jscrambler

Security threats to gaming/gambling apps

A data sheet by Jscrambler

JavaScript and HTML5 power the whole web

JavaScript and HTML5 enable companies, from startups to enterprises, to develop **highly advanced web apps and games in record time.**

97%
Modern web apps using JavaScript

100%
Fortune 500 companies using JavaScript

85%
Websites using HTML5

Attacks to JS/HTML5 are growing

Because JavaScript and HTML5 can't be feasibly encrypted and often have to be placed on the client-side of applications, **it greatly increases their attack surface.**

Fake apps
can reside for months on Google Play or the App Store before they get removed

Gaming apps
are often targeted by hackers, especially massively multiplayer online games

60%
of online gamers have had their experience negatively impacted by other players cheating

The Threats of Exposed JavaScript and HTML5

Key business threats

Loss of revenue, since players can tamper with client-side logic to cheat and unlock paid features. Attackers may also create copycat apps and monetize them.

Loss of player engagement, as users are prone to abandoning the game when cheaters modify leaderboards and gain illegitimate advantages.

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

Main attacks to gaming/gambling apps

Cheating and piracy

Players can easily access the app's JavaScript/HTML5 source code and tamper with it to access locked features or reverse-engineer it to distribute copycat apps.

Transaction fraud

Attackers may tamper with the logic behind in-app payments, rewards, or mobile wallets, potentially hijacking transactions. Any type of client-side payment processing code is prone to attacks.

Intellectual property theft

Competitors may retrieve and reuse any type of first-party code such as proprietary algorithms, posing a direct threat to your competitive advantage.

Lack of compliance with regulations, as attackers may tamper with transactions.

Automated application abuse
Attackers can use bots to exploit app functionalities and gain illegitimate access or privileges. This attack automation often requires manipulating the app's JavaScript source code.

Securing JavaScript/HTML5 in gaming & gambling apps

Key business threats

Safeguard revenue streams by reducing the attack surface for cheating and protecting anti-cheating JavaScript agents.

Minimize exposure to piracy and copycat apps by making it extremely hard for attackers to reverse-engineer the code, plus restricting app execution.

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 allows you to define the environment where the app is allowed to run. Lock to specific domains, browsers, and OSes, and enforce expiration dates for trials.

Minimize exposure to transaction fraud by protecting important code that handles payments, rewards, or users' wallets.

Keep intellectual property secure by using runtime defenses that prevent static and dynamic code analysis.

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.

Real-time notifications
Jscrambler warns you if your code is being debugged, tampered with, or used outside a code lock, enabling you to immediately take any supplementary actions.

References

Irdeto Global Gaming Survey Report, 2018, https://resources.irdeto.com/irdeto-global-gaming-survey

NordVPN, How to spot a fake app, January 1, 2023, https://nordvpn.com/pt/blog/fake-apps/

W3 Techs, "Usage statistics of HTML5 for websites", October 2020, https://w3techs.com/technologies/details/ml-html5

C. Cimpanu, "Google Removed Over 700,000 Malicious Android Apps From the Play Store in 2017", January 30th, 2018, https://www.bleepingcomputer.com/news/security/google-removed-over-700-000-malicious-android-apps-from-the-play-store-in-2017/

J. Rajasegaran et al., "A Multi-modal Neural Embeddings Approach for Detecting Mobile Counterfeit Apps", May 2019, https://doi.org/10.1145/3308558.3313427

Proofpoint, "Is nothing sacred? Risky mobile apps steal data and spy on users", December 2015, https://www.proofpoint.com/us/threat-insight/post/Risky-Mobile-Apps-Steal-Data

Kroll, "2021 Data Breach Outlook", June 2021, https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2021

N. Granados, "Report: Cheating Is Becoming A Big Problem In Online Gaming", April 30th, 2018, https://www.forbes.com/sites/nelsongranados/2018/04/30/report-cheating-is-becoming-a-big-problem-in-online-gaming/

Accenture, "The Cost of Cybercrime", 2019, https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Ponemon Institute, "Data Risk in the Third-Party Ecosystem", November 2018, https://promotions.opus.com/l/12092/2018-11-14/6bj4g6

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