

North America Community Meeting 2023



Scaling 6.4.3 & 11.6.1: **Browser Script Management & The Large Enterprise Journey to Compliance**

Introductions



Steven Eric Fisher

Senior Cyber-Security Risk Expert,
Compliance
Walmart Global Tech*



Jeff Zitomer

Sr. Director of Product Management,
Client-Side Defense & PCI DSS
HUMAN Security

** My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.*

Agenda

1. From Browser Script Risks to PCI DSS v4.0
2. The Large Enterprise Journey



From Browser Script Risks to PCI DSS v4.0

Jeff Zitomer, HUMAN Security

Script-Based Attacks “Became a Thing” Around 2018

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS MORE SIGN IN SUBSCRIBE

How Hackers Slipped by British Airways' Defenses

Security researchers have detailed how a criminal hacking gang used just 22 lines of code to steal credit card data from hundreds of thousands of British Airways customers.



NEWS POLITICS U.S. NEWS WORLD BUSINESS TECH HEALTH WATCH NOW

TECH & MEDIA

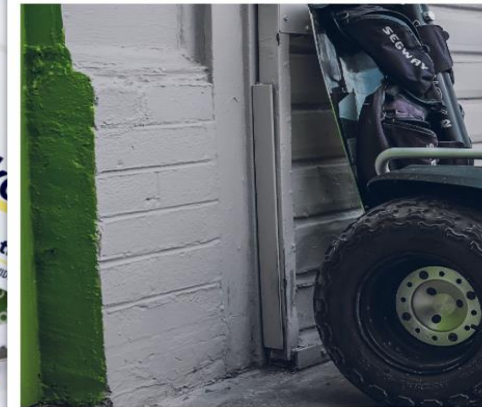
Ticketmaster data theft part of larger credit card scheme, security firm says

"We've identified over 800 victim websites making it likely bigger than..."



Segway store hacked to steal customers' credit cards

By Bill Toulas



Segway's online store was compromised to include a malicious threat actors to steal credit cards and customer information.

DBIR

2023 Data Breach Investigations Report

Stolen credentials: \$5. Domain hosting: \$12. Malicious JavaScript: \$50. Snagging all the fullz: priceless.

paying attention to. Within Retail, we often find the "Magecart"⁵¹-type actors. These criminals find ways of embedding their malicious code within your site's credit card processing page.

Browser Scripts Are a Lucrative Attack Surface

1. Modern websites (and payment pages) heavily depend on them



Analytics



Promotion



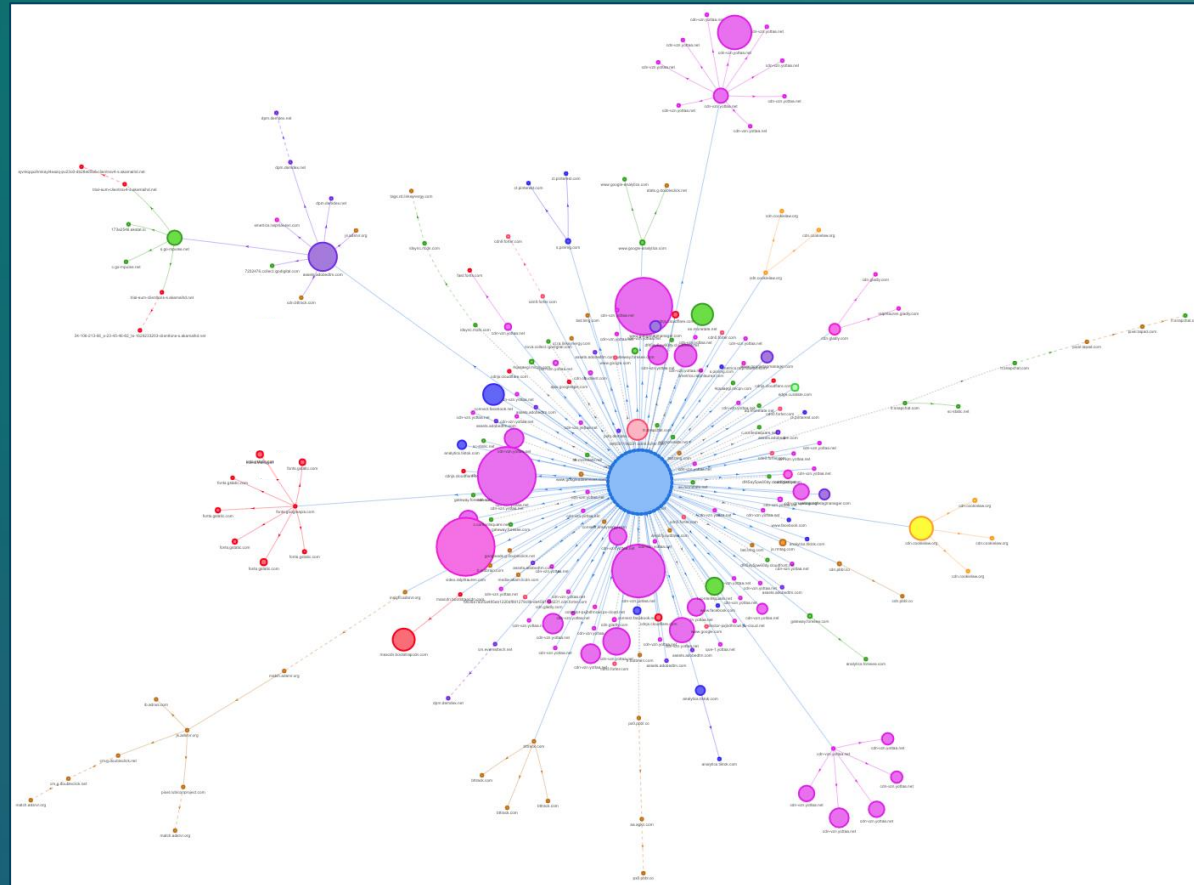
Advertising



Social Media



Chat & Support



Browser Scripts Are a Lucrative Attack Surface

2. They load dynamically from across the Internet...



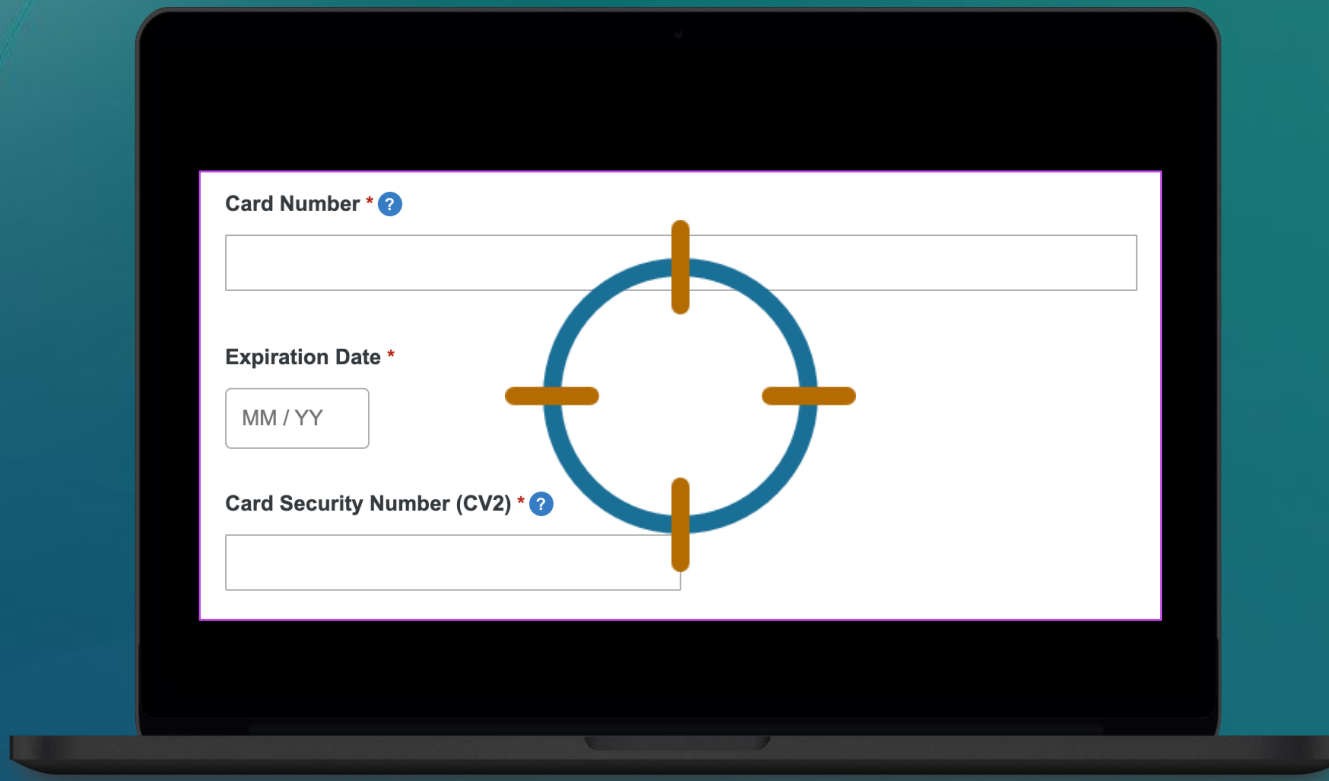
Browser Scripts Are a Lucrative Attack Surface

3. ...bypassing change management & security controls



Browser Scripts Are a Lucrative Attack Surface

4. They can compromise cardholder data



- Skimming
- Formjacking
- Malicious Redirects

Browser Scripts Are a Lucrative Attack Surface

5. They are largely unmanaged



Enter PCI DSS v4.0

6.4.3 & 11.6.1 (primarily)



In a Nutshell

Goal: Protect cardholder data from payment page browser scripts

6.4.3 Script Management

- Confirm scripts are authorised
- Assure scripts' integrity
- Maintain inventory with written justification

Requirements and Testing Procedures	Guidance
Defined Approach Requirements 11.3 All scripts loaded and executed on the payment page must be authorized as follows: <ul style="list-style-type: none">• 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 loaded and executed on the payment page is maintained and updated with all elements specified in this requirement.	Purpose Payment pages may contain scripts that provide functionality to load additional external scripts (for example, advertising and tracking, tag management systems). Such seemingly harmless scripts can be used by potential attackers to upload malicious scripts that collect and exfiltrate cardholder data from the consumer's browser. It is necessary for the operation of the payment page to minimize the number of scripts that could be tampered with. Ensuring that scripts have been explicitly authorized reduces the probability of unnecessary scripts being added to the payment page without authorization. When the payment page is loaded with the scripts, the merchant must ensure that the script being modified to carry out unauthorized behavior, such as skimming the cardholder data from the payment page. Good Practice Scripts may be authorized by manual or automated (e.g., workflow) processes. Where the payment page will be loaded into an inline frame (IFRAME), restricting the location that the payment page can be loaded from, using the parent page's Content Security Policy (CSP) can help prevent unauthorized content being substituted for the payment page. <i>(continued on next page)</i>
Customized Approach Objective Unauthorized code cannot be present in the payment page as it is rendered in the consumer's browser. Applicability This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties. <i>This requirement is effective as of 3/31/2025, and fully compliant by 6/30/2025.</i>	

11.6.1 Change & Tamper Detection

- Alert to unauthorized modification to the HTTP headers (...) as received by the consumer browser

Requirements and Testing Procedures	Guidance
11.6 Unauthorized modification to the HTTP headers as received by the consumer browser 11.6.1 A change- and tamper-detection mechanism is deployed as follows: <ul style="list-style-type: none">• To alert the merchant to unauthorized modification to the HTTP headers as received by the consumer browser, the mechanism is configured to evaluate the received HTTP headers as received by the consumer browser.• The mechanism is configured to verify the integrity of the received HTTP headers as received by the consumer browser.• The mechanism is configured to verify the integrity of the received HTTP headers as received by the consumer browser.	Purpose Many web pages now rely on assembling objects, including active content (primarily JavaScript), from multiple internet locations. Additionally, the content management and tag management systems that may not be possible to monitor using traditional change detection mechanisms. Therefore, the only place to detect changes or indicators of malicious activity is in the consumer browser. The payment page is considered and all content is rendered in the consumer browser. The HTTP header and the active content of payment pages as received by the consumer browser with prior or known versions, it is possible to detect unauthorized changes that may indicate a skimming attack. Additionally, by looking for known indicators of compromise and script elements or behavior typical of skimmers, suspicious alerts can be raised. <i>(continued on next page)</i>
Customized Approach Objective 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.	

Deadline: 3/31/2025

Top Techniques to Protect & Comply

Avoid cardholder data



Top Techniques to Protect & Comply

Avoid scripts



Top Techniques to Protect & Comply

Evaluate the options in the standard



Content Security Policy & Subresource Integrity

Proactive
Free

Complex to manage
Blunt & brittle
No script inventory



Synthetic Scanner

Inventory/management
Unintrusive

Incomplete & bypassable
Setup & maintenance
Monitoring only



Real User Monitoring & Defense

Inventory/management
Setup & maintenance
Precision blocking

Yet another script



The Large Enterprise Journey

Steven Eric Fisher, Walmart

My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.

You've Got Work To Do

Know what's coming
Assess risk
Evaluate blast-radius

Digest

Map current website state
Identify envisioned state & "Pass" State
Design for defense-in-depth
Vet tooling

Plan

Analyze

Remediate findings
Simplify architecture
Reduce scope

Implement

Improve

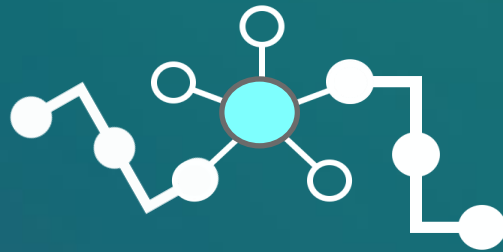
Map dependencies
Create program
Communicate

Address script bloat
Gate 3rd parties
Roll out security tools

My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.

Digest

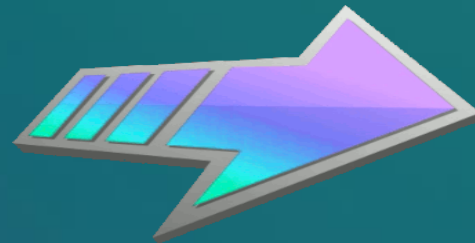
- Journeys start with an origin and a destination
- Nexus – a connection or link between things, especially that is or is part of a chain of causation



My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.

Plan

- 2017-2018 – The rise of the e-skimmers
- App engine native security – was too immature and inconsistent
- Balancing effort, cost, and risk – short term & long term goals



My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.

Analyze

- Engage experts
- Identify script bloat
- Tool up? Identify existing reuse or gap coverage



My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.

Implement

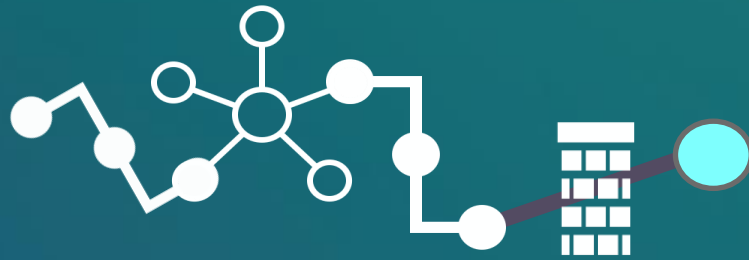
- Layer security features
- Controlled gating for 3rd party scripts
- Beware timelines and impacts



My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.

Improve

- Simplify, reduce
- Integrate, automate



My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.

Key Takeaways

1. New payment page protection requirements (6.4.3 & 11.6.1) address an important security gap, but effective implementation can be challenging for enterprises
2. Large enterprises should start ASAP with scoping, aligning stakeholders and process, and deploying technology that can balance security and business needs
3. We recommend engaging expertise, layering multiple technical & process controls, and seeking opportunities to simplify and automate with maturity

Thank you!

