CASE STUDY

Strengthening Biometric Protection with Jscrambler & Build38

build38 jscrambler BUILD38.COM

How Jscrambler & Build38 Strengthened Biometric Security

A joint effort to secure biometric authentication

INTRODUCTION

A London-based identity verification provider and one of Europe's leading biometric vendors partnered with Build38 and Jscrambler to deliver advanced, cross-platform protection against digital fraud.

By securing their unique approach to passwordless authentication—which verifies users without storing any biometric data—they successfully mitigated the risk of unauthorized account access.

This collaboration enabled the company to expand its biometric authentication security from mobile app to web, providing users with a unified, frictionless, and highly secure experience across all devices.

Industry
Identity verification

Headquarters
London, UK

Use case
SDK protection

With Jscrambler since
2025

ABOUT

Our provider delivers a passwordless, multi-factor authentication approach that relies on biometric verification while safeguarding user privacy by storing no biometric data. This solution helps mitigate unauthorized account access and streamlines secure authentication across various devices

THE ROLE OF BIOMETRIC AUTHENTICATION IN FRAUD PREVENTION

Biometrics is transforming fraud prevention by anchoring identity to something uniquely human rather than a password or card that can be guessed, stolen, or shared. Traits such as fingerprints, facial recognition, or voice patterns are extremely difficult to replicate, making impersonation far less likely.

This has made biometrics a critical safeguard in digital transactions, where reducing account takeovers and fraudulent payments is a top priority. Beyond finance, it is also finding growing applications in healthcare to secure patient records, and in government services, to verify citizens with greater confidence. The result is stronger security paired with a smoother, more trustworthy user experience across sectors.

How Jscrambler & Build38 Strengthened Biometric Security

Confronting new fraud challenges in user authentication

CHALLENGE

The company had previously partnered with Build38 to protect its mobile SDK against video injection attacks, in line with CEN standards. It then sought to implement comparable safeguards for its web channel, where threats like synthetic or replayed video streams could undermine liveness verification mechanisms.

The organization detected two distinct attack vectors targeting its web SDK: crafted video injection and virtual camera bypass.

CRAFTED VIDEO INJECTION

An attacker could tamper with the DOM by removing the **ImageCapture** global, causing the Web SDK to revert to drawing frames directly from the video element rather than from the stream. Under these cirumstances, the attacker could replace the video element's source attribute with a maliciously prepared video hosted on a public URL.

VIRTUAL CAMERA BYPASS

In this scenario, the attacker monitors for the presence of the solution provicamera element in the DOM. When detected, they could alter the constraints attribute to enforce the use of a specific device ID—such as that of a virtual camera (e.g., OBS)—effectively bypassing normal camera selection controls.

Ensuring compliance with LoIP and eIDAS 2.0 standards

The company also needed to meet the injection attack protection requirements for the Extended Level of Identity Proofing (LoIP), a core condition for EUDI wallets seeking to offer full identity services under eIDAS 2.0.

The client's team looked for a solution to defend against these attacks, specifically, custom element tampering, to prevent manipulation and reverse engineering of their SDK, and to protect their secure business apps.

How Jscrambler & Build38 Strengthened Biometric Security

Combining strengths for complete platform security

SOLUTION

Having already trusted Build38 to secure its mobile SDK against video injection and reverse-engineering attacks, the team sought to extend the same certified level of protection to its web SDK.

The objective was to create a unified, cross-platform defense that could withstand sophisticated fraud techniques while maintaining an effortless user experience. To achieve this, the company selected Jscrambler's Code Integrity to shield its JavaScript code from runtime manipulation, DOM tampering, and reverse engineering.

BUILD38'S MOBILE SDK SECURITY

Build38 provided the foundation for mobile SDK security, safeguarding app integrity, preventing tampering, and ensuring compliance with CEN/TS 18099 — the European standard for injection attack detection

JSCRAMBLER'S CODE INTEGRITY TECHNOLOGY

Jscrambler extended this protection to the web SDK through its Code Integrity technology, which shields JavaScript code from runtime manipulation, DOM tampering, and reverse engineering.

Build38 and Jscrambler partnered on a proof-of-concept (PoC) during which real-world attack scenarios were simulated to evaluate the solution. To counter these threats, Jscrambler deployed its anti-DOM tampering and anti-monkey patching capabilities and Code Integrity protection features.

The PoC focused on two primary objectives: performance and code security. The implementation needed to operate seamlessly, preserving the user experience while effectively defending the application against simulated attacks. Jscrambler's library met both requirements, protecting the code without compromising speed, which ultimately led the organization to move forward with a full license.

DEVELOPMENT LEAD AT THE IDENTITY VERIFICATION PLATFORM

>We jumped on a call with the Jscrambler team and got very good guidance about what we needed to do. It was easy to set up, easy to fine-tune when it needed fine-tuning, and that was it. Then we let it run_

How Jscrambler & Build38 Strengthened Biometric Security

Delivering resilient, cross-platform protection

RESULTS

By combining the strengths of Build38 and Jscrambler, the identity verification company achieved a comprehensive, end-to-end security solution. Build38 provides protection for the mobile application, while Jscrambler's Code Integrity technology secures the web SDK with runtime protection, making it resilient to tampering.

UNIFIED CLIENT-SIDE PROTECTION

The customer now has a unified security solution that protects its platform across both mobile and web channels. This is essential for protecting sensitive data and ensuring fraud-free identity verification

RELIABLE-AT-SCALE PERFORMANCE

The Jscrambler solution was proven effective against the attacks the customer wanted to test, while maintaining excellent performance and ensuring a secure, seamless user experience.

MITIGATION OF SDK SECURITY RISKS

This partnership demonstrates how companies can proactively address SDK security risks by implementing runtime protection and robust client-side security.

Ultimately, Jscrambler and Build38 enabled the identity verification customer to extend their leadership in biometric authentication by ensuring their web channel is as secure as their mobile one, ensuring the same trusted protection across web and mobile experiences.

- Discover how Build38 protects mobile apps and digital identities.
- See how Jscrambler strengthens web application security.

About Build38

Your trusted Mobile Application Security partner

Build38 is a leading cybersecurity firm specializing in mobile application security. Our expert team provides comprehensive security solutions designed to protect mobile applications from a wide array of threats. With a focus on the fintech sector, Build38 offers tailored services that ensure the integrity, confidentiality, and availability of your mobile applications.

For more information, visit www.build38.com.

About Jscrambler

Jscrambler is the leader in Client-Side Protection and Compliance. Jscrambler is the first to merge advanced polymorphic JavaScript obfuscation with fine-grained third-party tag protection in a unified Client-Side Protection and Compliance Platform. Jscrambler's integrated solution ensures a robust defense against current and emerging client-side cyber threats, data leaks, misconfigurations, and IP theft, empowering software development and digital teams to innovate securely online with JavaScript.

For more information, visit www.jscrambler.com

Disclaimer

This case study is intended for informational purposes only and reflects the findings based on the analysis conducted internally by Build38. It does not guarantee the absolute security of any mobile application and recommends continuous security evaluations to address emerging threats.