approov
mobile security

CASE STUDY

scoffable.com

Minimizing Revenue Loss and Protecting Sensitive Data for Online Ordering App

"It was our API that we were looking to harden against abuse and potential bad actors attempting to threaten the security and availability of our service."

– Daniel Jones, a Founding Partner, Scoffable

With the increase in online transactions and the use of mobile apps, protecting sensitive data has not only become a part of doing business but a requirement to earn the trust of customers. In order to better serve their customers, Scoffable knew that they needed to secure their online ordering app to include protection against Distributed Denial of Service (DDoS) and data scraping. Approov Mobile Security worked with the security they already had in place to protect against both and secure their API.

The Client

Scoffable, a Scottish technology company founded in 2010, provides a fast and convenient online ordering experience for takeaway consumers. Customers can visit the Scoffable website or download their app to discover nearby takeaways and restaurants, browse menus and order online. Scoffable also makes their online ordering system available to partner takeaways and restaurants to use for their own businesses.

The Challenge

As the mobile channel continues to grow, apps and the APIs that service them are increasingly targeted for malicious purposes. With data breaches on the rise across all sectors, retail apps are particularly vulnerable to a number of threats, including DDoS and data scraping. In the case of data scraping, valuable content or data provided by the API is automatically collected and is then reused or redistributed with malicious intent.

Larger organizations in particular can be targeted because of the amount of data that can be breached. For instance, T-Mobile, Panera Bread, Facebook, Instagram and the McDonald's McDelivery service all had their security breached as a direct result of poorly secured API access.

However, these attacks are not limited to only large organizations, they can happen to any business with API access.

According to Gartner, APIs are one of the fastest growing attack vectors:

"Each new API represents an additional and potentially unique attack vector into your systems.' and 'Attacks and data breaches involving poorly secured application programming interfaces (APIs) are occurring frequently."

(Gartner, API Security: What You Need to Do to Protect Your APIs)

Mobile businesses need to control API access to ensure that requests from illegitimate sources are blocked without any impact on the user experience.

How Approov Mobile Security Helped

The food ordering app market is highly competitive with big investment from some major players. Scoffable understood that it was vital to maintain a responsive and frictionless experience for both users and partner takeaways in order to build and retain brand trust. Any service downtime through a DDoS attack by scripts or bots could result in the loss of revenue or valuable local restaurant data to competitors.

As Scoffable built out support for their partner takeaways and restaurants, their public API infrastructure also grew. Daniel Jones, a Founding Partner at Scoffable, explained that they were looking for a solution that would protect their API from unwanted requests such as scraper bots or malicious activity without adding any friction for legitimate users.

> ***"It was our API that we were looking to harden against abuse and potential bad actors attempting to threaten the security and availability of our service."***

The team at Scoffable had already employed some common techniques to prevent abuse, such as rate limiting, Google reCAPTCHA and the use of Cloudflare's Web Application Firewall product to help protect their services from various threats, including DDoS attacks. However, Scoffable discovered that while Cloudflare's page challenge works great for websites, responding to a challenge page was not available in native apps and Cloudflare actually recommended disabling that functionality in APIs.

It became clear that they would need to find a solution that was purpose built for mobile so they reached out to the Approov team. They were intrigued by the use of signed JWTs (JSON Web Tokens) that could be validated quickly and in conjunction with Cloudflare could solve the DDoS mitigation problem with their APIs.

Daniel explains how this works: *"Cloudflare has a 'workers' product that allows you to run JavaScript code at the Cloudflare edge. What we've ended up with is a solution whereby we validate the Approov JWTs at Cloudflare's edge, taking advantage of their massive network/compute capacity, and only legitimate requests will hit our public API infrastructure."*

Summary

Having successfully deployed Approov, Scoffable's latest generation of Android-based point-of-sale hardware used by their partner takeaways and restaurants to accept orders is now secure from DDoS and data scraping.

Daniel described the next steps: *"Once we had confidence in Approov, we rolled this out across all of our public facing APIs that support both our consumer facing apps and takeaway/restaurant partner apps. In addition to IP-based rate limiting, the Approov JWTs include device IDs could potentially be used as a more robust rate limiting solution (for unauthenticated endpoints). This is something that we would like to explore in the future."*

Finally, we asked Daniel why they chose Approov:

"We couldn't find anything else quite like Approov, for us it solved a number of problems:

- *Preventing non-Scoffable applications from making requests to our public APIs.*
- *Providing a DDoS mitigation solution (in conjunction with Cloudflare).*
- *Reducing legitimate user friction on iOS where Google reCAPTCHA is not native.*
- *Providing a simplified approach to the management of Certificate Pinning."*

We've found this has been a positive learning curve for both teams. While the Cloudflare integration was on Approov's radar, the input from Scoffable has been invaluable, because we now have other customers using it. We look forward to expanding our work together to continually strengthen the security of Scoffable's growing service.

You can learn more about how to secure your API with Approov and Cloudflare in our blog article.

approov
mobile security

Find out more about Approov Mobile Security
www.approov.io