

CASE STUDY

How Jscrambler Helps dotConnect Deliver Secure Banking Apps



“Since integrating Jscrambler, we have consistently passed strict penetration testing and delivered secure mobile banking apps to our clients.”



Mohamed Gamil, CEO & Founder of dotConnect

Overview

Developing Highly Advanced Banking Apps

dotConnect is a fintech with the vision to empower financial institutions to provide their clients with a platform that delivers an exceptional **digital banking experience**. Via cloud native solution architecture that is built for scale and resilience, dotConnect allows banks to accelerate their digital transformation and automation journeys. This enables these banks to provide a modern, customer-focused digital experience, reduce operational service requirements, and **achieve low and predictable operational costs**, while also guaranteeing flexible integration with new and legacy banking systems using a decoupled approach.

*“Our clients are always concerned when it comes to cloud applications and services. That’s why we partner and integrate with **field specialists and market-leading vendors.**”*

Betting on Best-of-Breed Security Tech

To ensure maximum reliability and security, the dotConnect multi-tenant platform separates sensitive data and components into distinct “tenants”. It adheres to the Application Security best practices outlined by OWASP and affiliates with market-leading specialists such as Microsoft Azure (for cloud services), OneSpan (for secure authentication), GBG (for identity verification), and now **Jscrabler** for the important task of **protecting and securing the source code** of these banking applications.

CHALLENGES

- Add new security layers to protect the source code
- Protect transpiled JavaScript code
- Reduce the overall exposure to client-side attacks
- Pass the bank's strict pen-testing

SOLUTION

Jscrambler Code Integrity:

- Best-of-breed JavaScript obfuscation
- Built-in protection against reverse-engineering tools
- Self-defensive capabilities to stop tampering and debugging attempts

RESULTS

- Simple integration and maintenance
- Using for 2 years with no issues
- Adds a robust security layer
- Increases compliance with OWASP recommendations
- Successfully protecting the banking apps of Al Rayan Bank and UBL UK
- Passed all 5 penetration testing rounds to date with excellent feedback

CHALLENGES

Today, **73% of all consumer interactions with banks are done digitally**. And when it comes to banking, security is a prime directive.

When asked about the most important attributes when choosing a bank, **82%** of consumers say “ensures my transactions are **safe/secure**”.

Being aware of how security is one of the key drivers in the ongoing banking digitalization, dotConnect wanted to ensure that they were developing secure banking apps. This meant **covering every inch of the attack surface**.

When it comes to web and hybrid mobile banking apps, one key security challenge is **protecting the JavaScript code**, which can be targeted by reverse-engineering, tampering, and injection attempts.

This layer of protection is especially important to reduce exposure to **data exfiltration** and **transaction fraud**, which can originate from client-side attack vectors.

*“When you have a financial product out in the public domain, you’re **a prime target for attackers.**”*

As part of the agreement and delivery of a dotConnect implementation to the bank, dotConnect and the bank administer multiple **strict penetration testing rounds** of all their client channels. This is especially common for cloud-based apps, where the attack surface is comprehensively larger than that of legacy banking systems.

Any app that runs in a browser or in a web-view is especially prone to client-side attacks. As such, these pentesting rounds are critical to certify the security of the final app, for the security of both the bank and its customers.

*“The browser is very challenging when it comes to security, especially when the app handles sensitive data. **The stakes are extremely high.**”*

The answer to dotConnect's challenges in terms of source code protection was the cutting-edge technology provided by Jscrambler. Both founders had previously used Jscrambler in a previous solution within the banking sector a few years ago. So, when embarking on this new venture, they re-visited the market to compare vendors and found that Jscrambler was still the market-leading specialist in this sector, thus it was the obvious choice.

Because dotConnect had to ensure maximum protection of the JavaScript source code, its team decided to combine two of Jscrambler's most effective client-side security layers: **JavaScript Obfuscation** and **Self-Defending**.


*"Jscrambler allows for **easy configuration** as well as a security setup with **different levels of evolving protection.**"*

Jscrambler's **polymorphic JavaScript Obfuscation** 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. Included in this layer is Jscrambler's **Code Hardening** feature, which provides up-to-date protection against all reverse-engineering tools and techniques. As stated by UBL UK, this was the feedback of one a penetration tester evaluating the banking app developed by dotConnect and protected by Jscrambler:

*“The protection layer that Jscrambler provides is **very, very difficult to interpret, break or bypass.**”*

On top of this advanced obfuscation, dotConnect uses Jscrambler **Self-Defending**, a security layer that adds **integrity checks** and other **runtime defenses** that **prevent attackers from debugging or tampering with the code**. As such, if anyone tries to debug the protected banking app at runtime, the app will immediately break. Likewise, if an attacker tries to modify the code to dynamically understand its logic at runtime, the application will break to stop the attack.

This advanced runtime protection reduces the attack surface to data exfiltration attacks, by making it much harder for attackers to understand how the software works and plan/ automate these attacks.



```
1 (function (window) == {
2   var canvas = window.document.getElement
3   if (canvas.getContext) {
4     var ctx = canvas.getContext('2d');
5
6     ctx.fillRect(25, 25, 100, 100);
7     ctx.clearRect(45, 45, 60, 60);
8     ctx.strokeRect(50, 50, 50, 50);
9   }
10 })(window)
```

```
uments];V2[4]=2;for(;V2[4]!==259;){switch(V2[4]){case 202:V2=V
2[0][0];},V2[33],V2[28]);C(V2[0][0],function(){var n2=[argumen
2[0][0][V2[57]][V2[34]];},V2[90],V2[29]);V2[4]=269;break;case
4(;S2[9]!==20;){switch(S2[9]){case 5:S2[1]=S2[6];S2[1]+=V2[8
3][0][V2[57]][V2[34]];},V2[18],V2[82]);V2[4]=259;break;case
[0][0];},V2[15],V2[36]);V2[4]=265;break;case 28:V2[89]="";V2[
ch(T5){case 2:return{u2:function t2(j5,c5){var a5=2;for(;a5!==
ction (){return typeof D8aa.R2.c==='function'?D8aa.R2.c.apply(
ch(D2){case 2:return{c:function(1){var j2=2;for(;j2!==10;){swi
ts];h5[9]=w5.W5()[17][12];for(;h5[9]!==w5.W5()[13][18];){switc
```

Original

Obfuscated

Results

dotConnect successfully applied Jscrambler during the development and delivery of the digital banking solutions for **Al Rayan Bank** and **UBL UK**, two fast-growing banking organizations in the UK.

The development team had no issues integrating Jscrambler into the CI build process, thanks to detailed documentation and support from Jscrambler.

*“The integration into our build pipelines was simple, hence **all our apps are protected** and deployed with minimal configuration. It’s a **very comfortable security layer.**”*

Azure DevOps Engineer, dotConnect Development Team

Jscrambler directly helps dotConnect increase compliance with the application security standards outlined by OWASP. Specifically, the **Mobile Top 10 Security Risks guide**, which advises the use of obfuscation technology and runtime protection to prevent **reverse-engineering and code tampering**.

Besides compliance with OWASP guidelines, Jscrambler supports in ensuring dotConnect satisfies the **PSD2 mobile app security criteria**. Namely, adopting security measures to mitigate risk from compromised mobile devices and cloning countermeasures (replication protection).

One of the key requirements of dotConnect was ensuring that they would pass their clients’ and their own strict penetration testing rounds. Jscrambler helped them achieve that by **passing 5 different penetration testing rounds with excellent feedback**, over the course of the last 12 months.

Results

*“Jscrabler played a key role in the penetration testing. With Jscrabler in place, **we have much more confidence in the security of the client-side.**”*

In the 16 months since the Al Rayan banking app was launched, it has been used by over **25,000 customers** for their day-to-day banking. Reinforcing its commitment to providing **secure** online and mobile products and services, the bank will enhance its digital offering in 2021 with further improvements to its mobile banking app.

Although UBL UK is a much more recent launch, everything is shaping up for this to be yet another success case for dotConnect. The implementation is expected to go through further penetration tests as the delivery progresses through its phases but dotConnect is comfortable and confident in the outcome.

For dotConnect, the road ahead looks extremely promising. With customer satisfaction at an all-time high, the company is growing fast and onboarding new banking clients, always assured that Jscrabler will provide **top-notch client-side security**.

*“Jscrabler is a key component that bolsters our security layer, thus assuring us at dotConnect that **we deliver secure and trusted solutions** to our clients and their customers”*

Saj Shahid, CXO & Founder of dotConnect

Contact Us

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

hello@jscrambler.com

+1 650 999 0010

Gartner[®]

Jscrambler is the leader in Client-Side Application Security
Recognized in Gartner's **Market Guide for Online Fraud Detection**
and in Gartner's **Market Guide for In-App Protection**

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