Tackling eSkimming and PCI Challenges in Higher Education Description

June 5, 2025

Matt McGuirk
Head of Field Engineering
Source Defense

CAMPUSGUARD®

ScriptSafe

Web Application Client-side Security

The Pioneer & Global Leader in eSkimming Security & Compliance

Category Creator & Market Leader

10 years of engineering and product development solely focused on eSkimming security
Trusted by more than 1,000 of the world's leading brands

Trusted by and Leading the PCI Community

PCI Principal Participating Organization, PCI SSC Board of Advisors,
PCI Small Merchant Taskforce, Global QSA Partner Enablement Program of 150+ QSACs, PSPs

PCI Security Standards Council
PRINCIPAL PARTICIPATING ORGANIZATION

Best-in-Class, Most Trusted Offering in Market

Dead-simple deployment, set-and-forget security with no operational burden
Purpose built for PCI Compliance, processes and reporting built-in by design

Robust Global Partner Ecosystem

Global & Regional partners leveraging
MSP, OEM, Reseller, Referral

IBM fiserv. GM sectec50 TRACE3 PCI Consulting Australia TEVORA OPTIV verizon

Consistently Recognized as Best in Class

JavaScript: The Root Cause of Client-side Security Problems

source DEFENSE

Client-Side security, specifically eSkimming prevention 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)

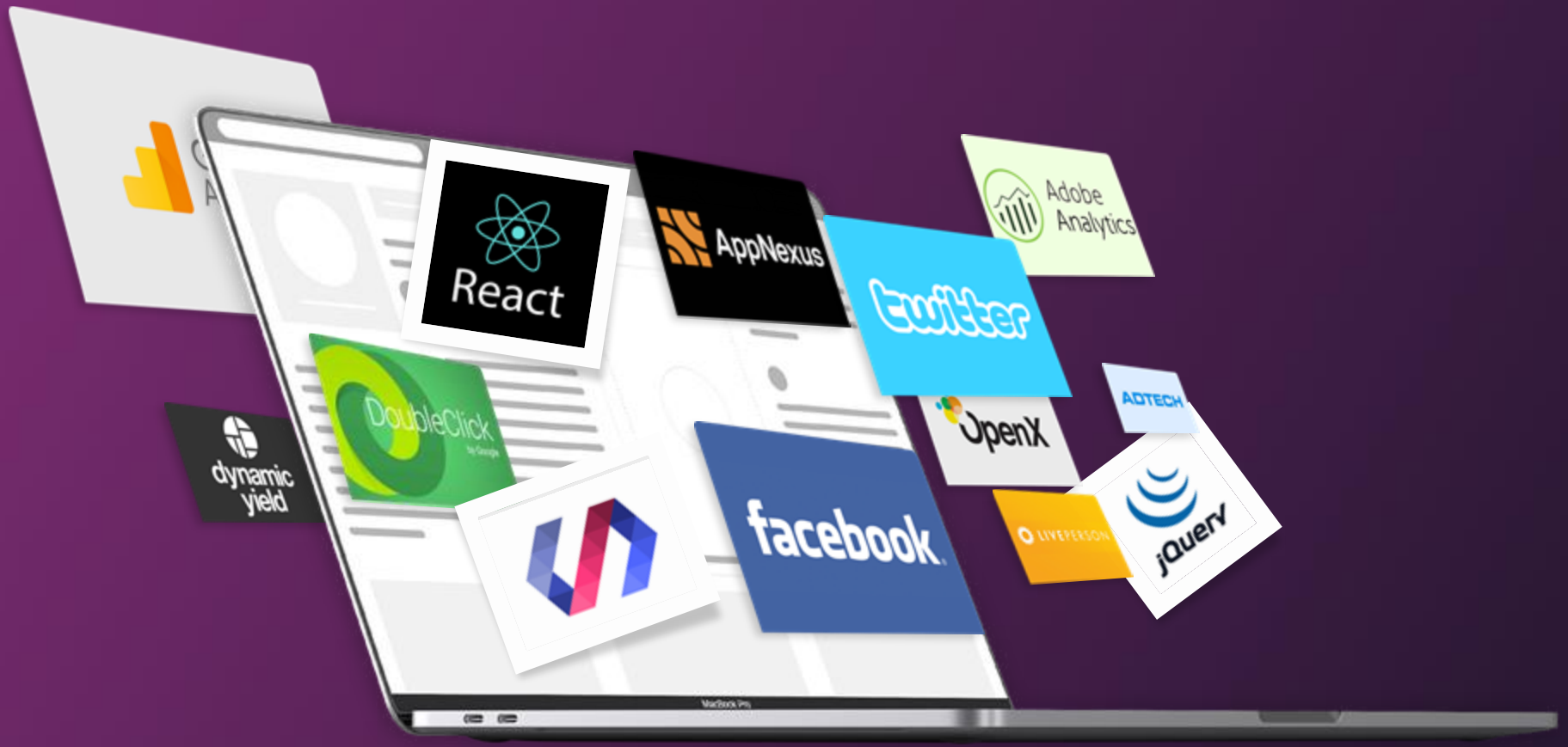
JavaScript has no native security controls

Attacks that use JavaScript

- Magecart (brand name)
- eSkimming (PCI terminology)
- Formjacking, Credential Harvesting, etc.

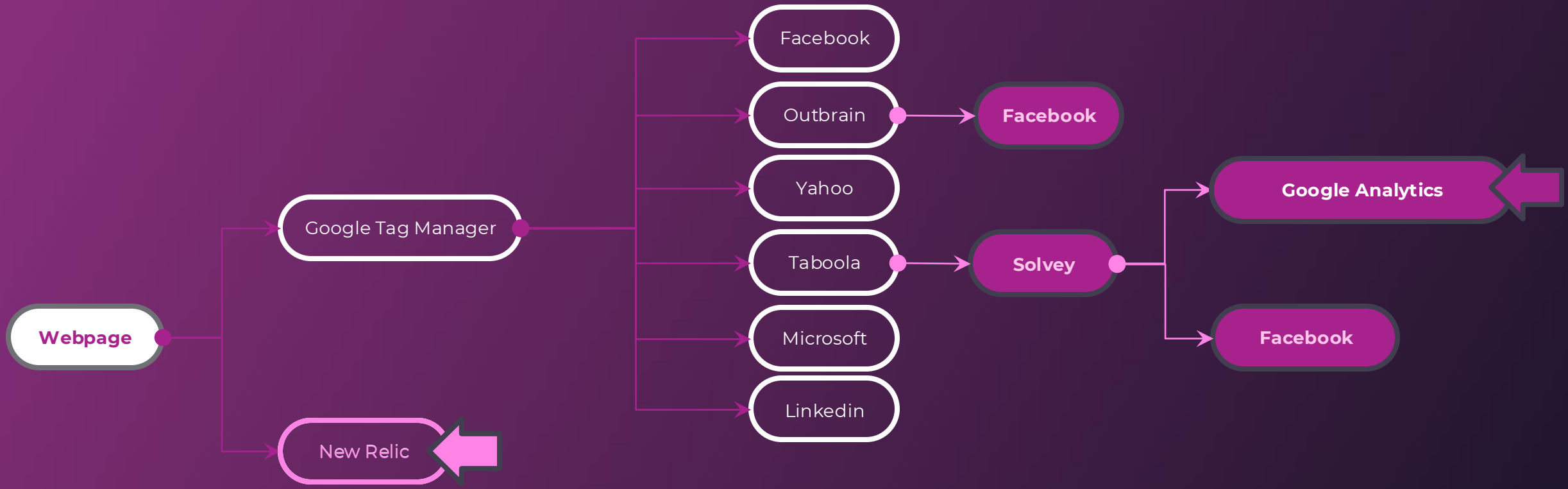
What is client-side JavaScript?

source DEFENSE

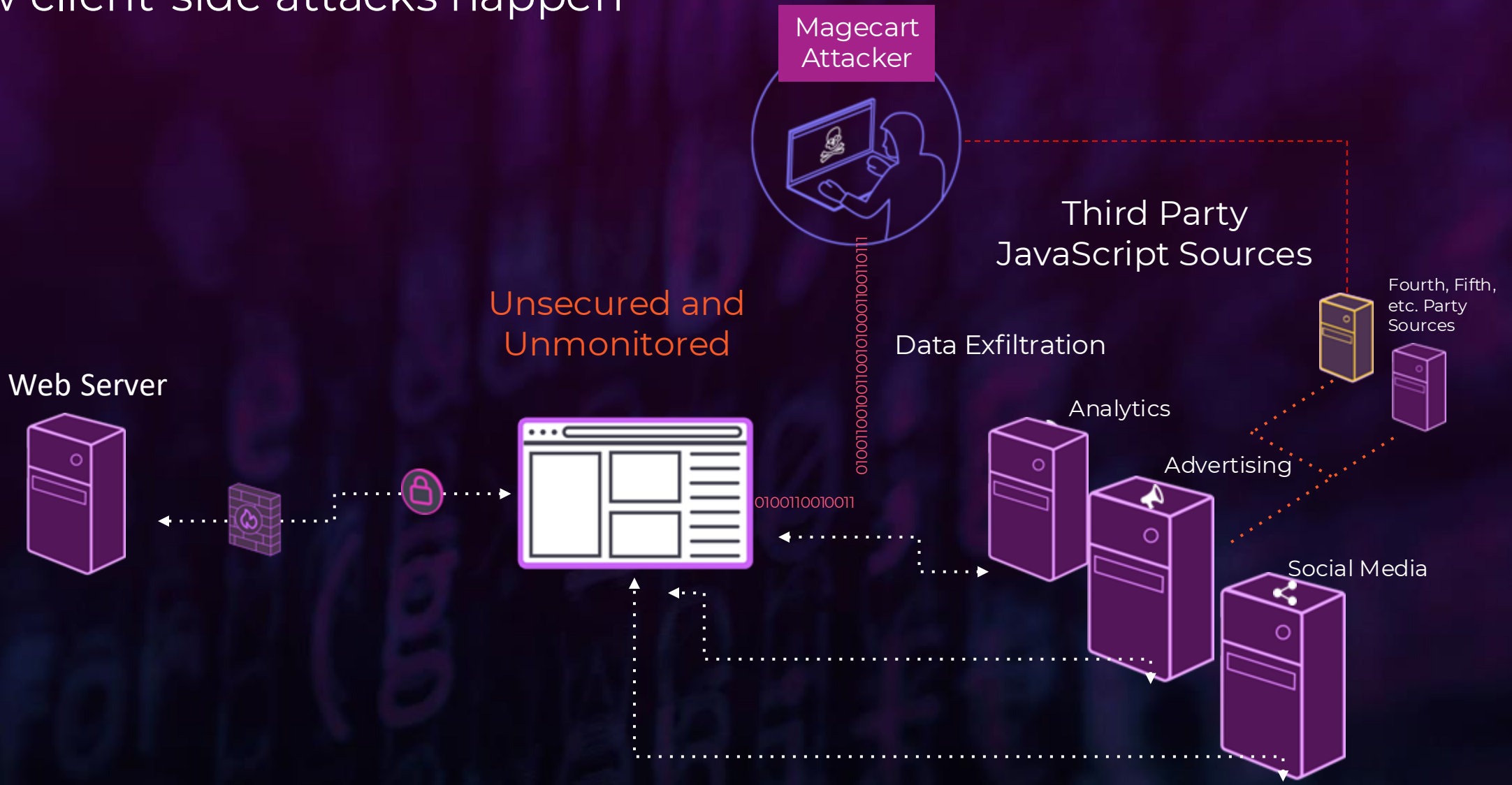


What is a client-side supply chain attack?

source DEFENSE



How client-side attacks happen



PCI DSS 4.0

source DEFENSE

PCI DSS v4.0
Requirement 6.4.3

Requirements and Testing Procedures	
Defined Approach Requirements	**Defined Approach Testing Procedures**
6.4.3 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 business or technical justification as to why each is necessary.	**6.4.3.a** Examine policies and procedures to verify that processes are defined for managing all payment page scripts that are loaded and executed in the consumer's browser, in accordance with all elements specified in this requirement. **6.4.3.b** Interview responsible personnel and examine inventory records and system configurations to verify that all payment page scripts that are loaded and executed in the consumer's browser are managed in accordance with all elements specified in this requirement.
Customized Approach Objective	
Unauthorized code cannot be executed in the payment page as it is rendered in the consumer's browser.	

1. **Inventory payment page scripts**
2. **Confirm authorization and provide a justification for each payment page script**
3. **Implement a method to assure the integrity of each payment page script**

source DEFENSE

PCI DSS v4.0
Requirement 11.6.1

Requirements and Testing Procedures	
11.6 Unauthorized changes on payment pages are detected and responded to.	
Defined Approach Requirements	**Defined Approach Testing Procedures**
11.6.1 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).	**11.6.1.a** Examine system settings, monitored payment pages, and results from monitoring activities to verify the use of a change- and tamper-detection mechanism. **11.6.1.b** Examine configuration settings to verify the mechanism is configured in accordance with all elements specified in this requirement. **11.6.1.c** If the mechanism functions are performed at an entity-defined frequency, examine the entity's targeted risk analysis for determining the frequency to verify the risk analysis was performed in accordance with all elements specified at Requirement 12.3.1. **11.6.1.d** Examine configuration settings and interview personnel to verify the mechanism functions are performed either: • At least weekly **OR** • At the frequency defined in the entity's targeted risk analysis performed for this requirement.
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. *(continued on next page)*	

1. **Monitor HTTP response headers**
2. **Monitor payment page script contents**

source DEFENSE

In a nutshell

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**