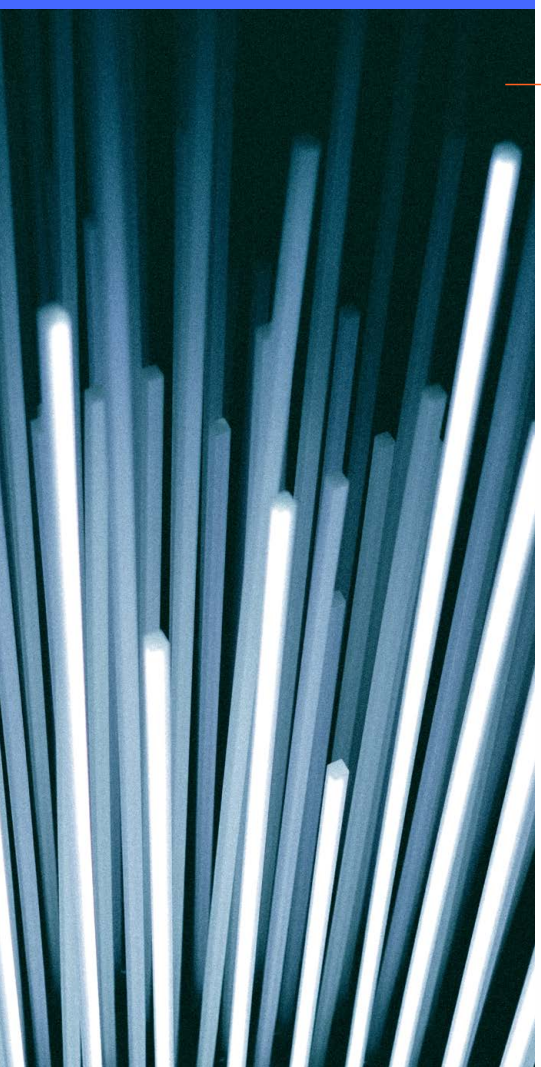
Reflectiz: Revolutionizing eCommerce Website Digital Security Standards

Leading US-based eCommerce business elevates its website digital application security to eliminate Magecart threats.

> We were not sure how many customers were affected by the attack, but we were sure that this issue was going to escalate fast.
>
> CISO,
> Online Retailer



About the Customer

Active since the early 1980s, this major retailer has created an active eCommerce platform in the last few years. With millions of Americans browsing its webpages that boast a huge product catalogue, thousands of transactions are made on a daily basis. This makes it crucial to have a safe and secure perimeter at all times, especially with privacy laws like California Consumer Privacy Act (CCPA) in full effect.

The Problem: Malicious Activity and Data Privacy Issues Caused by Third-parties and Digital Application Induced Blind Spots

This eCommerce vendor had apparently fallen prey to malicious activity, where user accounts were compromised, with personal and payment data allegedly stolen.

While the exact attack-vector was initially unclear, it was quite evident from the get-go that hackers had executed some kind of software supply chain attack by exploiting a third-party web application. **Web-skimming/Magecart techniques were used to exploit the website's payment page, where users unknowingly exposed their private and payment information to the hackers.**

Since the retailer was unaware about the extent of the compromise or for how long the breach lasted, all registered customers received an official email about the hack.

The customer were asked to change their passwords and check their financial statements to make sure that they were on the safe side. Once the damage control was complete, came the stage where security levels needed to be elevated.

But things got worse. **The company was also required to shell out hundreds of thousands of dollars in a CCPA-related lawsuit.**

The Solution: On-Demand Comprehensive Website Analysis for Effective Damage Control

The US-based retailer contacted Reflectiz and results were evident almost instantly. Firstly, the site analysis started on the same day. **Deployment and onboarding were a breeze since no installation was required.** Besides being a next-gen technology, Reflectiz prides itself in offering a solution that doesn't require in-depth technical training. This plug-and-play functionality was crucial in “stopping the bleeding” fast.

The Reflectiz scan was conclusive and pointed at a malicious script that was running on the website. The security team took care of the issue and the hackers were taken out of the picture. But that's not all, Reflectiz also created a detailed breakdown of what happened, while enabling the creation of customized alerts to detect future cases. An entire digital asset inventory clean-up was also performed.

Post-mitigation, an in-depth investigation was carried out with the help of Reflectiz's expert researchers. It was also found that the eCommerce website had fallen prey to a big malicious campaign, affecting hundreds of sites. **This case was very similar to the malicious Gocgle Campaign that Reflectiz experts exposed in 2020, which is still going undetected in hundreds of eCommerce and eService websites.**

The Benefits: Ongoing Digital Application Monitoring with Customized Alerts

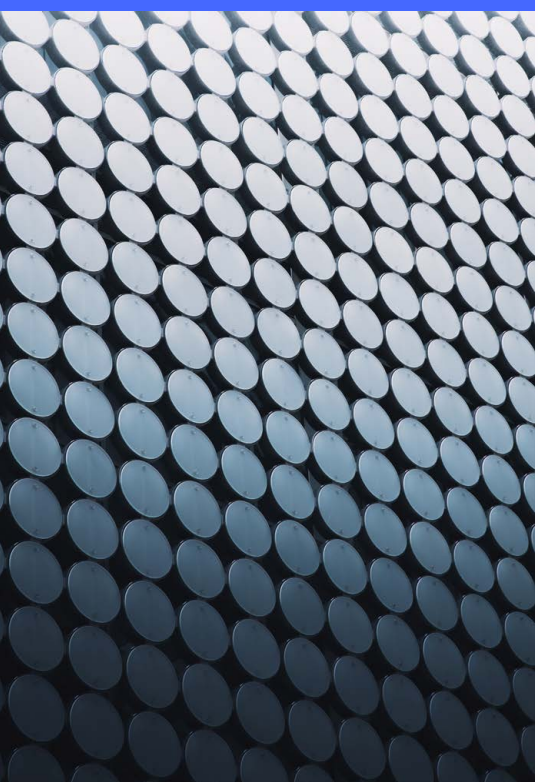
The average eCommerce website is implementing over 60 third-party and other digital applications today. These apps are helping these businesses by minimizing in-house development costs and enabling faster time-to-market. Tag managers, marketing automation tools, analytics software, social media management integrators, payment solutions - these are just a few essential digital applications.

Did You Know?

As per the CCPA, not addressing privacy and security issues on time can lead to fines of up to $7,500 per violation (customer).

> “Discovering and eliminating the dependencies and risks created by your digital applications is essential to achieving CCPA compliance.”

Idan Cohen,
Co-Founder and CEO,
Reflectiz



Not monitoring the dependencies that these apps are creating is leading to exploitable security blind spots, like in aforementioned case. Automated and ongoing analysis of your digital applications help in creating a multi-layered security approach, which is of the essence today.

Implementing a solution like Reflectiz basically allows you to:

1. Learn and monitor your digital web application ecosystem
2. Understand your applications' client-side behavior
3. Set up customized alerts and notifications for enhanced security

Last but not the least, you have the financial aspect of being compliant at all times. As mentioned earlier, not detecting issues or failing to mitigate them can cost you dearly.

For example, if 2000 customer records have been stolen and you have been found to be non-CCPA compliant, damages can reach up to 15 million USD.

That's before we discuss potential lawsuits and brand reputation damages.

Elevate your security and compliance posture with Reflectiz's comprehensive digital web application security solution. Start now.