



PAYMENTS



SECURITY



COMPLIANCE



Payments
Security
Compliance

PCI DSS v.4.0 Evaluation

Page Shield Product

Version 1.0

11 September 2024



Sponsored by Cloudflare

Table of Contents

Executive Summary	3
Introducing Page Shield	4
Page Shield applicability to PCI DSS Requirements	10
Scope and approach for review	13
Evaluation and assessment methodology	14
PSC Conclusion	14
Disclaimer	14

Executive summary

This document is intended to be a product applicability guide that provides understanding and context regarding how Cloudflare Page Shield product can be utilized to meet the new requirements in Payment Card Industry Data Security Standard (PCI DSS) v4.0. In this regard, Cloudflare engaged Payment Security Compliance (PSC), a reputable PCI Qualified Security Assessor (QSA) company, to conduct a technical assessment of Page Shield and how it can be configured to meet PCI DSS requirements. This document summarizes PSC's findings and conclusion from its review of product functionalities and features of Page Shield. Page Shield is a Cloudflare product designed to help manage resources loaded by website visitors — including scripts, their connections, and cookies — and triggers alert notifications for security teams when resources change or are flagged as malicious. This document is intended to be read in conjunction with Cloudflare's PCI DSS Attestation of Compliance (AOC) and Responsibility Matrix¹.

Opinion from PSC

Cloudflare, the client, enlisted PSC as a Qualified Security Assessor Company (QSAC) in good standing. PSC's role was to analyze Cloudflare's Page Shield Product and assess the controls related to PCI DSS requirement 6.4.3 (Payment Page Security) and requirement 11.6.1 (Payment Page Notifications) to ensure alignment with the intent of the PCI DSS 4.0 standard.

PSC evaluated these requirements, and the resulting conclusions are outlined in the Page Shield PCI DSS v4.0 AOC. Cloudflare provides configuration recommendations for Page Shield in this document. Although Page Shield offers the necessary functionality to meet PCI requirements, each organization remains responsible for individual PCI DSS compliance.

¹ To download these documents refer to these [instructions](#).

Introducing Page Shield

Page Shield, which was generally available since 2021, is Cloudflare's response to the increasing threats loaded by consumers' browsers.² Backed by Cloudflare's threat intelligence and machine learning capabilities, Page Shield protects website visitors from client-side attacks that target vulnerable JavaScript dependencies and more.

Continuous Monitoring

Page Shield's monitoring functionality continuously captures JavaScript used across the entire website, and connections any of these JavaScript are making, beyond just payment pages. Various filters are available to narrow down to part of the website, or certain vendors or dependencies. To inventory dependencies given a moment in time, monitoring data can be exported in CSV format.

Security

Page Shield

Keep track of your application's JavaScript dependencies and receive alerts when they change.

[Page Shield documentation](#)

Monitors Policies Settings

Scripts Connections Cookies

Scripts that have been captured in the previous 7 days more than 3 times. Malicious scripts are shown first. To explore all scripts, click on View all.

+ Add filter		Download CSV View all	
Resource	Last seen	Last seen on	
Malicious https://examples.page-shield.workers.dev/cf-malicious-test-script-V3X.js	about 1 hour ago	https://demo.page-shield.theburritobot.com/malicious	
Malicious https://jsdelivr.at/estimate-shipping-methods.css	about 1 hour ago	https://demo.page-shield.theburritobot.com/	
https://cdnjs.cloudflare.com/polyfill/v3/polyfill.min.js	about 1 hour ago	https://demo.page-shield.theburritobot.com/malicious	

Figure: Monitor Dashboard

²<https://blog.cloudflare.com/automatically-replacing-polyfill-io-links-with-cloudflares-mirror-for-a-safer-internet/>

Monitored Scripts

Given a monitored script, an in-house built machine learning trained on data from Cloudflare's network examines whether its code is obfuscated and performs data exfiltration. A combination of these insights signals malicious behavior of a script. For malicious scripts or domains known from threat intelligence feeds, they are flagged and categorized right away.

Whenever a script's content is changed through comparing its Abstract Syntax Tree, a new version is recorded, and the new content will be examined by the machine learning model and compared against threat feeds for maliciousness.

Script Details

Malicious code ⓘ

93 (machine learning)

- 93 (obfuscation)
- 99 (exfiltration)

Malicious URL

Malicious domain

Malicious category

No

Yes

- Malware
- Security threats

Script URL

https://jsdelivr.at/estimate-shipping-methods.css

Copy

Last seen

10 minutes ago

Seen on host

demo.page-shield.theburritobot.com

First seen at

Mar 6, 2024 12:00:19 PM

Seen on pages

- /page-2
- /
- /payment

First seen on

/

Last 10 changed versions

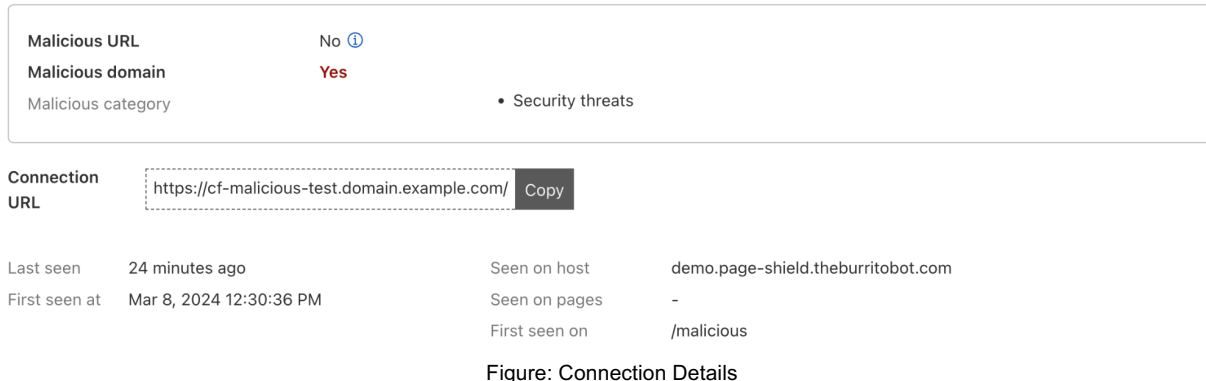
Seen at	Malicious code	Hash
July 17, 2024 12:02 PM	No, score 93	2f135aa00cf9f5f6ab21810d15d92867635d9b9a8e5f75faaae65566c5bba1b6
March 6, 2024 1:16 PM	No, score 93	55910eb57acdb7a180e5262c67fb30b3d9f734e23eaefb93268a726d16b38b2b

Figure: Scripts Details

Monitored Connections

For each captured connection used by any JavaScript, its URL and domain are checked against threat intelligence feeds to determine if the connection destination is deemed malicious – and thus should be refrained from data exchange.

Connection Details



For both monitored scripts and connections, metadata like timestamps and records of pages the script is used on, help determine whether a resource is still being actively used and where such resource can be tracked down to.

Script Classification through Machine Learning

In-house built machine learning classifies malicious scripts, especially Magecart-style scripts, through two key perspectives. Code obfuscation is a common technique used by malicious attackers to transform code into what is challenging to be analyzed. And data exfiltration scoring reveals how likely a script is trying to read user data and send to external destinations. A combination of both signals (the lower the score, the worse) indicate how likely a script is to be deemed as a Magecart-style attack.

Script Details

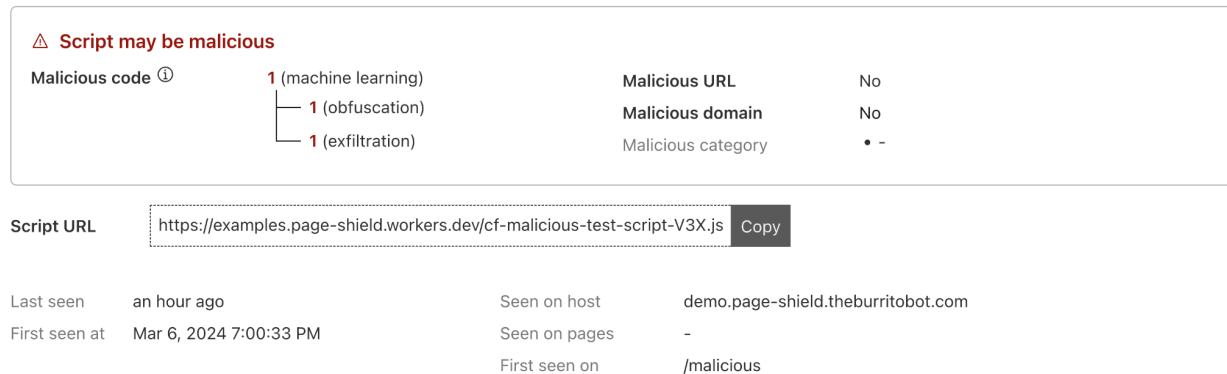


Figure: Malicious identification and scoring

Authorization with Policies

With monitored insights, Content Security Policies (CSPs) can be created to authorize resources to be allowed to run on a web application. Backed by the `Content-Security-Policy` header, various directives can be defined per policy, including but not limited to scripts and connections. Resources that are trying to be loaded but weren't allowed by a given policy will be reported back and visualized in the dashboard.

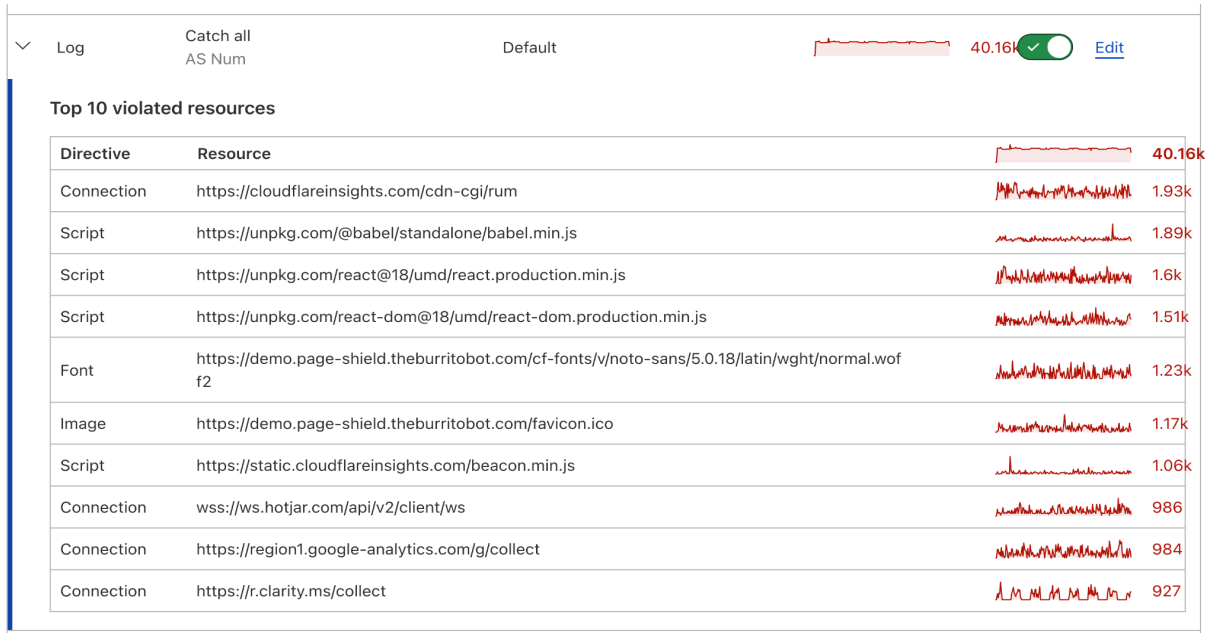


Figure: Policy Violations

Creating a policy for scripts and connections is made simpler with continuously monitored insights. A list of resources is available starting from the top-level domain down to individual resource seen. This policy builder supports a flexible approach of defining resources to be allowed, a script path, a vendor's domain name, or even a script's exact content hash value.

Allow these directives...

The resources listed below are based on reports received in the past 7 days. You can refresh suggestions based on the conditions above.

Scripts

Delete

[+ Add source](#)
[↻ Refresh suggestions](#)

☐ none
 ☒ self
 ☐ unsafe inline
 ☐ unsafe eval()

☒ sha256-Cz0biosN42V+4raM8E6Ms4276K60sjcod3TCOnWdU0=

>

cloudflare.com (4)

▼

cloudflareinsights.com (4)

☐ *.cloudflareinsights.com

▼

static.cloudflareinsights.com (2)

☒ https://static.cloudflareinsights.com/beacon.min.js
 ☐ *.static.cloudflareinsights.com

▼

googletagmanager.com (5)

☐ *.googletagmanager.com

>

www.googletagmanager.com (3)

▼

jquery.com (4)

☐ *.jquery.com

▼

code.jquery.com (2)

☐ https://code.jquery.com/jquery-3.7.1.slim.min.js
 ☐ *.code.jquery.com

>

stripe.com (4)

Scripts directive preview

```
script-src 'self' 'sha256-Cz0biosN42V+4raM8E6Ms4276K60sjcod3TCOnWdU0='
https://static.cloudflareinsights.com/beacon.min.js googletagmanager.com ;
```

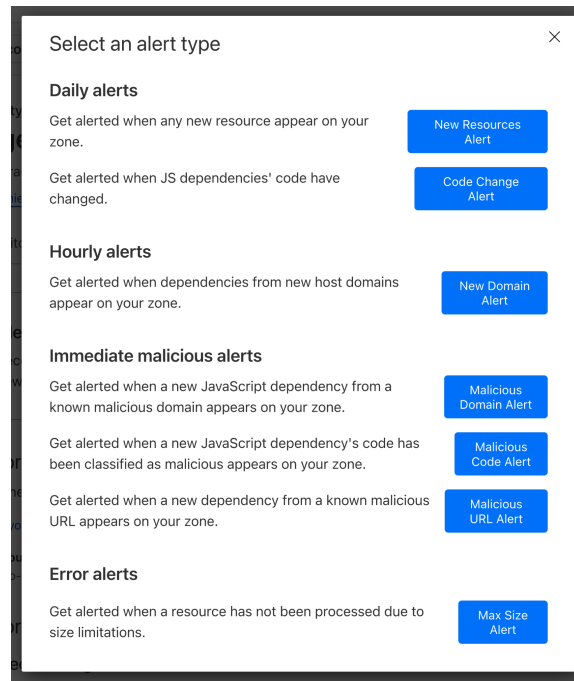
Figure: Policy configuration using script hash

© COPYRIGHT PSC, INC. 2024, ALL RIGHTS RESERVED.

8

Malicious and Code Change Alerting

With continuous monitoring, implementing organizations will be notified when code change is detected, or a malicious script is found. These alerts are delivered through the Cloudflare platform shared notification service in the format of emails or webhook messages.



Select an alert type

Daily alerts

- Get alerted when any new resource appear on your zone. **New Resources Alert**
- Get alerted when JS dependencies' code have changed. **Code Change Alert**

Hourly alerts

- Get alerted when dependencies from new host domains appear on your zone. **New Domain Alert**

Immediate malicious alerts

- Get alerted when a new JavaScript dependency from a known malicious domain appears on your zone. **Malicious Domain Alert**
- Get alerted when a new JavaScript dependency's code has been classified as malicious appears on your zone. **Malicious Code Alert**
- Get alerted when a new dependency from a known malicious URL appears on your zone. **Malicious URL Alert**

Error alerts

- Get alerted when a resource has not been processed due to size limitations. **Max Size Alert**

Figure: Alerts configurable for Page Shield

Page Shield applicability to PCI DSS Requirements³

With the changes in the PCI DSS standards, Page Shield is positioned to help organizations meet these new requirements:

Requirement 6.4.3

Defined Requirement

All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:

- A method is implemented to confirm that each script is authorized.
- A method is implemented to assure the integrity of each script.
- An inventory of all scripts is maintained with written justification as to why each is necessary.

The purpose of this new requirement is to ensure that unauthorized code cannot be present in the payment page as it is rendered in the consumer's browser.

Requirement 11.6.1

Defined Requirement

A change- and tamper-detection mechanism is deployed as follows:

- To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the security-impacting HTTP headers and the script contents of payment pages as received by the consumer browser.
- The mechanism is configured to evaluate the received HTTP headers and payment pages.
- The mechanism functions are performed as follows:
 - At least weekly, OR
 - Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).

The purpose of this requirement is to ensure that e-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.

³ Page Shield features are available through different subscription plans. Organizations intending to use Page Shield for PCI DSS compliance must ensure that the necessary features are available in their subscription.

Mapping of Page Shield Features to Requirements

The following content provides a mapping of Page Shield features and guidance on how organizations can configure Page Shield.

PCI DSS Requirement 6.4.3

A change- and tamper-detection mechanism is deployed as follows:

Defined Requirement	Feature	Guideline on how requirements can be met
A method is implemented to assure the integrity of each script.	Page Shield Policies	<p>Deploy policies on payment pages, based on monitored data suggestions, and/or hashes of inline scripts and third-party scripts.</p> <p>Implementing organizations can create ALLOW policies to define a positive security model, also known as positive blocking. According to this model, organizations can define selected JavaScript to run on the payment pages and deny-by-default any JavaScript's not explicitly allowed.</p>
	Malicious Script Detection	<p>Implementing organizations can configure CSP directives to meet this requirement. Configuring hash-based policies/directives provides a more effective way for validating script integrity.</p> <p>Reviewing alerts and violation reports based on hashes of inline and third-party scripts and incorporating organizations' own change management processes can help detect any unauthorized/change tampering.</p>
	Role Based Access	<p>Ensure that Malicious Resource Detection is enabled in the implementing organization's zone and set up an alert for malicious code detection.</p> <p>Cloudflare's Page Shield offers fine grained permission control per zone (website), so organizations can configure and assign only specific authorized individuals to have write and edit permissions to edit CSP directives. This provides them a preventive method to manage HTTP headers.</p> <p>Organizations are responsible for configuring user roles and permissions for accessing Page Shield.</p>
An inventory of all scripts is maintained with written business or technical justification as to why each is necessary.	Script Monitor	<p>The Monitor's dashboard will show which resources (scripts and connections) are running on your domain. Organizations can filter the data in these dashboards using different criteria and print a report with the displayed records.</p>

Defined Requirement	Feature	Guideline on how requirements can be met
	Export Data Feature	Use this feature to extract data from Page Shield that you can review and annotate. The data in the exported CSV file will honor any filters you configure in the dashboard.
		<p>Organizations are responsible for implementing approval processes and documentation on the scripts as part of their change management processes. To maintain the integrity of the inventory, organizations should review alerts for new resources, scripts and code changes.</p> <p>Organizations would need to print the report and/or export the scripts report and document/link necessary resources to their business and technical justification documentation.</p>

PCI DSS Requirement 11.6.1

A change- and tamper detection mechanism is deployed as follows:

Defined Requirement	Feature	Guideline on how requirements can be met
To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.	Page Shield Alerts (New Resource, Code Change, Malicious Resource)	<p>Using the change code alert, new resource alert and new malicious script alert, organizations can identify and be notified of new scripts/resources that are being loaded to the consumer browser or are considered malicious. Organizations are responsible for configuring these alerts.</p> <p>Organizations should review and validate whether the new resources and code changes to the scripts are authorized and have undergone their own change management processes. Accordingly, they can update the ALLOW policies enabled.</p> <p>Organizations should incorporate these alerts into their security events and incident response processes.</p>
	CSP Violations Log Push	<p>Violated resources will be blocked by the Policy and get reported back in real-time for further review through the dashboard. Organizations can use Log Push to send these violation logs to various destinations including their SIEM.</p> <p>Allowed resources are constantly being checked for changes and malicious behaviors and organizations can configure these alerts.</p>

Defined Requirement	Feature	Guideline on how requirements can be met
	Audit logs for CSP changes (Q3)	Review audit logs for Page Shield configuration changes. These audit logs can be pushed to implementing organizations designated SIEM (through Log Push) where organizations can configure tailored detection and alerting for unauthorized modifications.
The mechanism is configured to evaluate the received HTTP header and payment page.	Page Shield Policies Script Monitor	<p>Page Shield Policy and Script monitor both evaluate HTTP header (through CSP/SRI) and payment page (script monitor).</p> <p>Organizations are required to configure Page Shield Policies and monitoring policies tailored for their environment and approach.</p> <p>Deployed Page Shield Policy enforces JavaScript behaviors and can only be changed by users with write permission.</p> <p>Violated resources will be blocked by the Policy and get reported back in real-time for further review. Allowed resources are constantly being checked for changes and malicious behaviors.</p>
The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	Script Monitor Page Shield Policies	<p>The Monitor dashboard provides real time monitoring. However, whilst monitoring is done continuously and findings are available through the Monitor dashboard, some notifications and alerts relevant to PCI DSS are sent daily.</p> <p>Violation reports of deployed Policy can be log pushed to various destinations.</p>

Page Shield features are available through different subscription plans. It should be noted that simply enabling Page Shield or subscribing to different plans and features will not result in PCI DSS compliance; organizations must configure their use of Cloudflare's products and features in a way that it meets the defined requirements or customized approach objective whilst effectively managing their threats.

Scope and approach for review

PSC thoroughly assessed Cloudflare's dashboard offerings, specifically focusing on the Page Shield product. The scope of Page Shield encompasses the necessary functionality to secure payment pages

from exploitation via malicious scripts. To maintain integrity and authorization, organizations can configure policies for hash validation and page monitoring. Additionally, the “Monitor” dashboard within Page Shield provides an active inventory of running scripts, allowing for easy export and retention management.

Regarding change- and tamper-detection, PSC examined the deployed mechanism to alert personnel about unauthorized modifications to HTTP headers and payment page content. The Page Shield monitor dashboard allows organizations to configure alert mechanisms, evaluating payment page scripts at their desired frequency.

Evaluation and assessment methodology

The PCI DSS establishes fundamental technical and operational requirements to safeguard account data. Although originally tailored for environments with payment account data, PCI DSS can also enhance security across other aspects of the payment ecosystem. PSC assessed the applicability of specific requirements for payment page security using the PCI DSS v4.0 assessment process, focusing on requirements 6.4.3 and 11.6.1.

PSC Conclusion

After analyzing Cloudflare’s Page Shield product, PSC has determined that Cloudflare customers can meet PCI DSS requirement 6.4.3 (Payment Page Security) and Requirement 11.6.1 (Payment Page Notifications) by configuring the Page Shield product appropriately. The scope for Page Shield is defined by Cloudflare, and while the functionality for PCI DSS requirements is available, customers using Page Shield are responsible for configuring the product according to Cloudflare’s recommendations.

Disclaimer

This document serves solely for informational purposes. It is offered as a courtesy to assist customers in evaluating the applicability of Cloudflare products to meet PCI DSS compliance requirements. Importantly, this document does not replace or overlap with Cloudflare’s PCI DSS Attestation of Compliance (AOC). Further, the content in this document reflects the current product features and offerings as of the document’s issuance date, subject to potential changes without prior notice. Because of inherent limitations, even upon completion of our work PSC may not identify all security or compliance issues. Furthermore, the projection of any conclusions based on the findings and opinion in this report to future periods is subject to the risk that (1) changes made to this product, or other related systems, processes or controls, (2) changes in processing requirements, or (3) degree of compliance with related policies or procedures may alter the validity of such conclusions.

Customers bear the responsibility of independently assessing the information in this document and determining whether Cloudflare’s products or services align with their regulatory, compliance, and

operational requirements. Additionally, customers must configure Cloudflare offerings to meet these specific needs.

Notably, this document does not establish any warranties, representations, contractual commitments, conditions, or assurances from Cloudflare, its affiliates, suppliers, or licensors. The rights, obligations, and liabilities between Cloudflare and its customers are governed by separate agreements. This document does not alter or modify any existing agreement between Cloudflare and its customers.