The Digital Skimming Threat Landscape: What Security Leaders Need to Know

July 16, 2026

Matt McGuirk
VP of Field Engineering
Source Defense

CAMPUSGUARD®

ScriptSafe

Introduction and Agenda

source DEFENSE

ı at **Capture**
ta S **a Privacy *and***
)arty gration
ıe last mile of 3rd party risk management

- Supporting zero-trust and SBOM

Mastercard’s Global Partner in Digital Skimming Defense

source DEFENSE

Securing the backbone of eCommerce against eSkimming attacks

Driving down risk and fostering trust in digital commerce

Identifying active campaigns, disrupting fraud schemes, enriching global threat intelligence

Driving Down Digital Supply Chain Risk

Most organizations unknowingly grant full trust to:

- Analytics Platforms
- Chat Widgets
- Marketing Tags
- Social Integrations
- Scheduling Systems

Source Defense closes this gap – preventing inadvertent data leakage and cutting off the client-side attack pathway:

By default, third-party code has **full privilege** in the browser. Source Defense enforces **least-privilege access** and blocks unnecessary access to sensitive data

What are digital skimming attacks? Why are they important?

JavaScript:

The Root Cause of Client-side Security Problems

Client-Side security, specifically data leakage prevention and eSkimming protection starts with JavaScript

JavaScript can perform any action and behave in any way it wants on any site where it is running (over 97% of all websites)

JavaScript has no native security controls

Attacks that use JavaScript

- **Magecart (brand name)**
- **eSkimming (PCI terminology)**
- **Digital Skimming (Mastercard terminology)**
- **Formjacking, Credential Harvesting, etc.**

Real-World Risks to Your Institution

source DEFENSE

What a Single eSkimming Incident Puts at Stake

Client-side attacks on tuition payment and donation pages create cascading exposure across your institution

Reputational Damage

Public breach disclosure erodes trust with students, families, donors, and accreditors

Student & Donor Financial Harm

Stolen card data hits the people you serve most directly—those paying tuition or making charitable gifts

Regulatory & Legal Exposure

State breach notification laws, potential FTC scrutiny, and class action litigation can extend for years

PCI Non-Compliance Penalties

Card brand fines, mandatory forensic audits at your expense, and in severe cases loss of card processing

Operational Disruption

Incident response pulls IT, legal, finance, and communications into weeks of unplanned crisis work

Vendor Liability Ambiguity

Attacks often originate in third-party scripts, yet most vendor contracts don't clearly assign responsibility

How does a digital skimming attack happen?

source DEFENSE

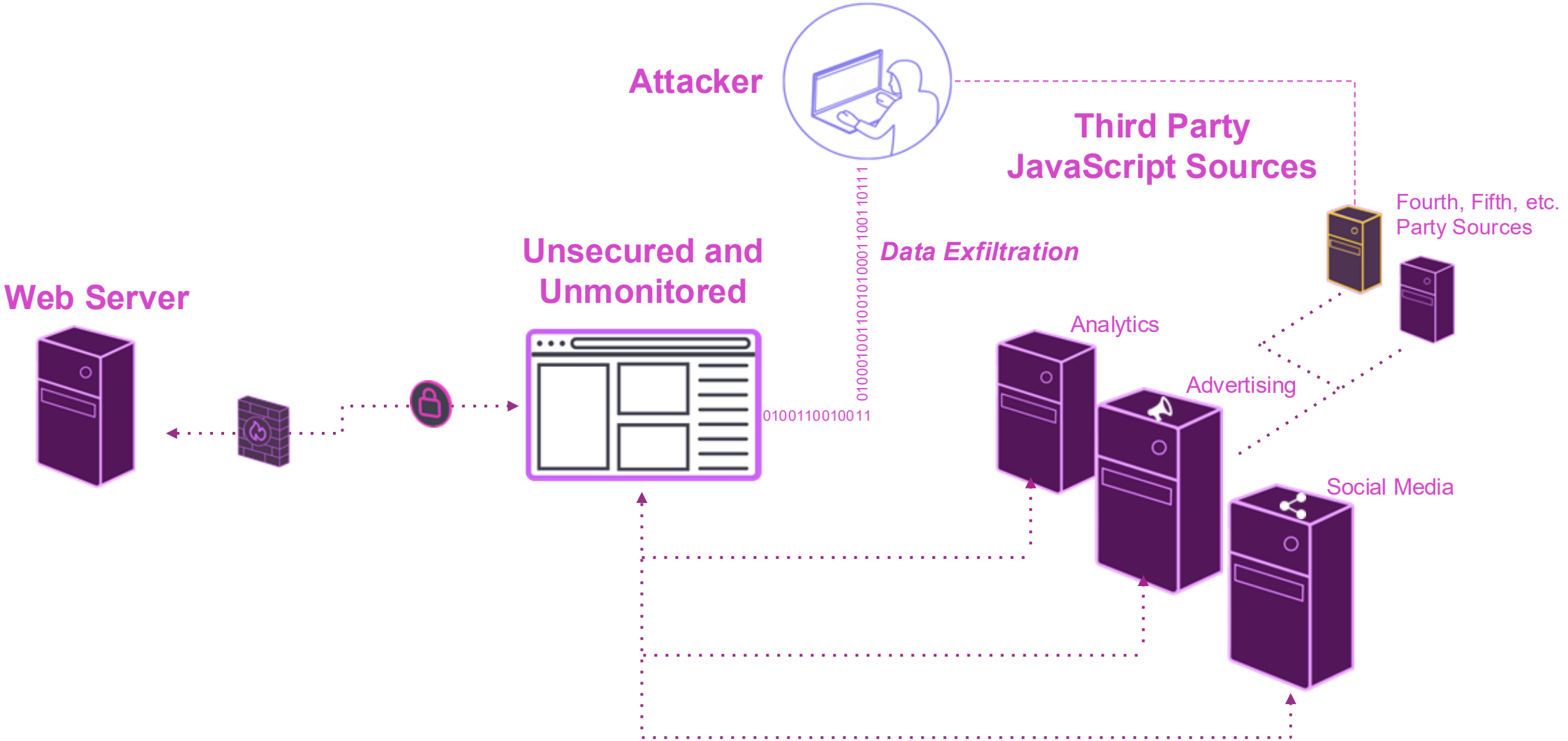
PCI DSS 4 Mandates
Digital Skimming Protection

Merchants and service providers must:

1. **Inventory payment page scripts**
2. **Provide a written justification for authorized scripts**
3. **Implement a mechanism to verify the integrity of payment page scripts**
4. **Implement a mechanism to verify HTTP headers retrieved from the payment page at least once every seven days**

Anatomy of a Client-Side Attack

source DEFENSE



A quick poll: how is your institution handling digital skimming risk?

What are some of the latest “innovations” in digital skimming attacks?

The Evolving eSkimming Playbook

A Taxonomy of Recent Attacks

Recent Source Defense threat research reveals a rapid evolution in attacker strategy.
Threat actors are no longer relying on obvious malicious domains. They are adapting across four fronts:

1. Living Off the Land

Abusing trusted enterprise infrastructure (GTM, GA4, Firebase).

2. Weaponizing Trusted APIs

Exfiltrating via valid GraphQL and cloud endpoints.

3. Evading Network Controls

Bypassing CSP using WebRTC, error pages, and decentralized C2s.

4. Shifting Left & Deceptive UI

Attacking pre-checkout pages and cloning payment iframes.

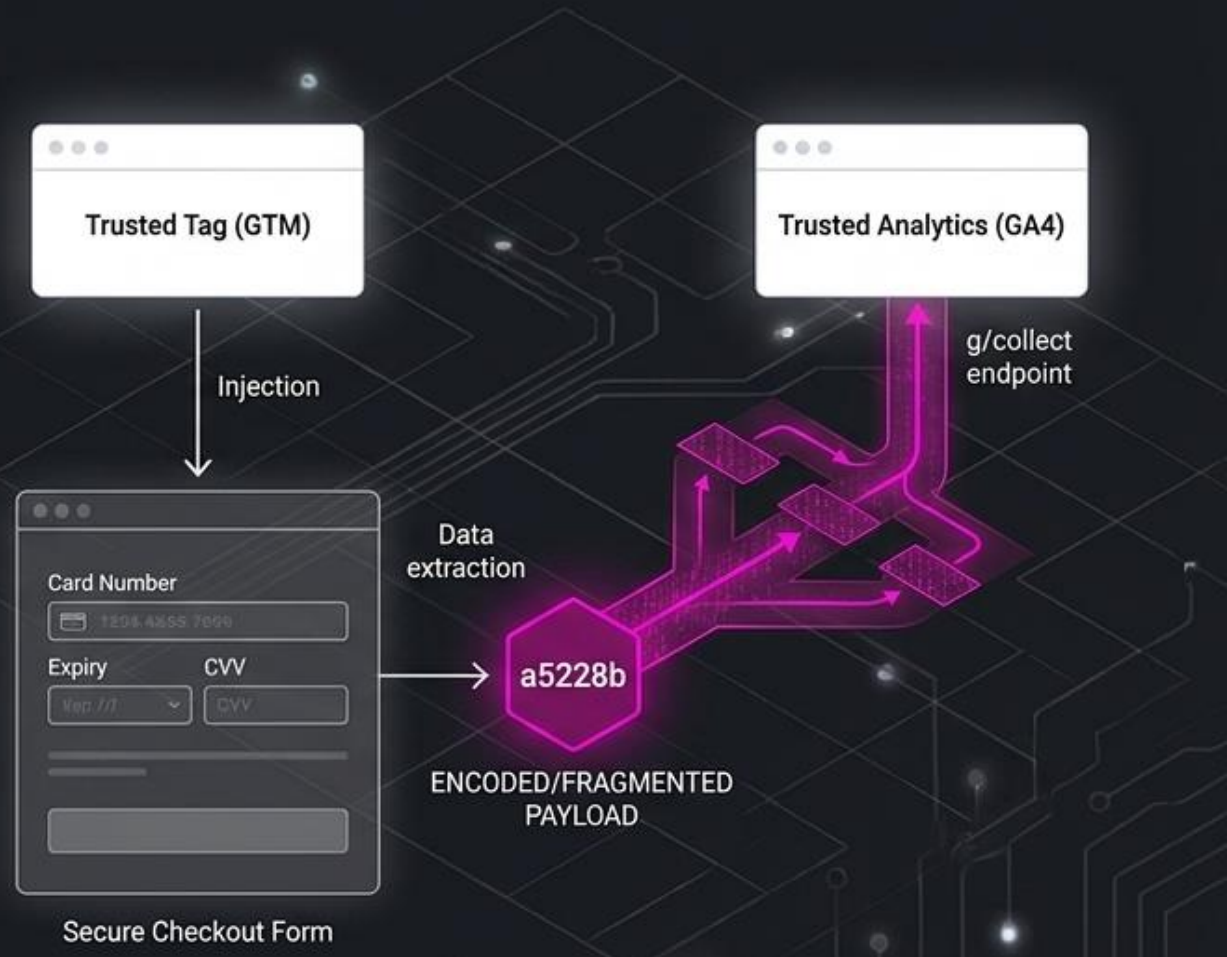
Tactic 1: Living Off the Land

Hiding in Trusted Google Infrastructure

The Strategy: Avoid suspicious domains by routing attacks through tools you already permit.

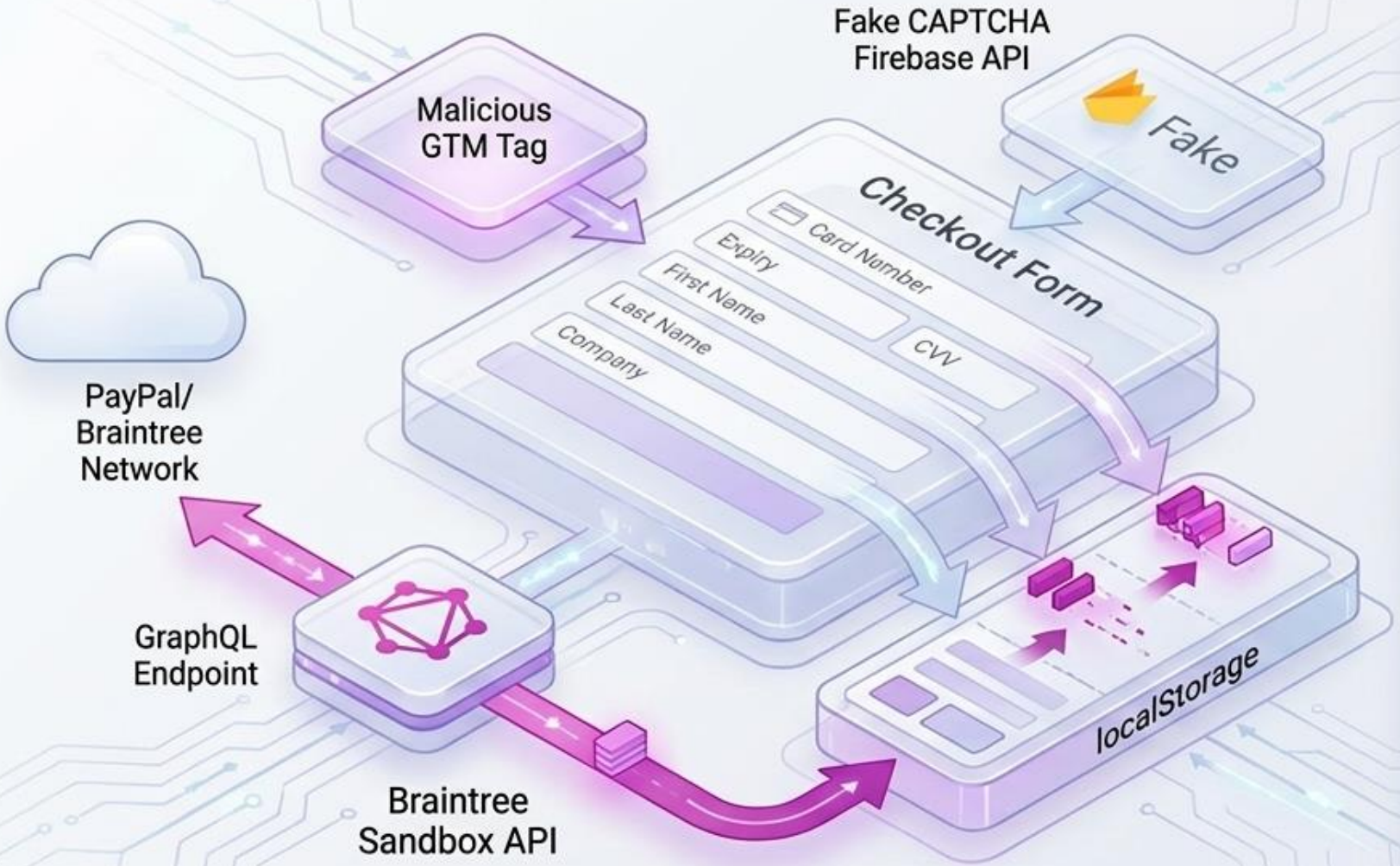
Case Study: Major US Auto Brands

- **Infiltration:** Attackers compromised a shared GTM container (GTM-MX8L362L).
- **Targeting:** Logic explicitly sought Authorize.Net CIM checkout flows.
- **Obfuscation:** Data was combined into a pipe-delimited string, XOR-encoded (key: 5d7845ac6ee7cfffafc5fe5f35cf666d), and Base64-encoded.
- **Exfiltration:** Fragments were placed into custom GA4 event parameters (ep.fields_p1, ep.fields_p2) and sent to the legitimate g/collect analytics endpoint.



Tactic 2: Weaponizing Trusted APIs

Data Exfiltration via Braintree GraphQL



The Strategy:

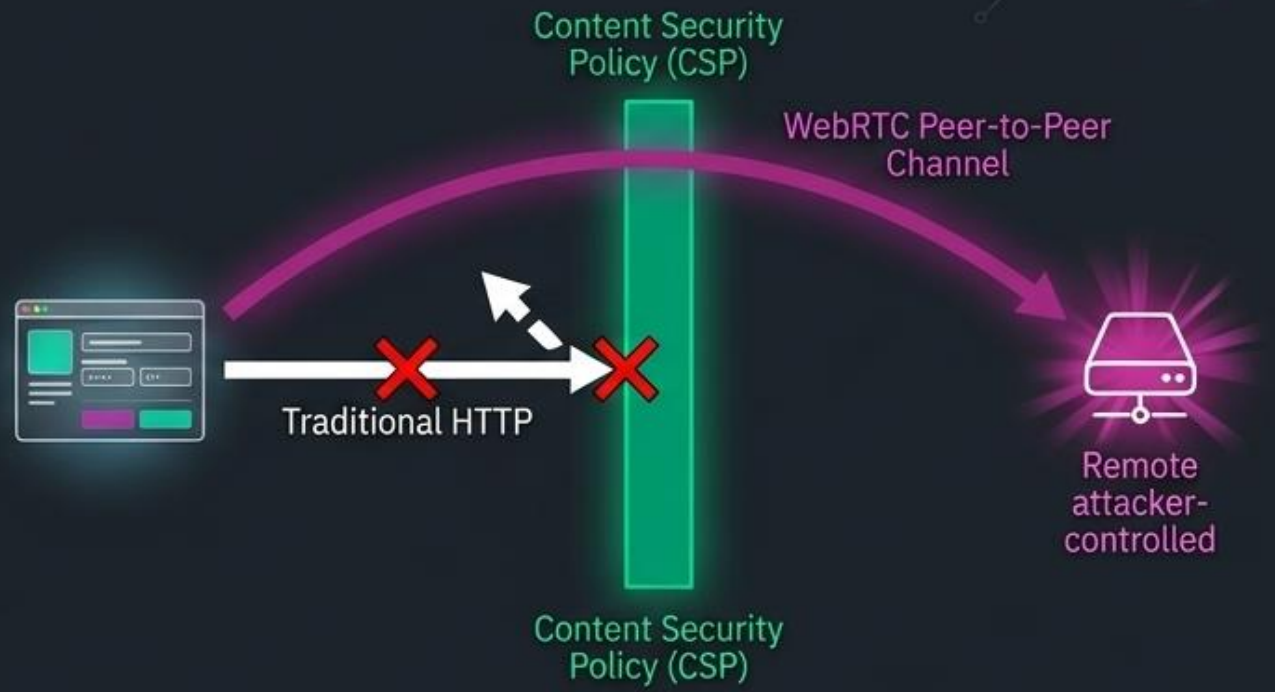
1. A malicious GTM tag fetches a JavaScript payload from a fake CAPTCHA-themed Google Firestore document API.
2. The script harvests billing and identity data, staging it in localStorage.
3. Staged data is split and packed into legitimate fields (e.g., placing card data inside first name and company parameters).
4. The payload is pushed out via a valid-looking PayPal Braintree Sandbox GraphQL customer creation request.

Tactic 3: Bypassing CSP (Covert Channels)

The WebRTC Exfiltration Pipeline

The Evasion

- **The Pivot**: Injected HTML uses an Angular-style ng-on-error handler on a broken image to copy a valid CSP nonce.
- **The Exfiltration**: The script opens a WebRTC peer-to-peer connection to an attacker-controlled TURN relay on port 443.
- **The Steal**: Checkout data is chunked and streamed outward hidden inside TURN username fields.



The Reality Check

- **The Crash**: Magento 2 dynamically rebuilds the checkout page during interaction. The script executed twice, hit a basic JavaScript scoping error, and hilariously crashed the browser session before it could steal data.

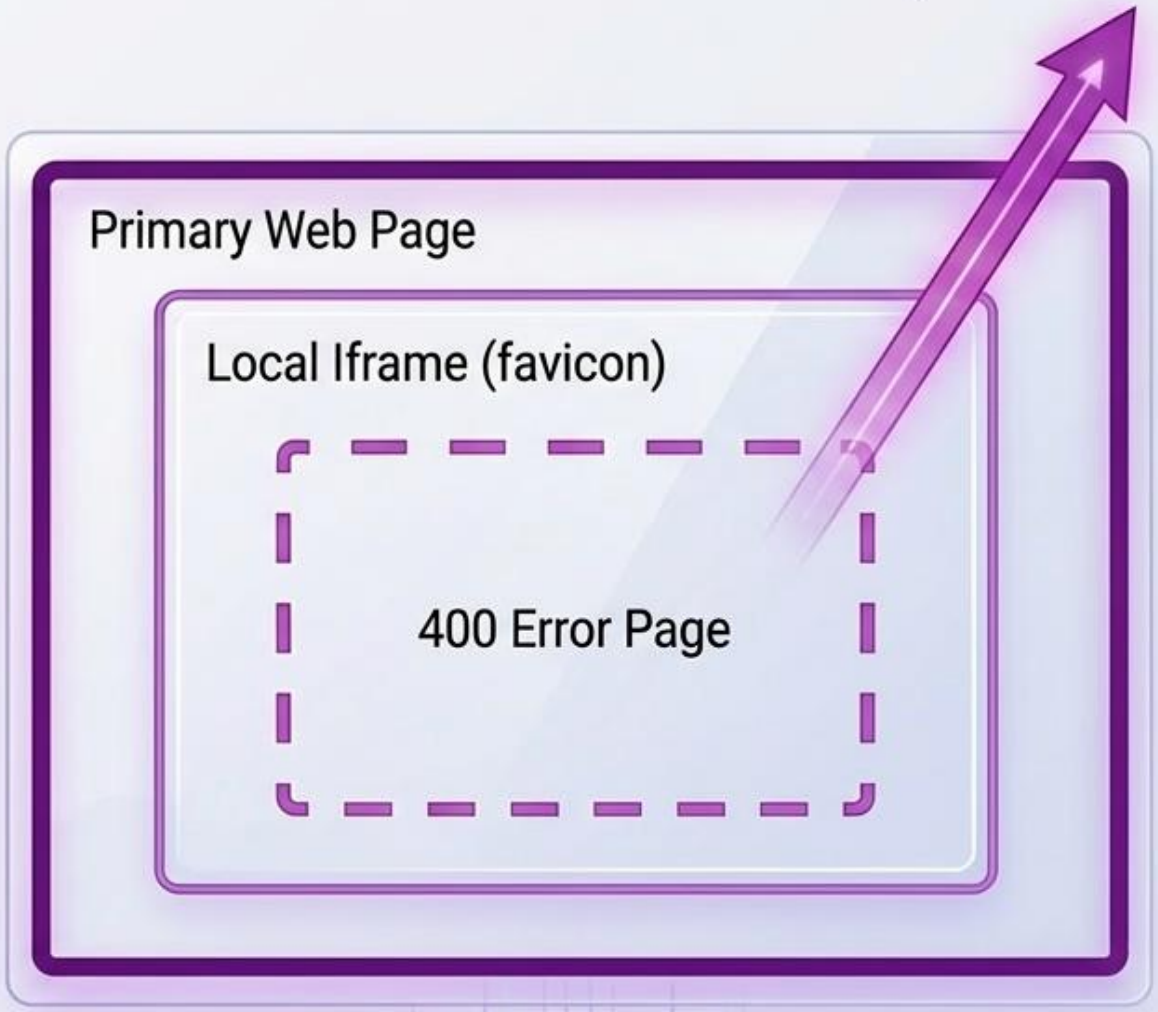
Tactic 4: The ‘Forgotten Page’ Loophole

Hunting for Uneven Policy Coverage

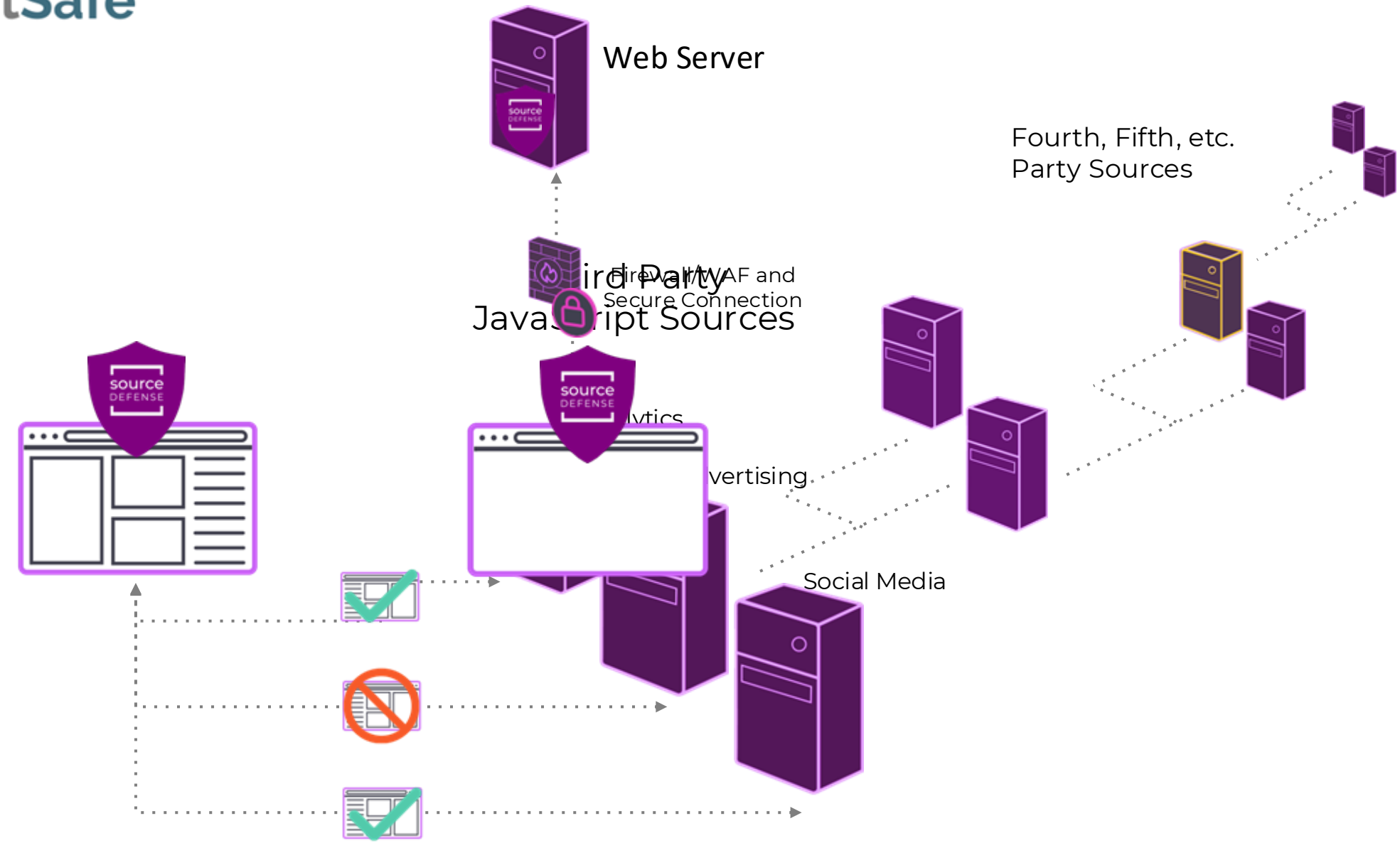
The Strategy: Don’t attack the heavily guarded checkout page; hunt for uneven policy coverage.

The Attack Chain:

1. **Foothold**: Attacker controls the page via a trusted GTM container.
2. **Local Iframe**: Creates a same-origin iframe to a trusted local resource (favicon).
3. **Path Traversal**: Creates a nested iframe using a path-traversal request to force a 400 Error Page.
4. **The Loophole**: The 400 error page lacks the strict CSP applied to the main checkout.
5. **Execution**: Outbound destination is placed inside a script src attribute. Data is safely exfiltrated.



ScriptSafe


Web Server
Fourth, Fifth, etc.
Party Sources
Firewall/WAF and
Secure Connection
Social Media

ScriptSafe

REAL-TIME CODE CONTROL AND SUPPLY CHAIN VISIBILITY

- **Isolate** foreign scripts from the web page
- **Block** harmful activities such as Magecart style attacks
- **Ensure** beneficial behavior
- **Thwart** attacks in real-time
- Securely **integrate** 3rd party code **with minimal effort**

Working with CampusGuard and Source Defense

Evaluations completed in as little as a week
(or even less)

Source Defense can create a testing environment for your payment pages in practically no time at all. Evaluations can take as little as one week from start to finish

Bespoke support for your process

Source Defense provides project-specific documentation and materials for all evaluation outcomes, commercial figures, and compliance-mapping so you can spend less time thinking about vendors

Deploy and deliver in days

Source Defense can deploy our solutions in as little as 24 hours. We provide zero-code deployment options, and code integration is as simple as copy-and-paste.

Thank you!

For more information:
sourcedefense.com/request-demo/
matthew@sourcedefense.com