SECURITY JOURNEY

Software Code

Security Journey Case Study

How a Fintech Streamlined PCI DSS Requirement 6.5 and Increased Developer Engagement

The Fintech Company

The results from the security test did not look good. While all the developers had completed their video-based secure coding training, a requirement to check the box for PCI compliance, it was clear from the final report that some development team members had not fully grasped the content. There were patterns in their coding practices that concerned the company. A portion of the development team had missed simple steps that would have eliminated some vulnerabilities.

The development team received secure coding training to fulfill Requirement 6.5 of the PCI DSS specification. But the company needed to do more than check a requirements box. They had to have improved application security. And what they saw was that they needed a better training solution.

The fintech company that boasts the title of “the first payments unicorn in Mexico, is based in Mexico City. Side note: Mexico is the 12th largest economy in the world. The company provides a wide range of payment solutions that make digital payments simple and easy to access, democratizing financial services in Mexico in the process.

The Company's Requirements

The fintech company had established a set of criteria for evaluating secure coding training solutions to replace their previous solution.

1.0 PCI DSS-specific Content

Fintechs that handle credit card payments and store personally identifiable information (PII) must comply with the PCI Data Security Standard. Requirement 6.5 of the current standard (v3.2.1) requires the company to "Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities." The topics listed in the requirement are covered by the OWASP Top 10. In turn, these became the requirements for baseline training content.

2.0 Simple Compliance Tracking and Reporting

The company wanted to significantly streamline its ability to track and report on completion of the training so that its administrators didn't spend tens of hours monitoring and chasing after developers to wrap-up their training in time. They also wanted to easily provide detailed completion reports for their PCI audit.

3.0 Engaging and Effective Platform

After getting feedback from the engineering team that the video-based training the company had used in the past was boring and repetitive, one of the priorities for the new solution was that the platform had to be engaging. It also needed to be effective in helping the company's developers improve their secure coding knowledge.

4.0 Programming Language Support

The company has hundreds of developers that work in a broad range of different programming languages and they had to be sure the secure coding training supported all of them.

5.0 Comprehensive Content Coverage

The OWASP Top 10 fulfills the basic PCI requirements. However, due to the nature of its business, the company wanted the secure coding training solution to provide lessons on API security and mobile security.

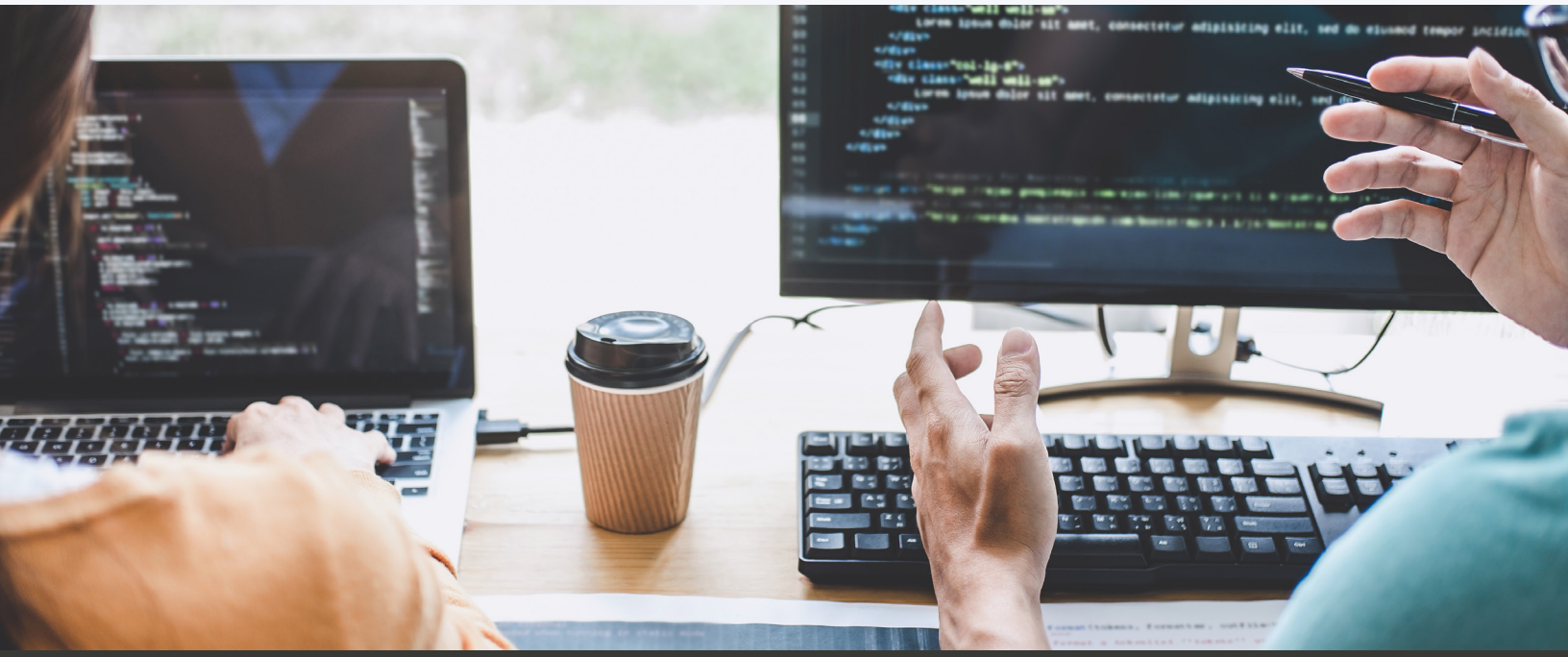
6.0 Ease of Deployment

Since the information security team handles many responsibilities, the solution had to be simple to set up and deploy.

7.0 Buy-in from the Engineering Team

While the information security team was responsible for evaluating and selecting the solution, the engineering team would take the training. Getting their buy-in was critical.

“..it’s easy to track and provide evidence of completion”



The Winning Solution

After carefully evaluating HackEDU's secure coding training platform, the company chose to move forward with them. The platform met all the fintech company's requirements they had set for their developers training. During the proof of concept phase, both the company's security and engineering teams became fans.

"When we tested HackEDU, we found that the challenges and hands-on lessons were attractive for the information security team. Also, for the engineering team, the proof of concept was really attractive. The platform was really cool and interesting".

Simple Deployment

Once the training was rolled out, the company discovered that, not only did HackEDU meet its requirements for a new training platform, it surpassed them in ways they didn't expect.

"It was really easy to set up the platform and integrate all users using single sign-on (SSO). We only had to give them access to the platform, and they already had all the mandated courses set up for them, by team. We did the entire rollout in less than two weeks."

Engagement

"Something that really got my attention was one user found he had access before the official launch, before the official communications, and he completed the training before it even rolled out."

"Even though our developers are very busy, they are making the time to complete the training. That says to me that they really like the training. I even have people approach and ask for access to other training modules that are not required."

Easy Reporting and Audit Compliance

"One of the criteria we had for selecting a platform was really easy reporting and to see how well everyone's doing in their training. What I like is there's a visual to easily see who's not started the courses. We can easily send out notifications and reminders through the Slack integration. For compliance, we can easily download the completion report for the people who have finished everything – it's easy to track and provide evidence of completion. It shows the names and completion dates. That's pretty much what we need from a compliance perspective."

A Nice Surprise

"Even though we've only used the platform for three months, HackEDU has already shown value by adding new content. We really appreciate that, especially since our previous solution used the same lessons year after year."

We help enterprises reduce vulnerabilities with application security education for developers and all individuals involved in creating software. Development teams are empowered through practical, skill-oriented secure coding training that easily satisfies compliance needs and goes beyond to build a security-first development culture.