jscrambler

E-Commerce security threats

A data sheet by Jscrambler

E-commerce is at an all-time high

People shopping online has been growing over the past few years. One in three people you see around you is an online shopper.

2023
has 80 million more digital buyers than in 2022

2024
e-commerce global sales will likely surpass $7 trillion in value

33.3%
of the population worldwide belongs to the digital buyer category

Attacks targeting E-commerce are growing

The client-side of E-commerce platforms has **too many security gaps**. Attackers are taking advantage of this and the cost of attacks is growing.

E-commerce
skimming cases increased 174% in the 2022 June-November period compared to December 2021 and May 2022

78%
of online shoppers think twice about buying from an online retailer after a breach

75%
of all breaches Visa investigated in 2022 involved e-commerce sites

The security threats to E-commerce

Organizations have zero client-side visibility and are still underprepared

41%
of consumers trust digital service providers to keep personal data secure

Up to 5%
E-commerce user sessions hijacked by pop-up ads and malicious extensions

3.6%
Annual E-commerce revenue lost due to malicious bots

Key business threats

Data breaches including payment card information, user credentials, or personally identifiable information (PII).

Heavy GDPR/CCPA fines following data breaches, which can amount to several hundred million dollars.

Lack of PCI DSS compliance by failing to ensure that third parties cannot leak payment card information.

Revenue losses from hijacked user sessions, bots and declining customer trust after data breach incidents.

Client-side attacks to E-commerce

Magecart web skimming attacks

E-commerce platforms rely heavily on third-party JavaScript (analytics tools, chatbots, etc). Cybercriminals are targeting the providers of these tools, launching supply chain attacks that inject web skimmers on the E-commerce websites, leaking user data and remaining undetected for months.

Customer Journey Hijacking

Browser extensions, malicious ads and price comparison tools can change how websites are displayed to end-users, diverting them to competitors' websites or scam pages.

Automated Abuse (Bots)

By manipulating the client-side code of E-commerce websites, attackers can create sophisticated bots that buy limited items before legitimate users, create fake accounts, scrape product details and perform other malicious activity.

Intellectual Property Theft

With growing competition in E-commerce, IP theft has become more prevalent. Because client-side JavaScript is exposed by default, competitors can freely retrieve proprietary logic, putting competitive advantages at stake.

Application security that drives more business

Key business threats

Minimize exposure to data breaches, by protecting JavaScript code and preventing client-side attacks like Magecart web skimmers.

Win back revenue lost from customer hijacking, by blocking pop-up ads, price comparison tools and malware and ensuring that the website is always displayed as designed.

Prevent highly-evolved bot attacks that evade bot detection solutions, by protecting JavaScript code, preventing bypass and vastly increasing the cost of creating new bots.

Code Integrity protects the source code of your E-commerce platform

Enterprise-Grade Application Shielding

With Jscrambler's resilient obfuscation, environment checks and defenses against malicious modification/injection of code, attackers won't be able to reverse engineer, debug or tamper with your app's JavaScript and native code.

Best-in-Class Runtime Protection

Give self-defending capabilities to your E-commerce platform, which will detect debugging/tampering attempts and trigger countermeasures like breaking the application.

Webpage Integrity secures your platform against malicious code

Full Client-Side Visibility

Monitor the behavior of each of your website's scripts in real-time, see the full details of each detection and receive warnings for critical security threats.

Increase compliance with regulations and standards such as GDPR, CCPA and PCI DSS by gaining client-side visibility and control.

Webpage Threat Mitigation
Mitigate client-side attacks to your website in real-time regardless of the attack vector and ensure it is always displayed as designed. Prevent Magecart web skimmers, data leakage, automated abuse and customer hijacking.

References

Jscrambler Infographic: “Your Online Shopping Form is a Hacker’s Favorite Store”, https://jscrambler.com/blog/checkout-forms-holiday-season

IBM, Cost of a Data Breach Report 2023, https://www.ibm.com/reports/data-breach

Visa Spring 2023 Biannual Threats Report, https://cdn.visa.com/dam/visa/vgb/visanotification/PFD-Biannual_Report_December_2022_Public-ACCESSIBLE.pdf

If you want to know more about how Jscrambler can help you prevent client-side attacks, don't hesitate to contact us.

hello@jscrambler.com | +1 650 999 0010