ECOMMERCE SECURITY TRENDS

Findings from SecurityMetrics' Ecommerce security service

SecurityMetrics Shopping Cart Inspect helps businesses detect if their Shopping Cart has been breached.

With the help of Shopping Cart Inspect, SecurityMetrics Forensic Analysts review businesses' rendered webpage code on their shopping cart URL to collect evidence of a skimming attack.

25.3%

of inspected ecommerce sites had malicious issues.

TRENDS FROM 2021 SECURITYMETRICS SHOPPING CART INSPECT INVESTIGATIONS

88.89%

88.89% of Shopping Cart Inspect reviews identified malicious, suspicious, and/or concerning issues on researched ecommerce sites.

1.88 issues

Average number of issues identified in a Shopping Cart Inspect review.

25.3% of inspected ecommerce sites had malicious issues.

63.86% of inspected ecommerce sites had suspicious issues.

33.73% of inspected ecommerce sites had concerning issues.

TOP 5 MALICIOUS ISSUES FOUND

1. Malicious Javascript
Javascript appears to be acting in a malicious manner, such as harvesting credit cards or other sensitive data.

2. Malicious Post
A script is running with a post of data to a known bad site.

3. Form Jacking
Authorized payment webform is being replaced by a counterfeit.

4. Directory Browsing Enabled
Directory Browsing is enabled on the web pages analyzed.

5. Malicious Double Checkout
Double post of credit card data returning to alternate checkout page on merchant's server.

TOP 5 SUSPICIOUS ISSUES FOUND

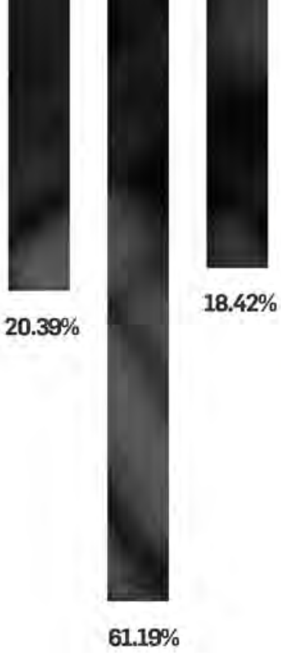
1. Javascript issue
Out of date JavaScripts can lead to vulnerabilities available for future malicious attacks.

2. Out of date CMS - Suspicious
Out-of-date web components. Unpatched or un-updated software is a leading cause of sites losing sensitive data.

3. Ads/Business Intelligence
Advertising/Analytics content is being pulled into the pages being reviewed in the checkout environment. This can be a source of intermittent card/data loss due to drive-by malvertising.

4. Configuration Issue
Missing required web server security headers.

5. iFrame Source Issue
iFrame source appears to be suspicious or improperly configured or protected. Attackers often change the iFrame source to point to malicious web forms. iFrame may be misconfigured, allowing cross-site scripting attacks.



18.42% of issues were malicious

Malicious: Evidence of card data being stolen. (*Highest threat level*)

61.19% of issues were suspicious

Suspicious: Identified issues increase the probability of a potential exploit. (*Medium threat level*)

20.39% of issues were concerning

Concerning: Unlikely method of being breached, but identified issues could lead to a potential exploit. (*Low threat level*)

TOP 5 CONCERNING ISSUES FOUND

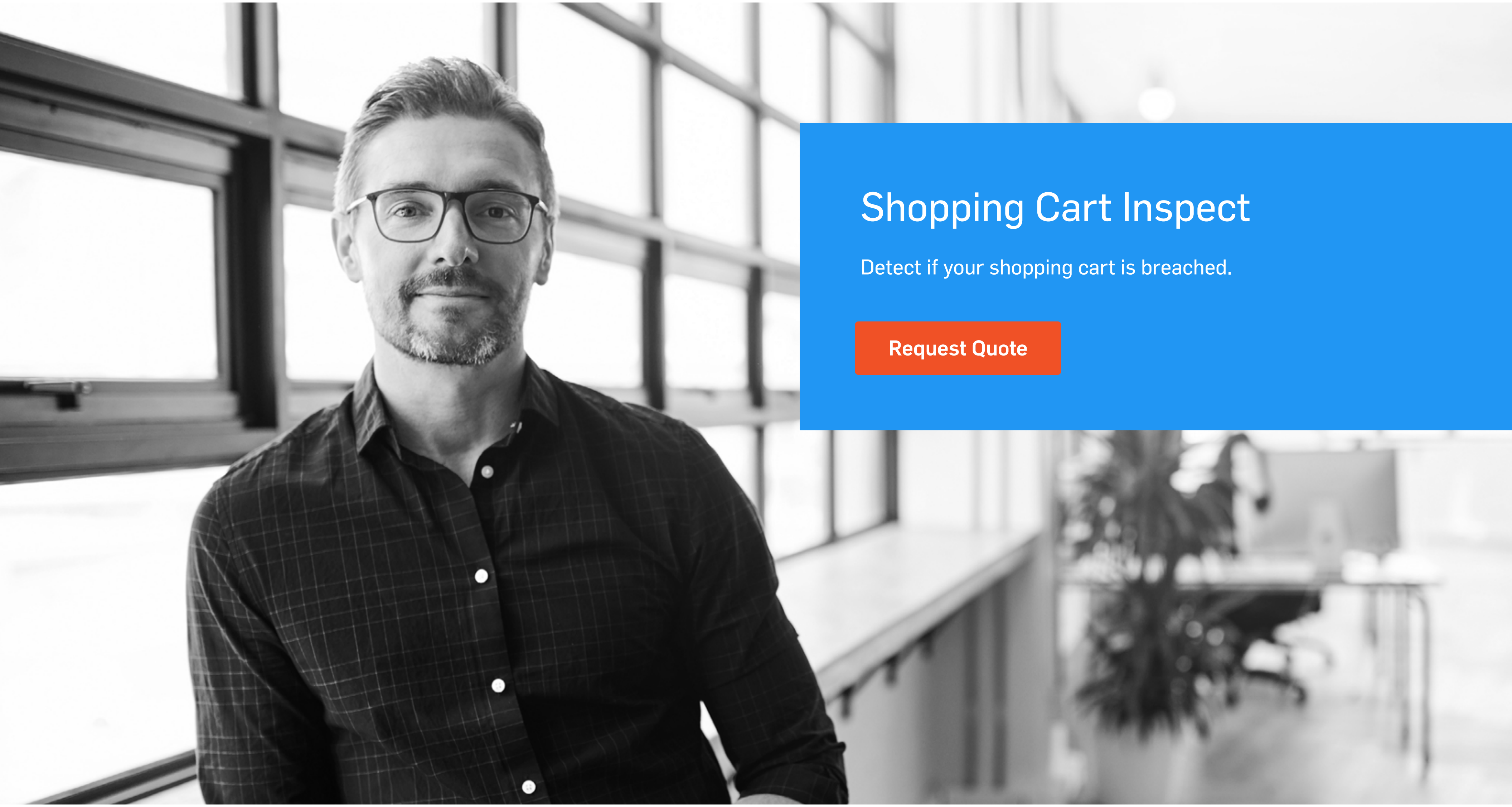
1. Configuration Vulnerability
A configuration item with a website or web server is not following best security practices.

2. Checkout Configuration Issue
The implementation of certain aspects of the checkout process may not follow best security practices and could leave merchants vulnerable to certain types of attacks

3. Out of date CMS - Concerning
Out of date web components, which would be unlikely to lead to a breach of site security but should be updated.

4. HTTP Header Issue
Improperly configured HTTP headers can provide attackers with specific information about your web server setup, such as vulnerable software versions.

5. Mixed HTTP/HTTPS
Content called via HTTP in an HTTPS environment, breaking strict SSL/TLS protocol. In severe cases, this can be exploited by bad actors to view privileged content.



Shopping Cart Inspect

Detect if your shopping cart is breached.

Request Quote

© 2022 SecurityMetrics | 1275 W 1600 N | Orem, UT 84057 | www.securitymetrics.com