

Managed Web Application Vulnerability Scanning



Unsere Kunden wählen uns aufgrund unserer Fachkompetenz. Diese Stärke und unsere Erfahrungen sind in unseren Web Application Vulnerability Scanning Service eingeflossen. Mit modernen Tools zur automatischen Schwachstellen-Identifikation und mit manueller Analyse ist unser Service optimal um die Scanfrequenz von exponierten Web Applikationen zu erhöhen oder um Compliance-Anforderungen erfüllen zu können.

Unsere Scans werden alle einer manuellen Verifikation unterzogen, was wir als "teilautomatisierten Test" bezeichnen. Damit sind alle Ergebnisse immer False-Positive bereinigt und je nach Modul auch in einem definierten Umfang um False-Negativ (nicht identifizierte Schwachstellen) reduziert. So können wir sicherstellen, dass unsere und Ihre Qualitätsansprüche erfüllt werden.

Recurring Scan:

Der Service entfaltet seinen Mehrwert vor allem dann, wenn ein Kunde seine Applikationen regelmässig prüfen lässt. Aus diesem Grund ist die Basis des Service auf eine wiederkehrende Durchführung (Standard 2x pro Jahr) ausgelegt. Dadurch kann trotz einem reduzierten Testaufwand gegenüber einem vollwertigen manuellen Test, die Test Abdeckung (Coverage) mit jeder Durchführung erhöht werden. Dies weil nicht immer die gleichen Funktionalitäten geprüft werden. Dadurch reduziert sich automatisch die False-Negative Quote. Zudem kann die zwischenzeitliche Schwachstellen Behebung verifiziert werden.

Preise im Abo

Modul	Preis	Initialisierungsgebühr
M1-Anonym	495.-	250.-
M2-Opportunistic	695.-	250.-
M3-Balanced	1995.-	250.-
M4-Advanced	2995.-	250.-

Preise pro Modul und Scan. Im Abo fällt die Initiale Gebühr nur 1 mal an.

Unsere Preise sind ausgerichtet an Standardfunktionalitäten und der Komplexität von typischen Applikationen und einer wiederkehrenden Durchführung.

Mögliche Zusatzkosten	pro Scan
Umfangreiche Webseite	400.-
Einmalige Durchführung	350.-

Beachten Sie für weitergehende Tests auch die Hinweise auf unserer Website zum Unterschied von automatischen versus manuell durchgeführten Sicherheitsanalysen (Penetration Tests).

Sie erhalten

- Regelmässige Übersicht über mögliche Schwachstellen und deren Schweregrad für Ihre Web-Applikationen
- Sehr gute Test Möglichkeit oder als Ergänzung zu manuellen Penetration Test
- Erhöhung der Test-Frequenz gegenüber jährlichen Penetration Tests
- Kontinuierliche Sicherheits-Analyse (zur Erfüllung von Governance Anforderungen)

Ihr Vorteil

- Speziell auf Web-Applikationen und API ausgerichtetes Verfahren
- Basis-Informationen über das Sicherheitsniveau Ihrer Web-Applikationen
- Risiko Reduktionen dank erhöhter Test-Frequenz
- Weniger False-Positives
- Weniger False-Negative
- Standardisiertes Reporting
- Erfüllung von Compliance-Anforderungen
- Qualität und Preise wählbar

Sämtliche Preisangaben in CHF und exkl. MwSt.



Service Übersicht

Feature	M1- Anonym	M2- Opportunistic	M3- Balanced	M4- Advanced
Authenticated Scan		✓	✓	✓
Automated scan ¹	✓	✓	✓	✓
Manual testing	basic	basic	balanced	advanced
Manual False positive validation	✓	✓	✓	✓
Manual False negative reduction			✓	✓
Recurring tests - remediation verification	✓	✓	✓	✓
Recurring tests - coverage improvement			✓	✓
Supports Single Page Application			✓	✓
Supports API Checks			✓	✓
Supports MFA Authentication			✓	✓
Report per scan	✓	✓	✓	✓

Hinweis: Der manuelle Test-Aufwand beträgt pro Durchführung bei M3: 300 Minuten und bei M4: 600 Minuten.

1) Beachten Sie die definierten Rahmenbedingungen auf unserer Website für einen automatischen Scan. Falls eine automatische Prüfung nicht möglich ist, können nur Module M3, M4 durchgeführt werden.

Reporting

Der Report enthält die Resultate aus dem Scan, False-Positives bereinigten und um False-Negative identifizierte Schwachstellen und wird im PDF-Format bereitgestellt.

Scan Report of http://testphp.vulnweb.com

Contents

- SQL injection
 - 1.1. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 1.2. http://testphp.vulnweb.com/products.php [id parameter]
 - 1.3. http://testphp.vulnweb.com/products.php [id parameter]
 - 1.4. http://testphp.vulnweb.com/products.php [id parameter]
 - 1.5. http://testphp.vulnweb.com/products.php [id parameter]
 - 1.6. http://testphp.vulnweb.com/products.php [id parameter]
 - 1.7. http://testphp.vulnweb.com/products.php [id parameter]
 - 1.8. http://testphp.vulnweb.com/products.php [id parameter]
 - 1.9. http://testphp.vulnweb.com/products.php [id parameter]
- Out-of-band resource load (HTTP)
 - 2.1. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 2.2. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 2.3. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 2.4. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 2.5. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 2.6. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 2.7. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 2.8. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 2.9. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 2.10. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 2.11. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 2.12. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 2.13. http://testphp.vulnweb.com/artists.php [artist parameter]
- Cross-site scripting (reflected)
 - 3.1. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 3.2. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 3.3. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 3.4. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 3.5. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 3.6. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 3.7. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 3.8. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 3.9. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 3.10. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 3.11. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 3.12. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 3.13. http://testphp.vulnweb.com/artists.php [artist parameter]
- Flash cross-domain policy
 - 4.1. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 4.2. http://testphp.vulnweb.com/artists.php [artist parameter]
- Password field with autocomplete enabled
 - 5.1. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 5.2. http://testphp.vulnweb.com/artists.php [artist parameter]
- Unencrypted communications
 - 6.1. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 6.2. http://testphp.vulnweb.com/artists.php [artist parameter]
- File path manipulation
 - 7.1. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 7.2. http://testphp.vulnweb.com/artists.php [artist parameter]
- Path-relative style sheet import
 - 8.1. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 8.2. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 8.3. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 8.4. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 8.5. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 8.6. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 8.7. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 8.8. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 8.9. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 8.10. http://testphp.vulnweb.com/artists.php [artist parameter]
 - 8.11. http://testphp.vulnweb.com/artists.php [artist parameter]

Scan Report of http://testphp.vulnweb.com

Summary

Severity	High
Status	Already reported
Host	http://testphp.vulnweb.com
Path	/artists.php

Issue detail

The artist parameter appears to be vulnerable to SQL injection attacks. The payloads 0123456789 or 0123456789 and 0123456789 resulted in different responses.

Report Information

Date	16.04.2020
Employee	SPR
Host	http://testphp.vulnweb.com
Description	This is an automatically generated report. Manual false positive reduction done. Report contains only true positives.

Vulnerability Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organisation. Issues are also classified according to Status as 'New' and 'Already reported' with a recent managed scan.

Severity	Status		Total
	New	Already reported	
High	0	0	0
Medium	0	0	0
Low	0	0	0
Information	0	0	0

Classification: Confid

Report im PDF Format