jscrambler

HOW JSCRAMBLER HELPS SUPER SECURE THEIR IONIC APP

Case Study

> **Jscrambler solved the majority of our concerns and the implementation process was very easy.**
>
> Willy Haryanto- Chief Technology Officer at Super

Introduction

About Super

As the first social commerce platform in Indonesia that is ISO 9001:2015 certified, Super aims to solve economic inequality across cities for Indonesia's future economy.
Super is also the first consumer technology company in Indonesia backed by Y Combinator, which oversees the main feature, SuperAgent, which is agent-led commerce that enables community leaders to become retailers within the communities.

Super empowers young people in the rural area to become self-made entrepreneurs by becoming our Super Agent; to sell goods to their communities and help them improve their family finances. Super provides more than 2000 SKUs of FMCG products for our Super Agent to sell, ranging from rice, cooking oil, milk, coffee, seasonings up to mosquito coils with the best price.

Super's Vision

"To solve Indonesia's economic inequality distribution across tier 2, tier 3 cities and rural areas. By building agent networks that aggregate demand in rural areas and by building hyperlocal supply-chain to make goods more affordable for the villagers. "

JavaScript Framework and Security Concerns

Super approaches software development with Agile in mind. Speed and agility are part of the company's competitive advantage. Super develops mobile apps using modern hybrid JavaScript frameworks, such as the Ionic framework.

Implementing JavaScript as their main tech stacks, Super is aware of the security gaps or flaws that are inherently present in mobile apps—code tampering, reverse engineering, data exfiltration and many others. With these in mind, Super made it a requirement to secure its JavaScript code with an enterprise-grade solution.

jscrambler

Summary

Challenges

- Obfuscate private API functionality.
- Prevent code tampering.
- Prevent reverse-engineering.

Solutions

Jscrambler Code Integrity:

- Polymorphic JavaScript obfuscation.
- Built-in protection against reverse-engineering tools.
- Self-defensive capabilities to stop tampering and debugging attempts.

Results

- Simple and fast implementation.
- Seamless integration with Ionic's build process.
- Successful mitigation of tampering and reverse engineering attempts at runtime.

Challenges

When choosing the tech stack they wanted to use for their application, Super privileged the fast adaptation and familiarity of the development team and decided to go with **Ionic**, a popular **cross-platform JavaScript framework.**

Soon after developing their application, the company understood there were some specific security concerns linked to using JavaScript. Specifically, every piece of **client-side JavaScript code is exposed at the client-side** and can be retrieved by attackers.

That is exactly what Super wanted to prevent: malicious users going through the source code of the company's app, in an attempt to make illegitimate use of the API key and access sensitive data, such as transactional and personal information.

To ensure that their JavaScript source code couldn't be used as a vector for these client-side attacks, Super made it a requirement to protect their JS source code and all the sensitive information it contained.

Solution

While searching for a security solution that met the company's specific needs, Super came across several options, but after trying out Jscrambler and seeing all the information they could access about threats in real-time, they decided to move forward.

> **"Jscrambler's Dashboard gave us detailed threat information and allowed us to monitor performance. It made us feel like we found the right solution.**

To protect their source code, Super leveraged one of Jscrambler's key features, **polymorphic JavaScript Obfuscation**, which includes several different techniques that transform the original source code into a new version that is extremely hard to understand and reverse-engineer, while keeping its original functionality. This security layer also includes Jscrambler's **Code Hardening** feature, which provides up-to-date protection against all reverse-engineering tools and techniques.

Then, Super also used the Jscrambler **Self-Defending capabilities**, which add **integrity checks** and other **runtime defenses** to **prevent attackers from debugging or tampering with the code.** As such, if anyone tries to debug or tamper with Super's app at runtime, it will immediately break and prevent the attack from even unfolding.

The combination of these layers greatly **reduces the attack surface** of Super's application, making it much harder for attackers to understand the logic behind the program, stopping them from getting access to sensitive information.

Results

The team at Super encountered no issues when getting started with Jscrambler, especially due to the **straightforward process.**

“Setting up Jscrambler was very easy, we had no troubles in quickly getting things ready to go.”

The company’s team also saw the value in Jscrambler’s detailed Ionic guide, which allowed them to effortlessly integrate Jscrambler into Ionic’s build process, ensuring that every new app build is protected before deployment.

Looking back at Super’s requirements, the company had an extensive checklist of application security challenges and Jscrambler managed to fulfill the vast majority of them, by providing in-depth protection of their app source code.

With Jscrambler’s thorough obfuscation and runtime solution, Super was able to address their main concerns, preventing reverse-engineering and tampering attempts.

> **“ Jscrambler solved the majority of our concerns and the implementation process was very easy.**

Contact Us

If you want to know more about how Jscrambler can help you secure your web and mobile applications, don't hesitate to contact us

hello@jscrambler.com

+1 **650 999 0010**

Trusted by the Fortune 500 and major companies in Finance, Broadcasting, Software Development, E-Commerce, and Healthcare.