jscrambler

PREPARING QUALIFIED SECURITY ASSESSORS FOR PCI DSS V4

The new requirements in PCI DSS v4 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 surveyed the **top 20 e-commerce sites in the US** and found as many as **42 third-party domains** receiving data from the payment pages. Companies must gain visibility and control over this activity to protect data.

Requirement 6.4.3
Reduce the attack surface by ensuring that an inventory of all scripts is maintained with written business or technical justification as to why each is necessary. 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.

Payment pages and SAQ A

Because of the increase in attacks against merchants outsourcing via iframes, redirection, and hosted fields, these new requirements apply to all parent pages - which means that directive is now not just in SAQ A but is applicable generally. Although the merchant is not responsible for meeting the requirements within the parent page that hosts the iframe(s) or redirection, they should get assurance that the Payment Processor / Payment Service Provider / E-commerce gateway is meeting the requirement.

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 J**scrambler's Webpage Integrity PCI DSS Module.**

Operationalization is the 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.

Evidence is also important

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.

How Jscrambler Webpage Integrity Helps Comply with PCI DSS v4

Jscrambler Webpage Integrity (WPI) offers a dedicated module designed to assist online businesses in meeting the rigorous requirements of PCI DSS 4 concerning the use of JavaScript within payment funnels.

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 as it can be configured to automatically block any malicious script that tries to skim or interfere with the contents of payment fields.

Support your assessment with a free Payment Page Analysis Report

The PCI DSS analysis report enables you to proactively assess client-side security risks across your clients' payment pages in preparation for PCI DSS v4 compliance. In other words, to understand which vendors or third-party tags are accessing sensitive payment page data.

What can you expect from our report?

- Visibility on how many vendors are on the payment page and who they are
- Understanding of which vendors or third-party scripts are accessing sensitive payment page data
- Getting to know which vendors are extracting customer data to outside domains
- Free consultation from our expert client-side protection team

Request your report