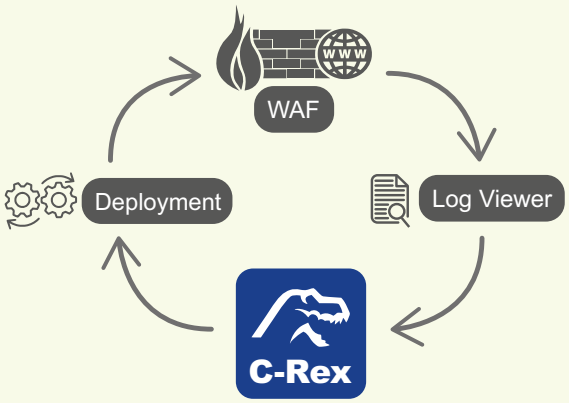
WAF Operations for PCI Companies – C-Rex by netnea

The Payment Card Industry Data Security Standard (PCI DSS) version 4.0.1 mandates that public-facing, custom-developed web applications be actively protected using automated technical solutions – such as a Web Application Firewall (WAF).

Since March 31, 2025, running WAFs in blocking mode is no longer optional. It's a formal compliance requirement:



§ Requirement 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.

Secure Development Backed by PCI DSS

Requirement 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 (e.g., SQL, LDAP, XPath)
- Buffer, pointer, and data structure manipulation
- Cryptographic implementation flaws
- Business logic attacks (e.g., API abuse, XSS, CSRF)
- Access control bypass
- Exploitation of high-risk vulnerabilities identified in Requirement 6.3.1
  (Source: PCI DSS 4.0.1, page 145)

WAFs are named explicitly as a technical safeguard against these attacks. C-Rex helps ensure that your WAF can fulfill this role – reliably and efficiently.

C-Rex

WAF Operations for PCI Companies – C-Rex by netnea

The Real-World Challenge

PCI DSS requires that alerts generated by the WAF be investigated immediately. In practice, this is difficult. Security teams are flooded with alerts – most of them false positives. These hide real threats and consume valuable resources.

To cope, many organizations either loosen WAF rules or run the WAF in monitoring-only mode. Both approaches contradict PCI DSS requirements and weaken your security posture.

The C-Rex Solution

C-Rex is a purpose-built tool suite that automates the identification and handling of false positives in ModSecurity-based WAFs. It ensures operational compliance without compromising application protection.

Features:

- **C-Rex Fangs**
  Intelligently detects false positives using a sophisticated filtering pipeline.
- **C-Rex Arms**
  A wizard-style interface that guides users – without requiring WAF expertise – through the process of reviewing and resolving alerts.
- **One-Click Rule Exclusions**
  Supports all four major rule exclusion techniques with minimal effort.
- **Integration**
  Seamlessly connects with your existing log viewers and CI/CD workflows.
- **Parsing**
  Handles all known ModSecurity alert formats across multiple versions.

Expert Advice: Dr. Christian Folini

A key aspect of PCI DSS is the development of secure software. The objective: custom-built applications must not be vulnerable to weaknesses in the code. This is defined in Requirement 6.2.3.

When used properly, the WAF acts as a critical second layer of protection in production environments – because no software is ever truly flawless. C-Rex eases the operational burden of WAF maintenance and empowers developers, even those without deep WAF expertise, to manage and respond to alert messages effectively.

C-Rex

C-Rex by netnea
PCI Data Security Standard

We quote the two key requirements in the original wording:

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.

Source: PCI DSS 4.0.1. page 150 ff

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.

Source: PCI DSS 4.0.1. page 145

Download the PCI DSS 4.0.1. Standard here:
https://www.pcisecuritystandards.org/

C-Rex

C-Rex by netnea
Meet the Experts

About netnea

netnea is a Swiss IT security company specializing in open-source cybersecurity and network monitoring solutions. With over 25 years of experience, netnea helps security-sensitive organizations deploy, operate, and optimize Web Application Firewalls – especially those based on ModSecurity and OWASP CRS. netnea is a recognized expert in WAF integration, false-positive tuning, and staff training, delivering digital security at the highest level.

Dr. Christian Folini – Creator of C-Rex

About:
LinkedIn Profile

Security engineer, CRS project lead, and OWASP Distinguished Lifetime Member. Christian brings 20+ years of experience in WAF tuning and cybersecurity best practices.

Alexander Glatzeder – Your Contact for Sales & Licensing

Book an appointment

About:
LinkedIn Profil

Director of Sales at freyraum marketing and C-Rex distribution partner. With over two decades in IT, Alexander supports companies across Europe in licensing C-Rex.

Phone:
+49 176 24471851

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

More about C-Rex:
https://c-rex.netnea.com/