jscrambler

JavaScript security threats

A data sheet by Jscrambler

JavaScript powers the whole web

JavaScript enables companies, from startups to enterprises, to develop **highly advanced web, mobile, and desktop apps in record time.**

97%
modern web apps using JavaScript

100%
fortune 500 companies using JavaScript.

>55
mobile apps using JavaScript

Attacks to JS are profitable and growing

Because JavaScript can't be feasibly encrypted and often has to be placed on the client-side of applications, **it greatly increases their attack surface.**

Globally,
an estimated 30,000 websites are hacked each day

USD 4.45 million
is the global average cost of a data breach in 2023, a 15% increase over 3 years

19%
of all cyber security incidents in 2022 were caused by supply chain attacks

The threats of exposed JavaScript

Key business threats

Loss of customer data including payment card info, user credentials, or personally identifiable information (PII).

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

Loss of revenue, as attackers can bypass restrictions and redistribute the app.

Loss of competitive advantage, as competitors can retrieve proprietary logic and uncover business or technology secrets.

Main attacks to JavaScript applications

Automated application abuse

Attackers can use bots to exploit a web application's functionalities and gain illegitimate access or privileges. Attack automation often requires manipulating the app's JavaScript source code.

Cheating and piracy

By easily accessing the app's source code, attackers can tamper with it to gain advantages in HTML5 games or bypass protections such as DRM or watermarking in OTT players.

Intellectual property theft

Companies often have to place important algorithms in the client-side of their applications. As so, this proprietary logic can easily be obtained by competitors.

Data exfiltration

JavaScript is commonly used to create web forms that handle sensitive logic such as credit card data or user credentials. If this JavaScript is exposed, attackers can tamper with this logic to exfiltrate data.

Companies are still underprepared

83%
of breaches in 2023 involved external actors

Only 12%
of insider-related incidents were contained in less than 30 days

87%
of all detected threats in 2022 are from third-party vendors and suppliers or malicious actors

Enterprise JavaScript meets enterprise security

Key business threats

Protect IP and important algorithms that are vital to your competitive advantage by preventing reverse engineering.

Minimize exposure to data breaches by preventing attackers from tampering with the code that handles authentication or sensitive operations.

Jscrambler secures the client-side of your application

Polymorphic JavaScript obfuscation

Jscrambler is the only solution that offers Enterprise-grade polymorphic JavaScript obfuscation, transforming your code so that it's extremely hard to reverse-engineer.

JavaScript Code Locks

Jscrambler provides a series of code locks that enable you to restrict app execution to trusted environments, such as specific browsers, OSes, non-rooted/jailbroken devices, and more.

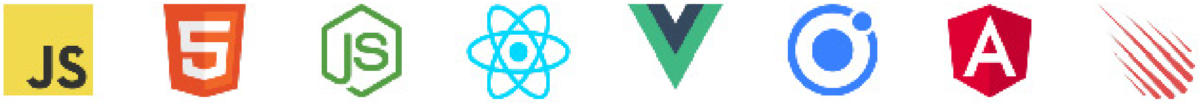
Enforce licensing agreements by ensuring your code can't be changed by attackers attempting to bypass restrictions.

Self-defending capabilities and countermeasures
When your protected code faces a debugging or tampering attempt, Jscrambler's integrity checks break the application or trigger a countermeasure specified by you.

Improve compliance with regulations and standards such as PCI DSS, GDPR, CCPA, NIST and OWASP guidelines by maximizing your app's resilience.

Real-time notifications
Jscrambler warns you if your JavaScript Code is being debugged, tampered, or used outside a code lock, enabling you to immediately take any supplementary actions. Easily integrates with your SIEM to enable real-time threat mitigation.

Compatible with the main frameworks and stacks



References

Verizon 2023 Data Breach Investigations Report: https://www.verizon.com/business/resources/reports/dbir/

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

Annual Threat Trends Analysis by CybelAngel: https://discover.cybelangel.com/2023-state-of-the-external-attack-surface

Accenture, State of Cybersecurity Resilience 2023: https://www.accenture.com/us-en/insights/security/state-cybersecurity

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