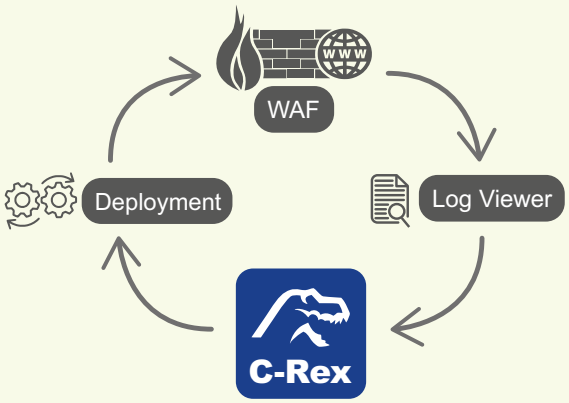
C-Rex by netnea
für die Payment Card Industry

Der Payment Card Industry Data Security Standard (PCI DSS) Version 4.0.1 beschreibt verschiedene Vorschriften über den Betrieb von Web Application Firewalls (WAFs) und den Schutz eigenentwickelter, öffentlich zugänglicher Web-Applikationen (public-facing web applications).

Seit 31.03.2025 ist der Betrieb von Web Applications Firewalls (WAFs) im Prevention oder Blocking Mode per Payment Card Industry Data Security Standard (PCI DSS) Version 4.0.1 im „Requirement 6: Develop and Maintain Secure Systems and Software“ vorgeschrieben.



§ Die Vorschrift

Requirement 6.4.2 beschreibt den Idealzustand:
Öffentlich zugängliche Web-Applikationen sind in Echtzeit vor bösartigen Angriffen geschützt.

Die Vorschrift konkretisiert:
Kontinuierlicher Betrieb einer „automatisierten technischen Lösung“, die fortlaufend überwacht und Web-basierte Angriffe vorbeugend verhindert.

Und präzisiert:
Aktiv und up to date
Generiert Audit Logs
Blockiert Web-Angriffe oder alarmiert
Die Alarme sind sofort zu überprüfen

Als „Good Practice“ schlägt sie beim Einsatz einer automatisierten technischen Lösung vor: Prozesse, die die zeitnahe Reaktion auf generierte Alarmmeldungen sicherstellen

Und sie zieht eine in Requirement 6.2.4 aufgestellte (nicht vollständige) Liste der Bedrohungen hinzu, gegen die die Lösung zu schützen hat.

Als technische Lösung ist eine Web Application Firewall (WAF) benannt.

Das Requirement beschreibt dazu detailliert, wie die Einhaltung zu überprüfen ist.

C-Rex

C-Rex by netnea
für die Payment Card Industry

X Die Schwierigkeit

Die Anforderung, Alarme sofort zu untersuchen und zu bearbeiten stellt Security-Teams vor große Herausforderungen, wenn deren Anzahl besonders hoch ist. Vor allem die Masse der False Positives verdeckt die Sicht auf die echten Angriffe und erschwert den Betrieb.

! Die Lösung

C-Rex identifiziert und behandelt Fehlalarme von ModSecurity-basierten WAFs effizient, automatisiert, schnell und zuverlässig. Und sie unterstützt bei der Anpassung der Regeln. C-Rex ist eine Suite von Tools zur Behandlung von False Positives mit folgenden Features:

- **C-Rex Fangs** erkennt False Positives durch einen ausgefeilten Filter Prozess.
- **C-Rex Arms** unterstützt durch ein intuitives Wizard-ähnliches GUI den Anwender, individuelle Fehlalarme zu behandeln.
- **Rule Exclusions** C-Rex unterstützt die vier klassischen Rule Exclusion Methoden mit einem einzigen Klick.
- **Integration** C-Rex arbeitet mit existierenden Log Viewern zusammen und fügt sich nahtlos in bestehende CI/CD Prozesse ein.
- **Parsing** C-Rex kann die vollständige Bandbreite aller ModSecurity-Warnmeldungen über verschiedene Versionen hinweg parsen.

Christian Folini rät:

Ein wichtiger Aspekt der PCI Spezifikation ist die Entwicklung sicherer Anwendungen. Das Ziel: Maßgeschneiderte und Individual-Software ist nicht durch Schwachstellen im Code angreifbar. Festgehalten ist das in Requirement 6.2.3.

Richtig eingesetzt dient die WAF als Unterstützung und zweite Sicherheitsschicht für die Produktionsumgebung, denn Software ist nie ganz fehlerfrei. C-Rex hilft bei der anstrengenden Arbeit mit der WAF und erlaubt den Entwicklern ohne tiefere WAF-Kenntnisse selbst mit den Alarmmeldungen umzugehen.

C-Rex

C-Rex by netnea
PCI Data Security Standard

Der Blick in den PCI Data Security Standard:

Seit dem 31.03.2025 ist das Requirement 6.4.2 des Payment Card Industry Data Security Standard (kurz PCI DSS) Version 4.0.1 – der Einsatz einer aktiven Web Application Firewall – nicht mehr Best Practice, sondern Vorschrift. Alarme sind sofort zu behandeln.

Requirement 6.2.4 spezifiziert eine (nicht vollständige) Liste der Angriffe, vor denen öffentlich zugängliche Web Applikationen (public-facing web applications) zu schützen sind.

Wir haben die beiden wesentlichen Requirements hier im Originaltext zitiert:

6.4.2
For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following:

- Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks.
- Actively running and up to date as applicable.
- Generating audit logs.
- Configured to either block web-based attacks or generate an alert that is immediately investigated.

Customized Approach Objective
Public-facing web applications are protected in real time against malicious attacks.

Applicability Notes
This new requirement will replace Requirement 6.4.1 once its effective date is reached. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Quelle: PCI DSS 4.0.1, Seite 150ff

6.2.4
Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following:

- Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.
- Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.
- Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.
- Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, clientside functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery(CSRF).
- Attacks on access control mechanisms, including attempts to bypass or ause identification, authentication, or authorization mechanisms, or attempts to exploit weaknessesin the implementation of such mecha nisms.
- Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

Quelle: PCI DSS 4.0.1, Seite 145

Die gesamte Spezifikation finden Sie hier:
https://www.pcisecuritystandards.org/

C-Rex

C-Rex by netnea
Ihre Ansprechpartner

Über netnea

netnea ist ein spezialisiertes Schweizer IT-Unternehmen mit Schwerpunkt auf Cybersicherheit und Netzwerk Monitoring. Als anerkannte Experten im Bereich Open-Source-Sicherheitslösungen hat netnea über 25 Jahre Erfahrung bei der Unterstützung von sicherheitssensiblen Unternehmen und Institutionen. netnea ist führend im Bereich WAF-Integration, Tuning von False Positives und der Schulung von Mitarbeitenden auf diesen Themen. Das Unternehmen steht für digitale Sicherheit auf höchstem Niveau.

Der Experte – Christian Folini

Zur Person:
LinkedIn Profil

Weil ihm False Positives schon immer ein Dorn im Auge waren, hat Dr. Christian Folini C-Rex entwickelt. Der Security Engineer ist Partner bei netnea. Er leitete mehrere Jahre das OWASP CRS Projekt. In seinen Schulungen vermittelt er das Know-how, um ModSecurity und CRS skalierend zu betreiben. Christian wurde als „OWASP Distinguished Lifetime Member“ ausgezeichnet.

Ihr Ansprechpartner – Alexander Glatzeder

Jetzt Termin vereinbaren

Zur Person:
LinkedIn Profil

Alexander Glatzeder, mit Sitz in Neuchatel in der Schweiz, ist seit mehr als zwanzig Jahren in der IT-Branche aktiv, seit 2015 als Director Sales bei freyraum marketing. Als Vertriebspartner unterstützt freyraum marketing netnea und deren Kunden bei Information, Beratung und Lizensierung von C-Rex.

Telefon:
+49 176 24471851

E-Mail:
alexander.glatzeder@freyraum-marketing.de

Mehr Informationen zu C-Rex finden Sie hier:
https://c-rex.netnea.com/

C-Rex