The rise and risk of third-party scripts in modern websites

An excerpt from the 2024 Verizon Payment Security Report

September 2024

A Verizon Business Cyber Security Consulting and Source Defense publication

verizon business

Appendix A: The rise and risk of third-party scripts in modern websites

By Stephen Ward
Chief Marketing Officer
Source Defense

Cyber adversaries increasingly are targeting third-party scripts to steal data at the point of input. This term spotlights the shift in focus from traditional data targets—data in transit or at rest—to the point where users first input their data. Attackers exploit vulnerabilities in third-party scripts to inject malicious code, which enables them to capture data as soon as it's entered into the online forms that power e-commerce. These attacks are referred to as Magecart, e-skimming, digital skimming, clickjacking, credential harvesting and other terms, but they are all synonymous with a major threat confronting consumer personally identifiable information (PII), credentials and payment card data.

The ability of cybercriminals to target this data in real time, exposing potentially billions of online consumer sessions to their illicit activities, stems from the evolution of the modern website and a fundamental weakness in website design, security and third-party risk management. JavaScript powers the vast majority of the world's websites. The JavaScript powering these sites increasingly comes from third-party digital supply chain partners, whose code is neither vetted by website owners nor controlled by them with any regularity.

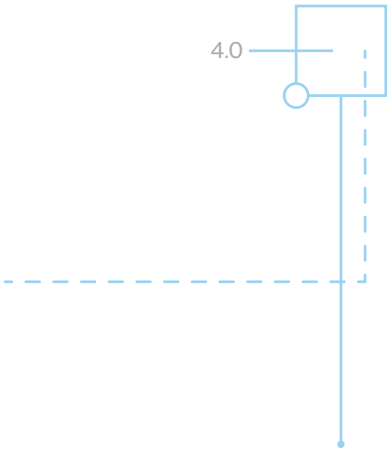
Requirements 6 and 11 and scripts

New updates to Requirements 6 and 11 in the Payment Card Industry Data Security Standard (PCI DSS) include a requirement to inventory, authorize, monitor and secure scripts running on payment pages and within payment flows. Monitoring the script behavior and preventing unauthorized access to this sensitive data is key to meeting PCI DSS v4.0x[1] compliance. In addition, National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 has clear directives to inventory third-party services, understand data access and flows between those third parties, and guide organizations to mitigate and manage data loss incidents. Both frameworks highlight the critical blind spot third- and fourth-party scripts represent in safeguarding online transactions and user data against cyberthreats.

The modern website now has its own third-party supply chain. Source Defense's comprehensive analysis of more than 7,000 of the world's largest merchant websites reveals a disconcerting landscape dominated by third- and fourth-party scripts, with a staggering 129,897 scripts identified. These scripts, often embedded within payment pages and directly interacting with PII and payment data, underscore a significant cybersecurity and payment security vulnerability.

Specifically, 51,968 scripts were found on payment pages (40% of the total observed), 17,002 were accessing PII, and thousands more were handling sensitive payment and credentials data. The findings highlight a pervasive oversight.

They show an average of more than 18 scripts per page—with a distinction between third- and fourth-party contributions—further highlighting the extent of potential exposure. This represents a 50% increase in script use compared to our previous findings, which underscores the urgent need for enhanced scrutiny and strategic oversight within digital security frameworks.



1 The "x" designates any incremental or future versions of the PCI Data Security Standard.

New updates to PCI DSS include a requirement to inventory, authorize, monitor and secure scripts running on payment pages and within payment flows. Monitoring the script behavior and preventing unauthorized access to this sensitive data is key to meeting PCI DSS v4.0x compliance. In addition, NIST CSF 2.0 has clear directives to inventory third-party services, understand data access and flows between those third parties, and guide organizations to mitigate and manage data loss incidents. Both frameworks highlight the critical blind spot third- and fourth-party scripts represent in safeguarding online transactions and user data against cyberthreats.

The evolution of third-party scripts

The inception of third-party scripts dates back to the early days of web development, when the need for dynamic content and functionality led to widespread adoption. Initially, these scripts were simple tools for enhancing website aesthetics or tracking basic user interactions. As the internet matured, so did the complexity and capabilities of these scripts, evolving into sophisticated tools integral to e-commerce, social media and data analytics.

Today, third-party scripts are indispensable, powering everything from chatbots and payment gateways to analytics and advertising tools. Scripts can help businesses better understand their customers and tailor their offerings accordingly. However, this reliance poses significant security challenges. These scripts, by nature, can access, modify and transmit sensitive user data, making them prime targets for cyber adversaries. The data compiled and analyzed by Source Defense shows the alarming prevalence of unsecured third- and fourth-party scripts across various industries.

Several high-profile breaches over the years highlight the critical need for robust security measures for third-party scripts, particularly those handling sensitive user data, such as a:

- **Large children's apparel retailer (2019):** Threat actors compromised the merchant website by inserting malicious code that skimmed customer financial details directly from the payment process. The breach potentially exposed customer names, shipping and billing addresses, payment card numbers, card verification value (CVV) codes, and expiration dates.
- **Global airline (2018):** A breach occurred through malicious third-party scripts on the airline's website. Attackers injected code to capture customer data during payment, affecting 380,000 transactions. This breach highlighted the vulnerabilities in scripts managing sensitive data, leading to significant financial penalties and reputational damage.
- **Ticket sales and distribution company (2018):** The company website was compromised through a third-party chatbot script. The breach exposed the personal and payment information of thousands of customers.

Percentage of scripts on payment pages, accessing PII data, accessing payment data or accessing credentials

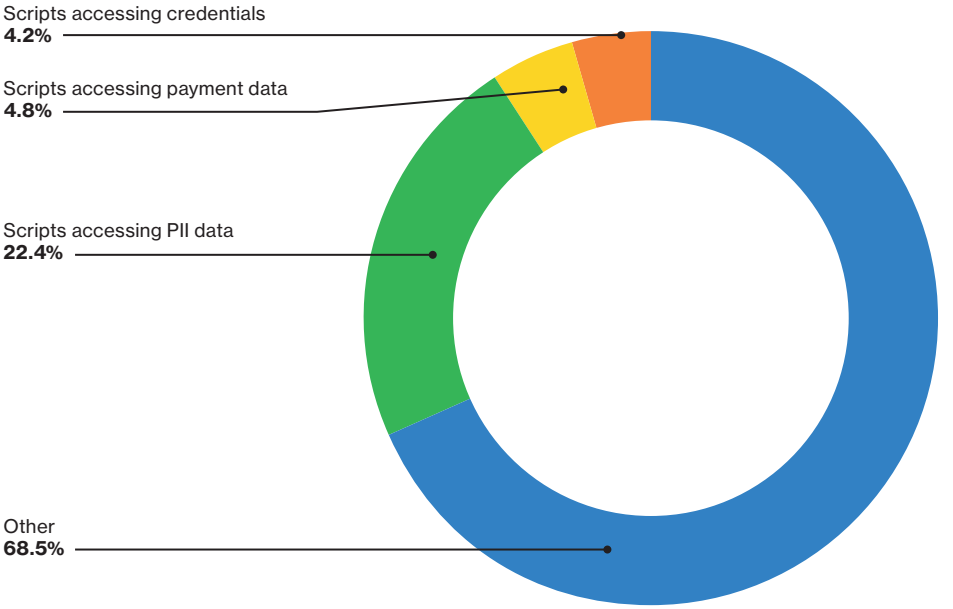


Figure 34. 7,075 unique websites from 6,342 companies

Visa's biannual report continues to highlight the threat of e-skimming, reporting that, "The targeting of eCommerce platforms and third-party code integrations are among the most common tactics utilized by threat actors ... threat actors are targeting supply chains and third-party service providers with high frequency and exhibiting continued interest in payment account data and personally identifiable information."[2] The security firm Recorded Future found that 1,520 unique malicious domains were involved in the infections of 9,290 unique e-commerce domains at any point in 2022.[3] And as late as January 2024, Europol disrupted an organized e-skimming operation that was impacting hundreds of European Union merchants and millions of consumers.[4]

Recommended reading: "Biannual Threats Report," Visa, December 2023. https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/pfd-biannual-threats-report-december-2023.pdf

Changes to safeguard scripts

The new requirements in the PCI DSS recognize this evolving threat and the critical role of script management in safeguarding payment data. Compliance now requires a proactive approach to script security to protect against data breaches. This includes implementing robust monitoring and control measures to ensure that scripts do not become a weak link in payment card data security.

Different approaches can be taken to mitigate the risks associated with third-party scripts. Subresource integrity (SRI) checks can help prevent tampering with a script, while content security policies (CSPs) can restrict which scripts run on a webpage. Proprietary script management solutions, such as the pioneering Source Defense platform, offer another option by providing a comprehensive framework for managing and securing scripts.

Script mitigation strategies

Script security will likely expand as the digital landscape evolves. Future changes may include a greater emphasis on behavioral-based assessment and authorization of scripts. This could involve analyzing the behavior of scripts in real time to detect and block potentially malicious activity.

The rise of third-party scripts has brought with it new challenges and risks. However, by understanding these risks and implementing effective mitigation strategies, organizations can harness the benefits of third-party scripts without compromising security or privacy.

The most effective approach to third-party script management and security involves real-time monitoring and control. This method includes proactively identifying and mitigating threats and ensuring that script vulnerabilities are addressed promptly. This approach bolsters web application security by focusing on preemptive defenses and aligns with data protection standards, safeguarding sensitive customer data against potential cyberthreats.

Third-party scripts are a game-changer in web development, offering unparalleled functionality. But the security challenges are massive. Protecting data at the point of input is a critical step in addressing these challenges.

2 "Biannual Threats Report," Visa, June 2022. https://usa.visa.com/content/dam/VCOM/regional/na/us/run-your-business/documents/biannual-threats-report.pdf

3 "Annual Payment Fraud Intelligence Report: 2022," Recorded Future, January 17, 2023. https://www.recordedfuture.com/annual-payment-fraud-intelligence-report-2022

4 "Action against digital skimming reveals 443 compromised online merchants," Europol, December 22, 2023. https://www.europol.europa.eu/media-press/newsroom/news/action-against-digital-skimming-reveals-443-compromised-online-merchants

Data findings summary report

Generally, a strong correlation exists between how customizable a product or service offering may be and the utilization of scripts on the websites that sell them. This makes sense because many scripts in use today relate to customization, suggestions to consumers on additional products, and shopping cart value enhancement and conversion.

High volume of scripts in certain industries: The apparel and fashion industry leads with a significantly higher volume of scripts than other industries, indicating a heavy reliance on third-party services for analytics, marketing, customer engagement and e-commerce functionalities. This suggests that industries with a strong online retail presence tend to integrate more third-party scripts to enhance user experience and drive sales, but at the potential cost of increased exposure to security vulnerabilities.

Widespread use of third-party services: The presence of third-party scripts across various industries highlights the reliance on external services for a wide range of functionalities, including analytics, payment processing, marketing and customer support. While these services can provide valuable insights and capabilities, they also introduce potential risks because each script represents a vector through which data breaches or leaks can occur if not properly managed.

Most prevalent script categories

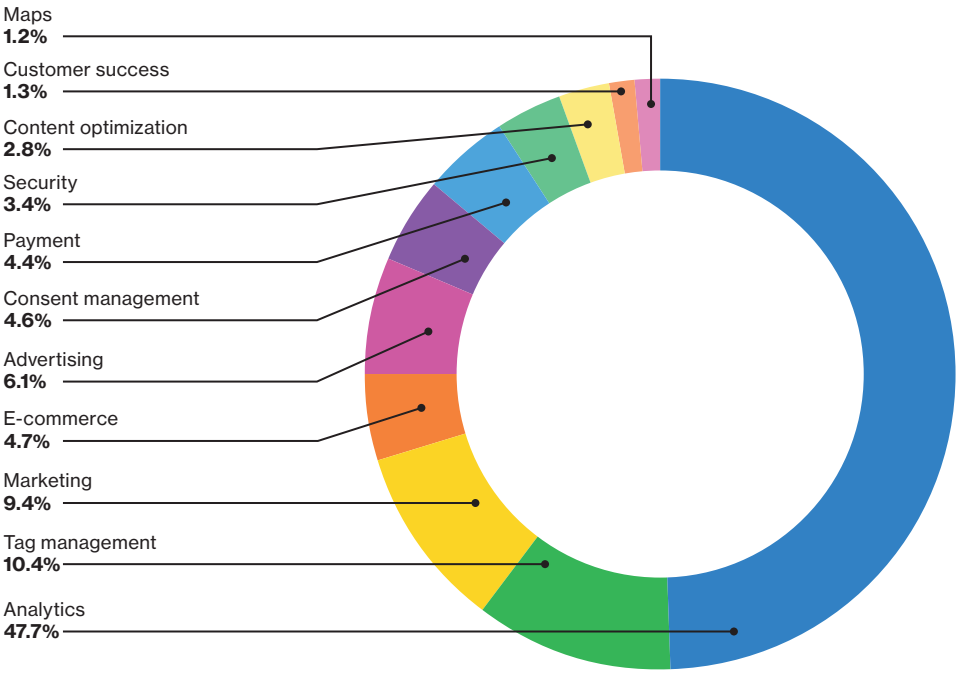


Figure 35. 7,075 unique websites from 6,342 companies

Potential security risks: The accessing of PII, payment data and credentials through scripts poses significant security risks, especially if the scripts are from third-party sources. Each script with access to sensitive data increases the attack surface for potential exploitation by malicious actors. Industries with high numbers of such scripts need to implement robust security measures to protect against data breaches, cross-site scripting (XSS) attacks and other vulnerabilities.

Need for rigorous security policies and practices: The data underscores the importance of implementing rigorous security policies and practices—including regular audits of third-party scripts, ensuring compliance with data protection regulations (such as the General Data Protection Regulation [GDPR] and the California Consumer Privacy Act [CCPA]), and adopting secure coding practices. Industries must prioritize data privacy and security by vetting third-party vendors, using CSPs to restrict script sources and employing data encryption in transit and at rest.

Client-side security solutions: There's a clear need for advanced client-side security solutions, such as real-time monitoring tools, that can detect and mitigate threats posed by third-party scripts.

Consumer awareness and transparency: The extensive use of scripts that access sensitive information calls for greater consumer awareness and transparency from companies about how data is collected, processed and stored. Providing clear, accessible privacy policies and offering users control over their data can help build trust and ensure compliance with privacy standards.

PCI DSS v4.0 implications of findings

The PCI DSS ensures that all companies that accept, process, store or transmit payment card information maintain a secure environment. The introduction of PCI DSS v4.0 brings more robust security measures and flexible compliance strategies to adapt to the evolving payment security landscape. Given the analysis of script usage across various industries, particularly those accessing PII, payment data and credentials, several implications are worth highlighting.

Increased scrutiny on third-party service providers

The reliance on third-party scripts, especially in industries such as apparel and fashion, which showed the highest volume of scripts accessing sensitive data, underscores the need for rigorous vendor management policies under PCI DSS v4.0. The PCI standard requires that entities maintain and manage a list of service providers with access to cardholder data (CHD), including the nature of the services provided and the responsibility for securing CHD. Given the analysis, businesses must ensure that their third-party scripts and service providers adhere to PCI DSS requirements to prevent data breaches and ensure compliance.

Enhanced focus on security of payment page scripts

The significant number of scripts accessing payment data indicates a potential risk area for PCI DSS compliance. Under PCI DSS v4.0, there is an enhanced focus on protecting the cardholder data environment (CDE) against unauthorized access, including client-side attacks such as formjacking and e-skimming. Companies must implement strong controls over scripts running on payment pages and within payment flows, with additional requirements to inventory, authorize, ensure integrity, turn on alerts and block all malicious activity related to these scripts.

Requirement for advanced monitoring and detection

With the high volume of scripts accessing sensitive data, the need for advanced monitoring and detection mechanisms is imperative to identify and mitigate threats in real time. PCI DSS v4.0 emphasizes the importance of promptly detecting and responding to security incidents. Businesses must deploy solutions capable of monitoring script behavior on client-side web applications, detecting anomalies and preventing data exfiltration attempts by malicious scripts.

Data protection and encryption

The analysis revealed that scripts are accessing a wide range of sensitive data, including PII, payment data and credentials. PCI DSS v4.0 mandates the encryption of transmission of CHD across open, public networks. This extends to ensuring that any script or service that handles CHD must also employ strong encryption methods to protect data in transit and at rest, aligning with the PCI standard's requirements for robust encryption and key management practices.

Impact on risk assessment and mitigation strategies

Given the widespread use of scripts across industries, PCI DSS v4.0 requires entities to perform regular risk assessments to identify vulnerabilities within their payment processing systems, including those introduced by third-party scripts. The data highlights the need for a comprehensive risk management strategy that considers the variety of scripts accessing sensitive data, evaluating their necessity and implementing appropriate controls to mitigate identified risks.

Conclusion

In conclusion, the extensive use of third-party scripts across various industries, particularly those handling sensitive payment information, has significant implications for PCI DSS v4.0 compliance. Businesses must adopt a proactive approach to managing third-party risks, securing payment pages and payment flows, implementing advanced monitoring and detection capabilities, ensuring data protection, and conducting thorough risk assessments to maintain compliance with PCI DSS v4.0. Failure to address these issues not only poses a risk to data security but also jeopardizes an organization's compliance status, potentially leading to fines, reputational damage and loss of customer trust.

Source Defense data analysis findings

In the first quarter of 2024, Source Defense conducted its analysis and found:

- 7,075 unique websites from 6,342 companies
- Total number of third- and fourth-party scripts: 129,897
- Total number of scripts found on payment pages: 51,968
- Total number of scripts accessing PII: 17,002
- Scripts accessing payment data: 3,636
- Scripts accessing credentials data: 3,222
  - Average number of scripts per page: 18.37 (representing a 50% increase in script utilization since our 2023 analysis)
  - Average number of third-party scripts per page: 13.08
  - Average number of fourth-party scripts per page: 8.32 (previous data indicated two fourth parties—we are now seeing a fourfold increase)
  - Average number of scripts accessing PII: 2.40
  - Average number of scripts accessing payment data: 0.51

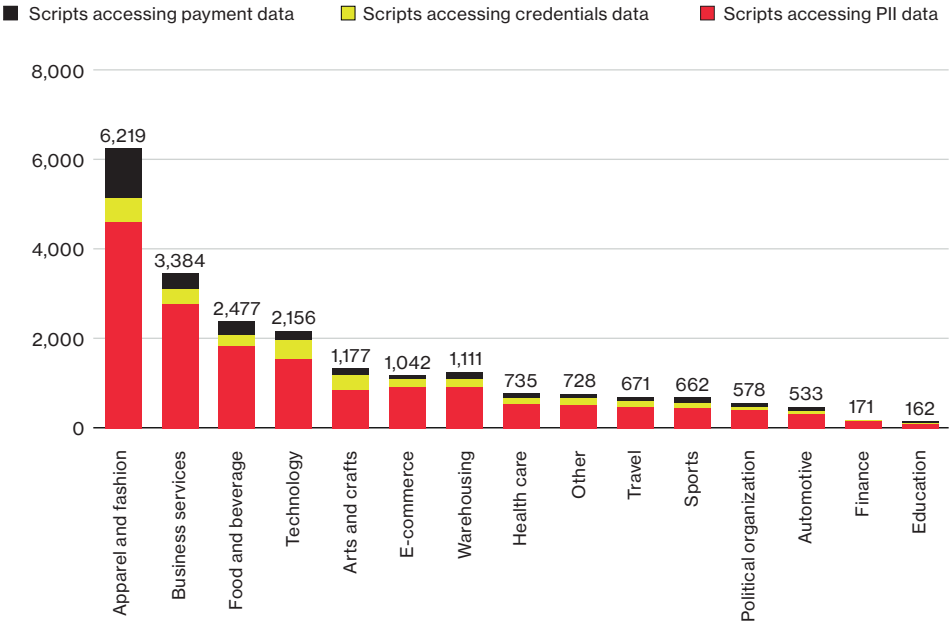


Figure 36. Number of web pages with scripts accessing PII, credentials and payment data

Most prevalent script types

The total number of script type occurrences is 36,356. The following script types, along with their percentage of the total, are arranged from highest to lowest:

1. Facebook Connect: 15.82%
2. Google Global Site Tag: 15.48%
3. Google Tag Manager: 15.47%
4. Google Analytics: 10.61%
5. Optanon: 6.32%
6. Pinterest Conversion Tracker: 5.98%
7. Universal Event Tracking (Bing): 5.32%
8. Klaviyo: 4.61%
9. Google Analytics—E-commerce: 4.51%

These script types are the most common in the dataset, indicating their widespread use across the analyzed websites. The presence of multiple analytics and tracking scripts (e.g., from Google, Facebook and Pinterest) suggests a strong focus on data collection and analysis in online platforms.

Top 15 industries overview ranked by total number of such scripts

1. Apparel and fashion | Total scripts: 81,850 (63% of the total, yet represented only 29% of the industry dataset); script origins include various analytics, marketing and customer engagement tools
2. Technology | Total scripts: 30,827 (24% of the total, yet represented only 14% of the industry dataset); script origins feature a mix of analytics, development tools and security services
3. Food and beverage | Total scripts: 27,518 (21% of the total, yet represented only 9% of the industry dataset); script origins include content delivery networks, marketing platforms and social media integrations
4. Business services | Total scripts: 23,629 (18% of the total, yet represented only 11% of the industry dataset); script origins range from customer relationship management to business analytics tools
5. Arts and crafts | Total scripts: 16,944 (13% of the total, yet represented only 7% of the industry dataset); script origins feature e-commerce platforms, analytics and marketing automation tools
6. E-commerce | Total scripts: 12,945 (10% of the total, yet represented only 6% of the industry dataset); script origins include payment processors, marketing tools and analytics services
7. Sports | Total scripts: 10,907 (8% of the total, yet represented only 5% of the industry dataset); script origins feature a mix of analytics, marketing and customer service tools
8. Warehousing | Total scripts: 9,420 (7% of the total, yet represented only 3% of the industry dataset); script origins include logistics and supply chain management tools, along with analytics
9. Travel | Total scripts: 8,191 (6% of the total, representing 3% of the industry dataset); script origins range from booking engines to customer feedback and analytics tools
10. Automotive | Total scripts: 7,030 (5% of the total, representing 3% of the industry dataset); script origins include dealer management systems, analytics and customer engagement platforms
11. Other | Total scripts: 6,678 (5% of the total); script origins feature a diverse range of tools tailored to specific industry needs
12. Health care | Total scripts: 4,431 (3% of the total, representing 2% of the industry dataset); script origins include patient management systems, analytics and health care compliance tools
13. Political organization | Total scripts: 4,217 (3% of the total, representing 2% of the industry dataset); script origins range from campaign management to voter engagement and analytics tools
14. Education | Total scripts: 2,243 (2% of the total, representing 1% of the industry dataset); script origins feature educational platforms, learning management systems and analytics
15. Finance | Total scripts: 1,246 (1% of the total, representing 1% of the industry dataset); script origins include banking systems, financial analytics and security tools

Script totals exceed 100% because many scripts are seen and used across multiple industries.

Behaviors

Using first-party cookies: **28,715**

Transferring data: **22,721**

Using browser storage: **20,722**

Executing risky actions: **4,586**

Accessing PII data: **3,932**

Accessing data: **3,538**

Accessing PCI data: **987**

Accessing credentials data: **830**

Accessing GPS: **13**

Loaded from blacklisted domain: **5**

Sending data to blacklisted domain: **3**

These behaviors range from common web functionalities, such as using cookies and browser storage, to more disconcerting actions such as executing risky actions and accessing sensitive data. The frequencies provide insight into how prevalent each behavior is within the dataset's context.

Client-side security risks associated with the most prevalent script types and PCI DSS v4.0 remedies

1. **Facebook Connect (5,838)**
   Risk: Data leakage through improper permissions or compromised application programming interface (API). Risk of oversharing user data or unauthorized access.

   PCI DSS v4.0: Limit data exposure to only what's necessary, monitor data access and usage, and ensure strict access controls and auditing.

2. **Google Global Site Tag (5,173)**
   Risk: Potential for sensitive information leakage or data exfiltration if misconfigured.

   PCI DSS v4.0: Ensure no capture or transmission of CHD, review and validate configurations regularly, and monitor for unauthorized data access.

3. **Google Tag Manager (5,709)**
   Risk: Can inject third-party scripts, leading to potential vulnerabilities if not secured or if third-party scripts are compromised.

   PCI DSS v4.0: Use strong user access controls, regularly monitor script changes, validate all third-party code and ensure that only authorized users can modify configurations.

4. **Google Analytics (3,914)**
   Risk: Could inadvertently capture personal or sensitive information if not configured correctly.

   PCI DSS v4.0: Ensure proper configuration to exclude any CHD from being captured, monitor data collection practices and regularly audit settings.

5. **Optanon (2,333)**
   Risk: Generally low risk, but misconfiguration can lead to compliance issues or unintentional data exposure.

   PCI DSS v4.0: Ensure that the script does not interfere with the secure handling of payment data and that consent preferences are respected and documented.

6. **Pinterest Conversion Tracker (2,205)**
   Risk: Tracks user interactions for marketing purposes, which could lead to data leakage if not configured correctly.

   PCI DSS v4.0: Ensure that no payment data is captured or processed by the tracker, regularly review data access and permissions, and monitor for unauthorized access.

7. **Universal Event Tracking (Bing) (1,963)**
   Risk: Similar to Google Analytics, tracking user behavior could lead to sensitive data exposure if misconfigured.

   PCI DSS v4.0: Verify that no CHD is captured, access only necessary information, and ensure regular monitoring and auditing of the tracking implementation.

8. **Klaviyo (1,700)**
   Risk: Manages and analyzes customer data for targeted campaigns, which involves data storage and processing, potentially introducing risks of unauthorized access or data leakage.

   PCI DSS v4.0: Ensure that Klaviyo does not store, process or transmit CHD unless it's absolutely necessary and secure. Implement strict data access controls and regular audits.

9. **Google Analytics – E-commerce (1,663)**
   Risk: Specifically designed for e-commerce analytics, but if misconfigured, could lead to sensitive data exposure.

   PCI DSS v4.0: Regularly audit and monitor data collection to ensure that no CHD is being captured or transmitted, and maintain strict access controls.

Top 10 domains based on various script categories, highlighting key trends in the dataset

- **Total scripts on page:** Shows domains with the highest total number of scripts (third- and fourth-party scripts combined). This indicates the overall load and potential complexity of interactions on these domain pages.
- **Third-party scripts:** Highlights domains with the highest number of third-party scripts. These scripts are typically used for various functionalities, including analytics, advertising and customer support tools.
- **Fourth-party scripts:** Focuses on domains with the highest number of fourth-party scripts, which are scripts called by third-party services. Their presence can indicate deeper levels of dependencies and potential security concerns.
- **Scripts accessing payment data:** Shows the domains with the most scripts accessing payment data, pointing to potential areas of vulnerability or increased security measures for handling sensitive financial information.
- **Scripts accessing PII:** Identifies the domains with the highest number of scripts accessing PII, highlighting privacy implications and the need for robust data protection practices.

These trends offer insights into the security, privacy and operational practices of the domains in question, revealing potential areas for further investigation, optimization or security enhancements.

A Verizon Business Cyber Security Consulting and Source Defense publication

verizon.com/paymentsecurityreport
sourcedefense.com

About Verizon Cyber Security Consulting

This research publication is a product of Verizon Cyber Security Consulting, a global leader in the payment security practice with a security team of more than 600 consultants in 30 countries. Verizon has one of the largest teams of PCI Qualified Security Assessors.

Verizon is the longest-running global PCI security consulting and assessment services provider in the world, offering services since 2002. Our payment security practice provides PCI and Society for Worldwide Interbank Financial Telecommunication (SWIFT) consulting, assessments and program maturity improvement services. Across its Cyber Security Consulting portfolio, Verizon offers services that help clients identify, protect against, detect, respond to and recover from cyberthreats while helping to comply with applicable regulations and standards.

Visit our website on October 3 to download the Verizon 2024 Payment Security Report: verizon.com/paymentsecurityreport.