VERACODE

Empowering Developers to Code Securely with Security Labs

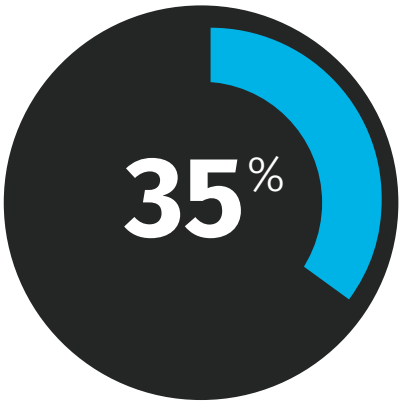
Developers need to know a lot about security at a moment's notice, but slowing down to research fixes can cause a myriad of delays.

Did you know that developers often fix security flaws by spending a great deal of time researching solutions on Google and Stack Overflow? The developers in your organization are often the only ones who can fix the vulnerabilities in their code, and yet they likely don't have the training or foundational security knowledge necessary to effectively identify and remediate flaws. In fact, 35% of organizations say that less than half of their development teams participate in formal security training, and less than 50% require their developers to engage in formal training more than once each year[1]. To top it off, most computer science programs at colleges and universities lack the foundational security education that is so critical to career growth in programming, which means students are often left to form clubs and competitions on their own.

Cyberattacks don't slow down to accommodate these knowledge gaps. They occur frequently (every 39 seconds[2]) and can jeopardize reputations while costing businesses a great deal to clean up. So how do you stay on top of your team's secure coding knowledge to improve their output and bolster the security of your entire organization? Secure code training provided early and often reduces the number of flaws and vulnerabilities developers introduce into their applications. That saves time, money, and sanity, and decreases technical debt that can add up over time behind the scenes. But not all training is created equal.

Effective secure code training doesn't just check a box. It's customizable and engaging, going beyond basic training to empower developers with relevant experience in the languages they use most. Effective developer training helps speed up production releases too—ever written code that's ready to push live only to run it through analysis and discover a list of pesky bugs that can potentially hold up the release? All developers go through these trade-offs, and it often comes with the stress of working alongside unhappy security counterparts in order to fix a critical last-minute issue or make security trade-offs that could leave your organization vulnerable.

With the right training tools, writing secure code doesn't have to be stressful.



35% of organizations say that less than half of their development teams participate in formal security training, and less than 50% require their developers to engage in formal training more than once each year[1].

Code with confidence using Veracode Security Labs.

With Veracode Security Labs, developers are empowered to take ownership over their security training and start using secure coding knowledge right away.

Accessed through a web browser, the lessons ("labs") use containerized, applications and APIs written in the developers' language of choice so that developers can get hands-on with real vulnerabilities and can directly apply these learnings to their code. It's all made possible with:

- Engaging training that features real-world examples of vulnerabilities.
- Interactive, real world scenarios that developers face.
- Detailed progress reporting and a leaderboard to encourage participation.
- The ability to create fun competitions to achieve annual compliance, and spot training for specific topics.

Development teams rely on Security Labs **Enterprise Edition**, which offers hundreds of courses that cover OWASP Top 10, CWE, data privacy, PCI, and more— to enable team members with software security training and practice. While individual developers can also access the complimentary Security Labs **Community Edition**, a limited functionality version of Enterprise Edition, featuring dozens of courses on selected topics anytime they'd like.

Unlike other training solutions that feature lecture-style webinars or mundane training videos, Veracode Security Labs requires hands-on-keyboard code changes that instill muscle memory to make developers more aware of secure coding best practices. They learn to think like an attacker first, exploiting and patching real apps, and then use that knowledge to avoid introducing harmful flaws and vulnerabilities down the road. That makes everyone's job easier, from developer to CISO.

Skills that are gained and refined through Veracode Security Labs are engrained into your developers to improve their coding process so that they're spending less time on security and more time pushing out code that is more secure from the start. It takes just five to ten minutes to get started solving labs, too, which means developers can start proving their skills right away by directly exploiting and patching real code.

Supported languages and frameworks include:

- .NET
- C++
- Golang
- Java
- JavaScript + Node.js
- PHP
- Python (Django and Flask)
- React.js
- Ruby on Rails
- Scala

View Full Course Catalog

The tool of every Security Champion's dreams.

Does a lack of security personnel or subpar communication between security and development cause roadblocks for your organization? A Security Champions program can help you jump those hurdles. Security Champions are developers with an interest in safeguarding software, working to amplify the security message at the team level—but aren't necessarily security pros. They just need to act as the security conscience of the team and stay on the lookout for potential issues.

Bolstering your Security Champions program with Veracode Security Labs helps your organization make up for a lack of security coverage or skills by empowering members of the development team to share best practices, answer questions, and raise security awareness. At the heart of it all is secure coding knowledge, which makes Veracode Security Labs a goldmine of insight for your organization.

With detailed progress reporting in Veracode Security Labs, you'll see where everyone in your organization stands. This gives you the ability to:

- Find advocates for your Security Champions program.
- Highlight leading team members and ask them to share knowledge.
- Publicly share accomplishments with LinkedIn badges.

By incorporating hands-on developer training as integral part of your Security Champions program and engaging the entire organization with security-minded best practices, you're offering critical transparency and consistency that's necessary to get everyone on board with security.

Effective Security Champions in your organization will help you:

Educate

They stay up to date with the latest practices through ongoing training with tools like Veracode Security Labs.

Inspire

They raise awareness of security issues within the development team and help inspire the same behavior.

Review

They act as critical reviewers of the team's code, looking for security issues early on to catch them sooner.

Escalate

They act as the point person to elevate an issue for the security team to review, bolstering communication.

Improve

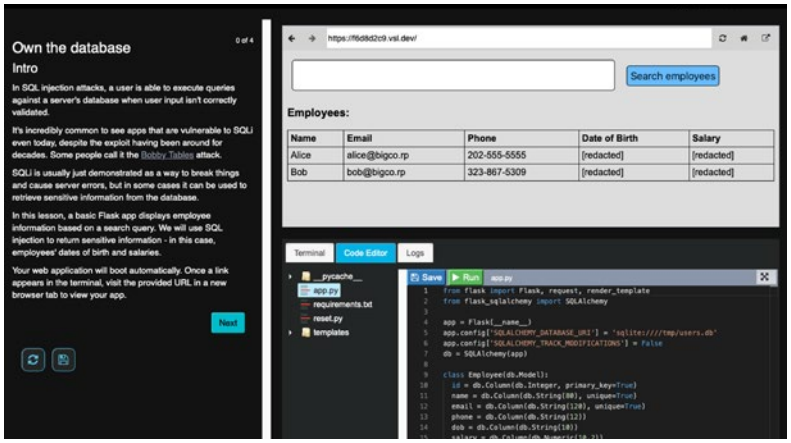
They become a point person to answer team member questions about secure coding best practices.

Share

They connect with other Security Champions throughout the organization to share helpful ideas and tips.

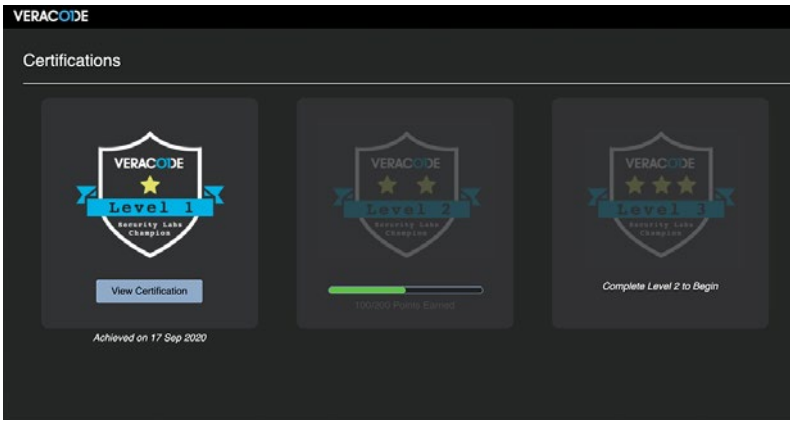
Learn more about setting up a Security Champions program

Getting started with Veracode Security Labs.



Tailored Topic Assignments

You can create a **customized experience** for developers on your team with relevant security topics that are assigned at a per-language, topic, and difficulty level to different groups of users. The course catalog offers broad and deep coverage across critical security topics. Even customize written training itself to your organization's specific needs, such as linking teams back to internal reference documentation.



Leaderboard and Badges

Within the platform, configurable **leaderboards** track user progress by team. Admins can set up timed competitions and challenges to spark competitive spirits. Users can also receive **certification badges** after successfully completing labs, equipped with a unique URL that they can share on LinkedIn or other social channels. Combined, the leaderboard and badges are a great way to showcase skills and encourage security knowledge.

Tracking Progress

It's easy to track progress at the **team** and **individual** level, which you can then use to celebrate success. Data is reported right within the platform, via CSV file export, and it is also available via API requests for teams that have their own internal dashboards.

Putting Veracode Security Labs into practice on day one.

Your organization just signed your team up, now what? Hit the ground running with these three easy (and impactful) uses cases:

Engaging Competitions

Choosing "Competition mode" when you are creating a campaign is a fun way to run timed challenges that gamify the training process and create friendly competition.

Auditing and Compliance Training

Completing labs with OWASP vulnerabilities that are part of your org's auditing process means your team is gaining critical skills to pass compliance requirements.

Spot Training

Using scan results to determine which flaws and coding errors your team sees most often enables you to spot train with precise lab topics to reduce the number of errors made.

Deep dive: reporting

Part of what makes Veracode Security Labs so powerful is the ability to foster real developer learning through competition, campaigns, and interactive labs. That's why the reporting feature is so important. It enables measurement of these critical drivers for developer learning and makes it easier for you to demonstrate how your team members are growing their skills. Reporting in Veracode Security Labs provides visual and downloadable feedback on onboarding, top users, developer self-ratings, time spent on labs, and campaign status so that you can keep a pulse on your team's progress. The feature is automatically enabled for all accounts, and all admin users can see reports across their organization for a level of transparency that's key to successful AppSec.

- Selecting "Allow late access" will allow access to the labs once the competition is complete.
- Selecting "Limit by deadlines" will not allow access to the labs once the competition is complete.
- A separate scoreboard will appear to make the campaign visible to all assigned users.
- All participating users will see the assigned labs highlighted at the top of their homepage.
- A timer will appear for participants, counting to the last assignment end date in the campaign.

Team vs. team competitions

If your organization has a lot of developers or several Security Champions who want to be team captains, consider setting up a friendly team-based competition — this can help foster collaboration within teams and inspire knowledge-sharing.

Competition mode by default is set to compare points across all individuals assigned to roles in the competition (Compete by User). If a competition campaign includes more than one role, then Compete by Role can be selected to create a team vs. team competition. Instead of listing individual users, Compete by Role will show a scoreboard that lists the name of each role and the total points of all labs completed by all users within the role. Let the games begin!

Motivation that sticks (so vulnerable code doesn't).

Hands-on training is critical for muscle memory, especially when you need skills to stick from project to project in software development. Customization features in Veracode Security Labs help you get the right training to the right people at the right levels, which means you can challenge the developers on your team without stretching them beyond their limits so they can work on refining the skillsets they need most on the job.

But this training platform doesn't just position developers for success by teaching them to exploit and patch real applications in contained environments; celebrating achievements and encouraging positive Security Champion behavior helps your whole company stay secure. By gamifying the learning process and applying custom assignments in Veracode Security Labs, you'll help team members level up within your organization while bolstering your business's security defenses too.

Start Trial

[1] ESG Survey Report: Modern Application Development Security
[2] University of Maryland A. James Clark School of Engineering Study: Hackers Attack Every 39 Seconds

VERACODE

Veracode is a leading AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of process automation, integrations, speed, and responsiveness, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities. Learn more at **www.veracode.com**, on the Veracode **blog** and on **Twitter**.