jscrambler

Preparing Qualified Security Assessors for PCI DSS v4.0

The new requirements in PCI DSS v4.0 become mandatory April 1, 2025. Given the effort it takes to design, implement and possibly procure solutions, now is the ideal time for assessors to consider the implications and how companies can prepare.

Requirements **6.4.3** and **11.6.1** are designed to **detect and prevent e-commerce skimming attacks,** which account for more than 50% of breaches of cardholder data. Jscrambler **recently surveyed the top 20 e-commerce sites in the US** and found as many as 42 third-party domains receiving data from the payment page. Companies must gain visibility and control over this activity to protect data.

Requirement 6.4.3

Reduce the attack surface by ensuring that all JavaScript contained in a payment page is necessary, is included in an inventory, and has been explicitly approved. It also requires assurance of the integrity of all JavaScript.

Requirement 11.6.1

Detect tampering of JavaScript included in payment pages. It requires changes to scripts and page headers to be detected, and the appropriate alerts generated.

What about SAQ A Merchants?

The new requirements also apply to SAQ A merchants due to the increase in attacks via iframes, redirection, and hosted fields. In this scenario the payment page is the responsibility of the payment service provider or e-commerce gateway; the merchant has no payment page. However, the new version of SAQ A applies these requirements to the merchant's parent page that hosts the payment iframe(s) or redirects to a payment page.

Operationalization is key

When advising entities about meeting the new requirements, it is crucial to understand how a solution will be incorporated into existing workflows. For example, e-commerce websites are changed regularly so solutions like CSP or SRI may not be ideal. First, they require significant manual intervention. Second, they don't allow for fine-grained control, rather they may indiscriminately block legitimate transactions.

Automation for evidence collection is essential

It's also important to ensure that any solution provides the evidence an assessor needs to meet the testing requirements. The more manual a process is, the less likely it is to maintain the evidence that the assessor needs.

What are the options?

There are a few ways to meet these new requirements. These include:

- Traditional methods, like a combination of **Content Security Policy** (CSP), **Subresource Integrity** (SRI), and some simple scanning to detect changes;
- Monitoring from within content delivery networks;
- Comprehensive JavaScript security management solutions such as **Jscrambler's Webpage Integrity.**

Jscrambler protects payment pages

Webpage Integrity (WPI) is a comprehensive platform that enables entities to manage all the first and third-party JavaScript on any web page, including payment and parent pages.

1 Meets all documentation and workflow demands of requirement 6.4.3. and provides automatic assurance of all the JavaScript on a page.

2 Meets requirement 11.6.1 by generating an alert when anything changes. It also evaluates risk by determining whether any change altered the approved behavior of a script, or if the change needs to be manually reviewed and approved. This means that JavaScript management can be successfully operationalized, reducing the risk that authorized changes are inadvertently blocked or that inefficient processes are rejected by the business.

3 WPI goes beyond the requirements of PCI DSS v4.0 as it can be configured to automatically block any malicious script that tries to skim or interfere with the contents of payment fields.