CRASHTEST SECURITY

LEISTUNGSBESCHREIBUNG

1 Inhaltsverzeichnis

2 Allgemein

2.1 Warum sollten Webapplikationen automatisch geprüft werden?

Die Entwicklung sicherer Software stellt viele Unternehmen vor Herausforderungen. Im Durchschnitt hat jede Webanwendung 7 kritische Sicherheitslücken, welche im Schnitt für mehr als 300 Tage ungeschlossen bleiben. Dieses Problem lässt sich zum einen darauf zurückführen, dass IT-Sicherheit während der Softwareentwicklung nicht ausreichend hoch priorisiert und der Fokus auf die Entwicklung neuer Features gelegt wird, da diese für die Unternehmen vermeidlich gewinnbringender sind. Zum anderen werden Webanwendungen im Rahmen der agilen Entwicklungsmethoden teilweise im Wochentakt aktualisiert und den Endnutzern zur Verfügung gestellt, jedoch werden Penetrationstests aufgrund der hohen Kosten meist nur jährlich durchgeführt. Dies eröffnet einen großen Raum für Angriffe und führt zu unsicherer Software. Die Folge hieraus ist, dass Unternehmen immer häufiger die Geschädigten von gezielten Cyber-Angriffen werden.

2.2 Produktbeschreibung

Die Crashtest Security GmbH bietet mit der Crashtest Security Suite ihren Kunden eine Software-as-a-Service (SaaS) Lösung zur automatischen Durchführung von Penetrationstests. Der Service ist speziell an die Bedürfnisse moderner Softwareentwicklung angepasst und lässt sich in den Continuous Integration (CI) / Continuous Deployment (CD) Prozess integrieren. Dieses Vorgehen, welches auch unter dem Begriff SecDevOps bekannt ist, stellt sicher, dass Ihre Webanwendung kontinuierlich auf Sicherheitslücken geprüft wird. Unsere Scanner decken die häufigsten auftretenden Sicherheitslücken im Webumfeld ab und benötigen keinen Zugriff auf Ihren Quellcode, da sie im sogenannten Blackbox-Verfahren testen. Darüber hinaus unterstützen wir Ihre Softwareentwickler bei der zeitnahen Behebung der gefundenen Sicherheitslücken mit konkreten Lösungsvorschlägen in unserer Wissensdatenbank. Hierdurch geben wir Ihren Mitarbeitern die Möglichkeit sich auf das Wesentliche zu konzentrieren nämlich der Entwicklung weiterer Features ohne die Sicherheit Ihrer Webanwendung zu vernachlässigen.

3 Leistungselemente

3.1 Benutzerverwaltung

Es kann ein Benutzer zur Verwaltung mehrerer Projekte angelegt werden. Der Nutzer kann seine Kontakt- und Authentifizierungsdaten pflegen.

3.2 Projektverwaltung

Entsprechend des gewählten Leistungspaketes (siehe 4) können ein oder mehrere Projekte verwaltet werden. Für jedes Projekt wird eine Webadresse (URL) hinterlegt unter der das zu testende System erreichbar ist. Wenn invasive Scans (siehe 3.3) durchgeführt werden sollen, stellt ein automatisiertes Verfahren sicher, dass der Kunde der rechtmäßige Inhaber der Domain und somit zur Durchführung der Sicherheitsscans berechtigt ist (siehe 5.3). Des Weiteren können für jedes Projekt spezifische Einstellung zur Konfiguration der Systemumgebung (siehe 3.3), dem Reporting (siehe 3.4), dem Zugriffsschutz der zu testenden Webanwendung (siehe 3.6) und der automatisierten Durchführung der Sicherheitsprüfungen (siehe 3.7) vorgenommen werden.

3.3 Sicherheitsscanner

Die Crashtest Security Suite ist aus einer Reihe von individuellen Sicherheitsscannern aufgebaut. Die einzelnen Scanner sind spezifisch an die zu testende Kategorie von Sicherheitslücken angepasst und ermöglichen hierdurch eine effektivere und effizientere Prüfung. Darüber hinaus ermöglicht die Kapselung der Sicherheitstests in unabhängige Komponenten eine starke Parallelisierung der Prüfung und somit eine deutlich kürzere Scandauer.

Ein Teil der Scanner prüft nicht-invasiv durch die Analyse der Antworten des Webservers (in der Auflistung mit * markiert) und kann auch zur Überprüfung von Produktivsystemen eingesetzt werden. Die verbleibenden Scanner versuchen durch gezielte Schadeingaben in die zu testende Webanwendung einzudringen und sollten ausschließlich auf Testsystemen eingesetzt werden.

Zum aktuellen Zeitpunkt umfasst die Crashtest Security Suite die folgenden Scanner:

- Fingerprinting *
- SSL / TLS *
- SQLInjection
- Cross-Site-Scripting (XSS)
- Cross-Site-Request-Forgery (CSRF)

3.4 Reporting

Die Ergebnisse einer Sicherheitsüberprüfung können in vollem Umfang über das Webinterface der Crashtest Security Suite eingesehen werden. Hier erhalten die Nutzer über das Dashboard einen Überblick der Sicherheitssituation ihrer Projekte und ausführliche Informationen zu den gefundenen Sicherheitslücken. Jede Lücke wird durch den Service gemäß des Common Vulnerability Scoring Systems (CVSS) bewertet, welches die Nutzer bei der Priorisierung der Behebungsmaßnahmen unterstützt. Darüber hinaus können die Entwickler auf eine Wissensdatenbank zugreifen, die konkrete Schritte und Vorschläge zur Behebung der Sicherheitslücken bereitstellt (siehe 3.5). Neben der Präsentation über das Webinterface kann eine zusammengefasste Benachrichtigung über die Ergebnisse über per E-Mail und über ein Chatprogramm an die Software Entwickler geschickt werden. Dies ist insbesondere bei der Nutzung der Automatisierung (siehe 3.7) nützlich, um direkt Feedback über die Sicherheitssituation der Webanwendung an die Entwickler weiterzugegeben.

Zum aktuellen Zeitpunkt unterstützt die Crashtest Security Suite ein Reporting über die folgenden Kanäle:

- Webinterface
- Chatprogramme
    - Slack

3.5 Wissensdatenbank

Die Wissensdatenbank stellt für die verschiedenen Sicherheitslücken konkrete Schritte und Vorschläge zu Behebung zur Verfügung. Die Lösungsvorschläge umfassen die marktüblichen Applikationen und Technologien (z.B. Apache und Nginx). Es handelt sich hierbei um ein lebendes System, welches laufend ergänzt und erweitert wird. Eine vollständige Abdeckung an Lösungsvorschlägen für jede potentielle Sicherheitslücke ist nicht gewährleistet. Kontaktieren Sie bitte unseren Support, falls für Ihre konkrete technologische Umgebung keine Lösungsvorschläge vorhanden sind. Die Wissensdatenbank ist nicht zugangsbeschränkt und kann auch öffentlich abgerufen werden.

3.6 Zugriffsmöglichkeiten auf Testsysteme

Öffentlich zugängliche Webanwendungen können ohne zusätzliche Konfigurationsaufwand durch die Crashtest Security Suite gescannt werden. Darüber hinaus bietet das System mehrere Möglichkeiten um auf geschützte Testsysteme

zuzugreifen. Den Scannern kann über eine IP-Adressen Freigabe in Ihrer Firewall Zugang zu Ihrer Webanwendung gewährt werden. Hierzu betreiben wir alle Scanner hinter einem NAT-Gateway und können Ihnen dessen fixe IPv4-Adresse für die Freigabe zur Verfügung stellen. Des Weiteren unterstützt die Crashtest Security Suite die HTTP-Basisauthentifizierung (.htaccess) und die Authentifizierung gegenüber der Webanwendung selbst (Login-Formular). Falls eine IP-Freigabe benötigt wird, kontaktieren Sie bitte den Support.

3.7 Automatisierung

Ein Sicherheitsscan kann nicht nur über das Webinterface der Crashtest Security Suite gestartet werden, sondern auch über einen Webhook. Ein konkretes Szenario hierfür wäre die automatische Durchführung eines Sicherheitstests nachdem Ihre Build-Infrastruktur eine aktuelle Version auf das Testsystem aufgespielt hat.

4 Leistungspakete

Die Crashtest Security Suite kann in unterschiedlichen Leistungspaketen bezogen werden. Sofern in der nachfolgenden Tabelle nicht gesondert aufgeschlüsselt, verfügen alle Pakete über die in 3 aufgeführten Leistungselemente.

	Free	Basic	Advanced	Profes-sional	Agency/ Team
Anzahl der Projekte	1	2	5	10	50
Anzahl der Scans pro Monat	1	10	25	100	250
Nicht Invasive Scans	Ja	Ja	Ja	Ja	Ja
Invasive Scans	Nein	Ja	Ja	Ja	Ja
Änderung von Test-/Produktivumgebung	Nein	Ja	Ja	Ja	Ja
Webhook	Nein	Nein	Ja	Ja	Ja
Benachrichtigung via Chat	Nein	Ja	Ja	Ja	Ja

5 Voraussetzungen und Mitwirkungspflichten

5.1 Webbrowser

Zum Abruf des Webinterfaces der Crashtest Security Suite benötigt der Kunde einen Webbrowser. Der Kunde hat dafür Sorge zu tragen, dass dieser auf dem aktuellen Stand gehalten wird.

Die Crashtest Security Suite wird auf Kompatibilität mit den folgenden Browsern geprüft:

- Chrome (>= 54)
- Firefox (>= 50)
- Internet Explorer (>= 9) / Edge (>= 14)
- Safari (>= 7)

5.2 Zugangsdaten

Der Kunde ist verpflichtet die Ihm zur Verfügung gestellten Zugangsdaten geheim zu halten und nicht weiterzugeben. Des Weiteren stellt der Kunde sicher, dass ausschließlich er bzw. hierzu berechtigte Dritte Zugriff auf den bei der Registrierung angegebenen E-Mail Account haben.

5.3 Berechtigung zum Scannen

Die Crashtest Security GmbH prüft bei der Durchführung von invasiven Scans durch automatische Prozesse, ob der Kunde zum Scannen der angegebenen Domain berechtigt ist. Dazu legt der Kunde eine von der Crashtest Security GmbH bereitgestellte Datei auf dem Server der zu testenden Anwendung ab. Ein Sicherheitsscan durch die Crashtest Security Suite kann nur gestartet werden, wenn sich diese Datei auf dem Server befindet. Diese Prüfung entbindet jedoch den Kunden nicht davon, sicherzustellen, dass er die Crashtest Security GmbH beauftragen darf, Sicherheitstests durchzuführen. Dies gilt auch für die Durchführung von nicht invasiven Scans. Es ist zudem durch den Kunden zu prüfen, ob die Bereitsteller der Infrastruktur der zu testenden Anwendung eine Genehmigung für Sicherheitstests erteilen müssen. Im Falle der Durchführung von Sicherheitsscans durch den Kunden für einen Dritten (z.B. Agenturgeschäft), muss diese Genehmigung ebenfalls eingeholt werden.

Insbesondere dürfen keine Sicherheitsscans für Domains durchgeführt werden, welche nicht der administrativen Kontrolle des Kunden unterliegen.

Dies Genehmigungen können von der Crashtest Security GmbH im Falle einer Klage oder Beschwerde eingefordert werden um der dritten Partei einen

Berechtigungsnachweis für die Durchführung der Sicherheitsscans vorlegen zu können.

5.4 Umgebung des zu testenden Systems

Die Crashtest Security Suite besitzt Scanner die invasive und nicht-invasive Verfahren im Rahmen ihrer Sicherheitsüberprüfung einsetzen (siehe 3.3). Bei invasiven Tests (z.B. SQL-Injection) kann es zur einer Beeinträchtigung bzw. Ausfällen von Systemen kommen, deshalb dürfen diese nicht bei Produktivsystem zum Einsatz kommen. Die Crashtest Security GmbH trägt dafür Sorge, sichere Standardeinstellungen für das Anlegen neuer Projekte zu wählen und den Kunden bei der Wahl der korrekten Einstellungen zu unterstützen. Die letztendliche Entscheidung, ob es sich bei dem zu testenden System um ein Produktiv- oder Testsystem handelt, kann nur durch den Kunden erfolgen und liegt in dessen Verantwortung.

5.5 Zugriff auf das zu testende System

Gemäß 3.6 bietet die Crashtest Security Suite verschiedene Möglichkeiten um auf ein zugriffsbeschränktes Testsystem zugreifen zu können. Die jeweils notwendigen Einstellungen auf Seiten der Kundeninfrastruktur für den Zugriff auf das Testsystem (z.B. Erstellung einer Firewall-Freigabe) werden nicht durch die Crashtest Security GmbH vorgenommen, sondern müssen durch den Kunden erfolgen.

5.6 Datenbestand des zu testenden Systems

Der Kunde hat sicherzustellen, dass das zu testende System im Falle eines Testsystems keine Produktionsdaten enthält, da bei der Durchführung von invasiven Tests ein Zugriff auf diese Daten nicht ausgeschlossen werden kann. Dies gilt es insbesondere bei Webanwendungen zu beachten, die personenbezogene Daten verarbeiten, speichern oder nutzen. Beim Einsatz von nicht-invasiven Tests gegen Produktivsysteme stellt die Crashtest Security GmbH sicher, dass die Überprüfung der Sicherheit ausschließlich anhand nicht zugriffsbeschränkter Datenfelder wie z.B. den HTTP-Headern oder der Index-Seite erfolgen.

6 Sonstiges

6.1 Preise

Die Crashtest Security Suite kann direkt über den Webauftritt der Crashtest Security GmbH bezogen werden. Die aktuelle Preisliste kann dem Webauftritt entnommen werden.

6.2 Vertragslaufzeiten

Zur Bestellung eines kostenpflichtigen Pakets ist ein Benutzerkonto notwendig. Die Laufzeit eines kostenpflichtigen Pakets beginnt mit dem Tag Bestellung über die Crashtest Security Suite. Die Mindestvertragslaufzeit der Crashtest Security Suite beträgt 1 Monat. Der Vertrag verlängert sich automatisch um 1 Monat, falls dieser nicht zum Ende der Mindestvertragslaufzeit bzw. zum Ende der Folgelaufzeit gekündigt wird. Eine Kündigung des kostenpflichtigen Pakets hat nicht die Löschung des Benutzerkontos, sondern nur die Herabstufung auf ein kostenloses Paket zu Folge. Der Wechsel auf ein anderes bezahltes Paket kann jederzeit erfolgen. Ein über den aktuellen Tag hinaus entrichteter Betrag auf das vorherige Paket wird der nächsten Rechnung gutgeschrieben.

6.3 Abrechnung

Die Berechnung erfolgt ab dem Beginn der Vertragslaufzeit. Der Abrechnungszeitraum der Crashtest Security Suite ist monatlich.

7 Services und Support

7.1 Service Level

Die Crashtest Security GmbH garantiert für die Crashtest Security Suite eine Verfügbarkeit 95%. Der Messpunkt für die Verfügbarkeitsmessung ist außerhalb des Rechenzentrums in welchem die Crashtest Security Suite betrieben wird. Die Verfügbarkeit wird nur außerhalb des Wartungsfensters garantiert. Das Wartungsfenster ist:

- Montag – Freitag: 18:30 – 22:30 Uhr
- Samstag: 8:00 – 12:00 Uhr

Service Level Periode beträgt jeweils den vollen Monat. Die tatsächliche Verfügbarkeit wird pro Service Level Periode berechnet. Das Service Level wird nur für die kostenpflichtigen Pakete der Crashtest Security Suite garantiert.

Falls die garantierte Verfügbarkeit nicht eingehalten werden kann, wird eine anteilige Entschädigung auf die folgende Rechnung gewährt. Diese beträgt maximal den Monatsbeitrag des zum Zeitpunkt des ersten Nichterreichens während der Service Level Periode gewählten Paketes.

7.2 System Monitoring

Die Crashtest Security GmbH überwacht den Zustand der Crashtest Security Suite um die Einhaltung des Service Levels zu überwachen.

7.3 Servicezeiten und Kontaktdetails

Die Servicezeiten der Crashtest Security GmbH sind Montag bis Freitag von 10:00 Uhr bis 17:00 Uhr. Während dieser Zeiten ist der Support auf folgenden Wegen erreichbar:

- Telefon: 089 / 21541665
- E-Mail: support@crashtest-security.com

Der telefonische Support steht nur Kunden eines bezahlten Paketes zu Verfügung.

Der Support ist auf Deutsch und Englisch verfügbar. Um eine Support-Anfrage zu stellen, muss die E-Mail-Adresse genannt werden, welche zur Anmeldung bei der Crashtest Security Suite verwendet wurde.