source DEFENSE

SOURCE DEFENSE

The 7 Things You Need to Know About Threats to Your Website's Payment Data

www.sourcedefense.com

| info@sourcedefense.com

EXECUTIVE SUMMARY

The Payment Card Industry Security Standard Council issues the PCI DSS framework to provide standards and requirements for merchants accepting payment cards and ultimately to secure consumers payment data. However, there is a specific and critical stage in the payment lifecycle that is currently absent from this framework – **data creation.** Websites are now a primary and growing entry/creation point for payment data. Due to a universal flaw in the construction of nearly every website, this data is left exposed to multiple unauthorized external entities and to hackers that exploit their access. Because this flaw is universal, nearly 5000 websites per month are victimized. This briefing explains the universal flaw, describes the attack methodology, discusses the benefits and limitations of various mitigation options, highlights the need for real-time prevention, and proposes requirements and a testing standard for website owners evaluating potential compensating controls. This white paper will discuss threats, caveats, and the impact of payment data exposure.

- PCI Framework: Intent, Responsibilities, and Scope
- Current Framework Gap: Protection of Payment Date Creation
- Payment Data Exposure & Theft Due to a Universal Flaw in the Website Supply Chain
- Threat Actor Exploitation & Potential Damages
- How a Website Supply Chain Attack Works
- The Attack Surface and “Hidden Tags”
- Scalability of Attacks

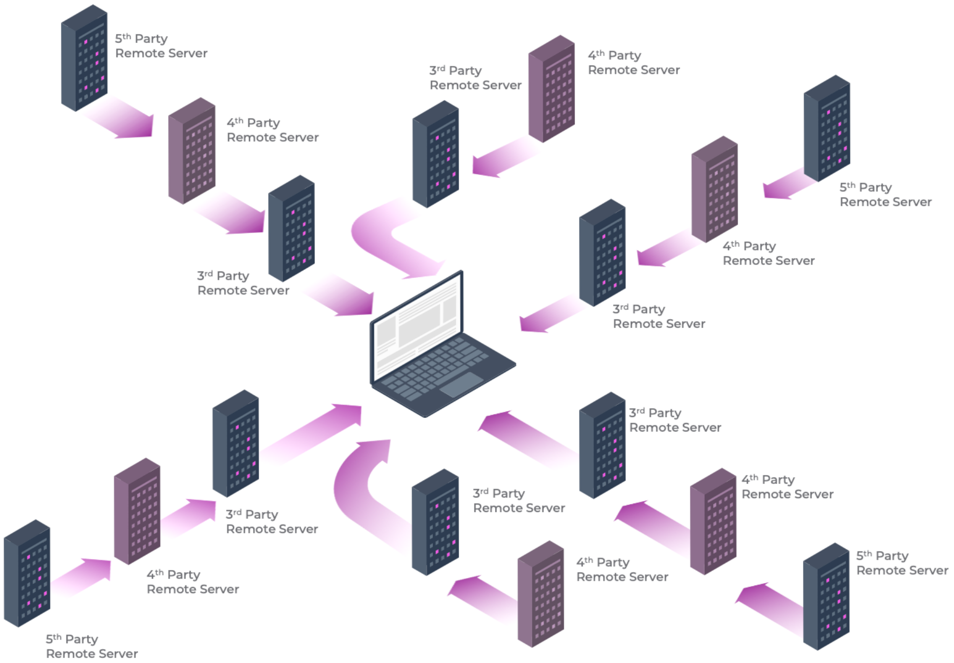
1. PCI INTENT, RESPONSIBILITIES, AND SCOPE

The Payment Card Industry (PCI) Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for data protection and to ensure that credit card transactions are both reliable and secure. Organizations that choose to accept credit cards as a form of payment are required to follow the standards established by the PCI Security Standards Council. Failure to comply can result in fines, more stringent compliance requirements, such as a third party onsite audit by a Qualified Security Assessor (QSA), and potential suspension of payment card processing services.

The PCI DSS framework offers testing and validation requirements and strategies for processing, storing and transmitting payment card transactions. The intent of the framework is to provide constructive guidance on securing payment transactions end-to-end. The standard includes controls for handling and securing credit card information.

2. THE ATTACK SURFACE & HIDDEN TAGS

The attack surface is much larger than the third-parties directly and purposefully integrated into a website. The attack surface rapidly expands as third parties routinely chain-in multiple fourth and fifth parties that share the same level of unrestricted access to the corporate webpage ("hidden tags"). Most corporate website owners are completely unaware and blind to the vast number of external entities with unlimited and unavoidable access. The sheer number of unmanaged connections between the client-side browser and external third-party servers provide attackers with an expansive attack surface.



3. SCALABILITY OF ATTACKS

This attack type is extremely scalable because the attackers immediately gain access to every website served by the compromised third-party JavaScript vendor. The compromise allows threat actors like Magecart to attack hundreds or thousands of organizations and in turn victimize huge aggregate user populations during each campaign.

Scalability of a Formjacking Attack

One 3rd Party ▸ Thousands of Websites

4. THREAT ACTOR EXPLOITATION & POTENTIAL DAMAGES

Threat actors are exploiting the universal website supply chain flaw at mass-scale — repeatedly victimizing hundreds and even thousands of sites per campaign. Recent research quantifies that nearly 5000 websites are successfully attacked per month while other research provides that 20% of victimized websites are re-infected within days – some up to 18 times. Based upon open-sourced reporting, notable victims have included Ticketmaster, Best Buy, Delta Airlines, NewEgg, Sears, Pizza Hut, Kmart, 1-800-Flowers, Puma, Equifax, and TransUnion. The velocity of attacks targeting this flaw highlights the inadequacy of current security controls and the nearly global vulnerability of corporate websites.

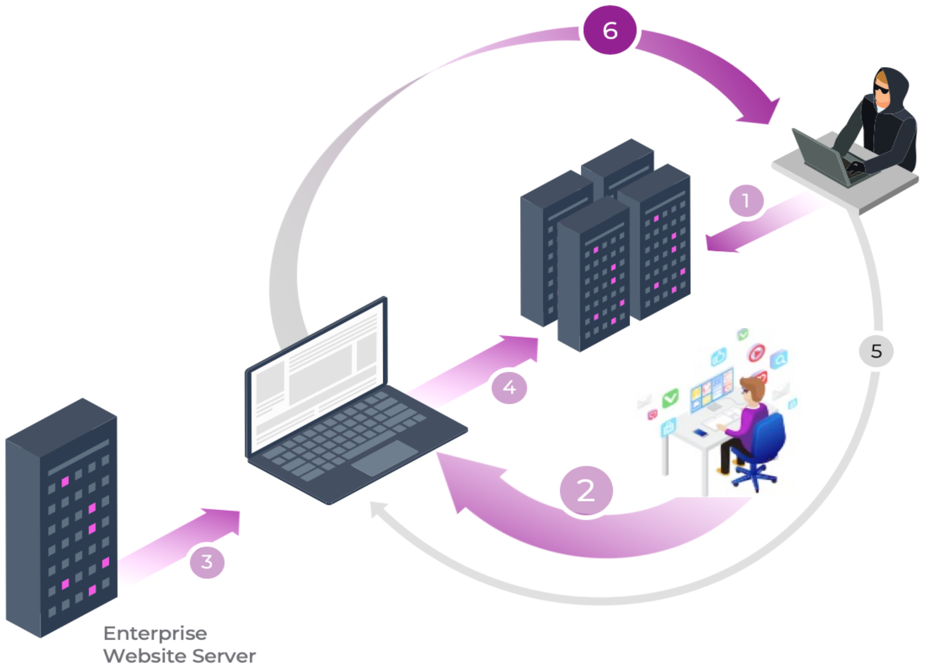
The scope of potential damages due to the unlimited webpage access is extensive:

- Data Skimming
- Formjacking
- Keylogging
- Screenscraping
- Clickjacking
- Phishing
- Web Injection
- Form Field Manipulation
- Defacement
- Malware, Banking Trojan, and Ransomware Distribution
- iFrame Attack

It's important to note that the PCI standard is not currently encompassing all of the potential vulnerability points and hopefully in the future will be expanded to include additional testing and validation controls for the highly vulnerable origination point of payment data on eCommerce websites.

5.
HOW A WEBSITE SUPPLY CHAIN ATTACK WORKS

Web Session Attack



1. Attacker compromises a 3rd party vendor & modifies the JavaScript to include malicious code
2. A user visits your site.
3. Your web servers provide your website to the visitor.
4. Your webpage, while rendered in the user's browser, requests content from the 3rd party server.
5. The modified JavaScript from the compromised 3rd party is sent directly to the user's browser, requests content from the 3rd party server.
6. The malicious code executes in the user's browser session. In cases of data theft attacks, data is exfiltrated either directly back to the compromised vendor's server or to the attacker's server.

6.
PAYMENT DATA EXPOSURE & THEFT VIA A UNIVERSAL FLAW IN THE CORPORATE WEBSITE SUPPLY CHAIN

Attackers have increasingly targeted the corporate website as it represents an attractive and vulnerable entry point for accessing customer payment data at massive scale. This vulnerability exists because nearly every modern website integrates code and tools from dozens of external website supply chain vendors (third party JavaScript tools). However, JavaScript tools are insecure allowing external, and often unauthorized entities, uncontrolled access to the entire webpage during live customer website sessions (which includes payment transactions). This flaw prevents website owners from explicitly controlling what data can be accessed by their third party website supply chain vendors and also hackers that seek to exploit this flaw.

The uncontrolled access to the webpage and all data transmitted during the user session provide threat actors with an easy path to penetrating a website's security and exfiltrating personally identifiable information (PII) and payment data. Instead of directly targeting the defences of the highly secured website owner, threat actors follow the path of least resistance by targeting the website supply chain's weakest link which is a vulnerable third party vendor's security infrastructure.

3.

PAYMENT DATA EXPOSURE & THEFT VIA A UNIVERSAL FLAW IN THE CORPORATE WEBSITE SUPPLY CHAIN

JavaScript's designed-in flexibility and external third party JavaScript provide full developer-level access (i.e., **DOM access**) to webpages. This results in merchant website owners being unable to control how the third party JavaScript modifies and interacts with the webpage during the user session. Once attackers have breached the security defences of a third-party vendor (or a linked fourth party – "**hidden tags**"), threat actors modify or replace the code served from the external third-party service directly to the client-side browser. Frequently these modifications involve adding **card skimming** or **formjacking** code as a means of data exfiltration.

The result is that third-parties and linked fourth, fifth, … nth parties may unknowingly access regulated customer and payment data. (Which may make these nth parties a Service Provider) The unapproved access constitutes a violation of many data privacy regulations and should be encompassed in the PCI DSS framework specifically.

7.

CURRENT FRAMEWORK GAP: PROTECTION OF PAYMENT DATA CREATION

Consumers navigate to websites and readily and routinely enter their payment card data, creating an entry origin point for payment data and simultaneously creating a security and privacy obligation for the website owner. The public website is the property of the organization, the primary or sole environment through which e-commerce can be conducted to actively solicit payment data. It is incumbent upon the website owner to ensure the environment provided to the customer adequately allows the secure entry (creation) of payment data.

As online e-commerce continues to grow, and payment data is exchanged on websites at an ever-increasing volume, the PCI DSS framework should review specific and new controls and requirements for the primary origination point of payment data; the corporate website. Currently, the PCI DSS framework does not specify controls for this vulnerable and increasingly exploited, the origination point of payment data.

ABOUT SOURCE DEFENSE

Source Defense provides an entirely new and unique solution to prevent Magecart-style browser session attacks originating via the website supply chain. Source Defense's real-time prevention isolates all 3rd party JavaScript from the webpage and leverages a fully automated and machine-learning assisted set of policies that control the access and permissions of all 3rd party tools operating on a website (including the 4th and 5th parties they chain-in). The Source Defense solution preserves the user experience, eliminates unnecessary latency introduced by 3rd party tools, and prevents stability issues caused by 3rd parties while ensuring 3rd parties may not be leveraged for malicious data extraction or website alteration.

This real-time prevention also unlocks the potential of digital channels and website marketing by empowering the use of technologies that provide enhanced analytics, competitive advantage through innovation and differentiation, customer retention, and customer conversion.

For a complimentary Risk Assessment & Attack Surface Map:

✉ info@sourcedefense.com

🔗 www.SourceDefense.com