächliche Sicherheitslage präzise zu bewerten.
* **Manuelle Funktionstests**: Manuelle Tests konzentrieren sich auf die kritischen Bereiche der Anwendung, insbesondere im Bereich der Benutzerverwaltung, des Dokumentenhandlings und der integrierten Kommunikationsfunktionen. Die Tests gewährleisten, dass sensible Daten und kritische Funktionen vor Manipulationen und unbefugtem Zugriff geschützt sind.
* **Manuelle Tests auf Sicherheitslücken**: Neben automatisierten Scans erfolgt eine manuelle Prüfung auf potenzielle Sicherheitslücken, einschliesslich typischer Angriffspunkte wie Cross-Site Scripting (XSS), SQL Injection und Command Injection, um Schwachstellen in der Eingabeverarbeitung zu identifizieren.
* **Prüfung der Zugriffsrechte, Rollen sowie Authentifizierungs- und Autorisierungsmechanismen:** Es wird überprüft, ob die Zugriffsrechte für verschiedene Benutzerrollen sauber implementiert sind und ob Benutzer ausschliesslich auf Daten zugreifen können, für die sie autorisiert sind. Zudem wird sichergestellt, dass privilegierte Aktionen nur mit den entsprechenden Berechtigungen ausgeführt werden können. Die Mechanismen zur Authentifizierung und Autorisierung werden getestet, um unbefugte Zugriffe auf sensible Bereiche der Anwendung zu verhindern.
* **Einsicht in Quellcode**: Auf Wunsch kann uns der Kunde bestimmte Codeabschnitte oder Konfigurationen zeigen, um Unklarheiten zu beseitigen. Dies ist kein umfassendes Code Review, sondern dient einer optimalen Validierung von möglichen Schwachstellen.

**Anforderungen**

Für die Durchführung des Penetrationstests sind folgende Vorbereitungen erforderlich:

* **Freischaltung der WAF**: Während des Tests wird die Web Application Firewall (WAF) für die IP-Adresse der   
  InfoGuard (85.195.223.145) temporär freigeschaltet, um eine realistische Sicherheitsbewertung zu ermöglichen. Dies erlaubt eine gezielte Identifikation von Schwachstellen, ohne dass die WAF Angriffe blockiert und dadurch Testegebnisse verfälscht. Falls erforderlich, kann die Freischaltung der WAF vor Abschluss der Testphase wieder aufgehoben werden.
* **Bereitstellung von Benutzerkonten**: Benutzerkonten mit verschiedenen Berechtigungsstufen sollten zur Verfügung gestellt werden, um die Zugriffsrechte und Rollen in der Anwendung umfassend zu prüfen.
* **Testumgebung (empfohlen):** Es wird empfohlen, eine stabile Testumgebung bereitzustellen, die der produktiven Umgebung möglichst nahekommt. Vor Testbeginn sollte ein Backup der Applikationsdaten erstellt werden, um eine einfache Wiederherstellung nach den Tests zu gewährleisten.
* **Technischer Ansprechpartner**: Ein technischer Ansprechpartner sollte während der Testphase für Rückfragen zur Verfügung stehen, insbesondere um Fragen zur Anwendung, Quellcode oder Infrastruktur zu beantworten.

**Erneuter Test der behobenen Schwachstellen (wenn möglich)**

Nach Abschluss der initialen Testphase führen wir einen gezielten Test der anfänglich identifizierten und zwischenzeitlich durch den Kunden behobenen Schwachstellen durch. Dadurch wird sichergestellt, dass die umgesetzten Massnahmen erfolgreich waren. Der Schwerpunkt liegt auf rasch umsetzbaren Sicherheitsverbesserungen („Quick Wins“ bzw. „Low Hanging Fruits“). Diese Überprüfung stellt keinen vollständigen Re-Test dar, ermöglicht jedoch eine schnelle Validierung, ob kritische Sicherheitslücken erfolgreich behoben wurden. Der optionale Re-Test wird zu einem späteren Zeitpunkt durchgeführt und ist nicht Teil dieser gezielten Überprüfung.

1. <https://github.com/wisec/OWASP-Testing-Guide-v5/> [↑](#footnote-ref-1)
2. <https://owasp.org/www-project-top-ten/> [↑](#footnote-ref-2)