
VERACODE SECURITY LABS
WHITE PAPER

VERACODE

HANDS-ON LABS TO SHIFT SECURITY KNOWLEDGE LEFT WITH VERACODE

YOUR DEVELOPERS ARE ASKED TO KNOW A LOT

When it comes to software, developers are really the only ones in an organization who can fix the vulnerabilities in their code. Yet developers often don't have the training they need to identify or remediate vulnerabilities and to code securely to reduce the number of vulnerabilities found in production. In addition, security teams often don't have the bandwidth or expertise to teach them. The result is an ever-growing mountain of security debt. Efforts to train developers to help solve this problem often fall short because content is too long, the content is irrelevant to an organization's tech stack and/or the approach to learning is unengaging.

HANDS-ON LEARNING WITH MODERN WEB APPLICATIONS

Veracode Security Labs shifts application security knowledge left, training developers to tackle evolving modern by exploiting and patching real code, and applying DevSecOps principles to deliver secure code on time. Through hands-on labs that use modern web apps written in your chosen languages, developers learn the skills and strategies that are directly applicable to your organization's code. Detailed progress reporting, email assignments, and a leaderboard encourage your developers to continuously level up their secure coding skills.

Training at the Speed of DevSecOps

Veracode Security Labs provides the AppSec training developers need, with exercises accessed through a web browserso that in as little as five to 10 minutes, developers can start proving their skills by directly exploiting and patching real code.

Supported languages and frameworks include:

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

Satisfy Compliance Requirements

Many compliance certifications, like SOC2, HITRUST, and PCI, require ongoing security training. Veracode Security Labs helps you satisfy these requirements while providing meaningful education to your development team. You can set required modules and deadlines, track your team's completion, and export progress reports to prove compliance.

Real Web Apps, Not Click-Through Simulations

Alternative “interactive” training solutions typically simulate a web app rather than using real code. The drawback of this approach is that, while passively looking at code snippets, a developer never actually touches the keyboard. No hands-on practice often means that no actual learning has occurred, since developers will simply click through multiple-choice examples until they “pass” a lesson.

Further, there are often many ways to resolve a vulnerability, and in a limited simulation a developer cannot explore these options. This can lead to frustrating situations where developers know a correct fix for a problem, but cannot get credit for their creativity.

Veracode Security Labs uses real, containerized web apps that developers can exploit and fix. This means that developers can fully explore how a given vulnerability affects an application in ways that are relevant to their situations, and creativity can be rewarded as developers gain valuable experience writing secure code in the context of real applications.

Bridge The Gap Between Security And Development

Developers often outnumber security professionals 100 to one – so when developers are empowered to fix flaws and code securely, AppSec becomes more scalable. Veracode Security Labs offers the capability to create customized labs that are relevant to an organization’s tech stack and business objectives.

This document provides detailed descriptions of all the training modules and labs that that are included with Veracode Security Labs, broken out by topic and languages. The labs were designed to teach all experience levels of individuals in your organization about the importance of secure practices during the software development cycle.

OVERVIEW OF LAB TOPICS

Veracode Security Labs provides training for the most relevant application security topics of today. For a more detailed description of our courses, please request a demo for a full experience of all of our lab topics.

VERACODE

OWASP 2017 Top 10 and PCI

- Injection Flaws
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Known Vulnerabilities
- Insufficient Logging and Monitoring
- Insecure Cryptographic Storage
- Insecure Communications
- Improper Error Handling
- Cross-Site Request Forgery (CSRF)
- Other High-Risk Vulnerabilities

Modern Application Weaknesses

- Insecure Direct Object References
- Open Redirects
- HTTPS and Insecure HTTP Traffic
- Secure Services and APIs
- Forced Browsing
- Directory Traversal
- Securing JSON Web Tokens
- Buffer, Heap, and Stack Overflows
- Race Conditions

Data Privacy and GDPR

- Limiting PII Storage
- Informed Consent
- Access and Erasure
- Data Rectification
- Data Portability
- Securing User Data

VERACODE

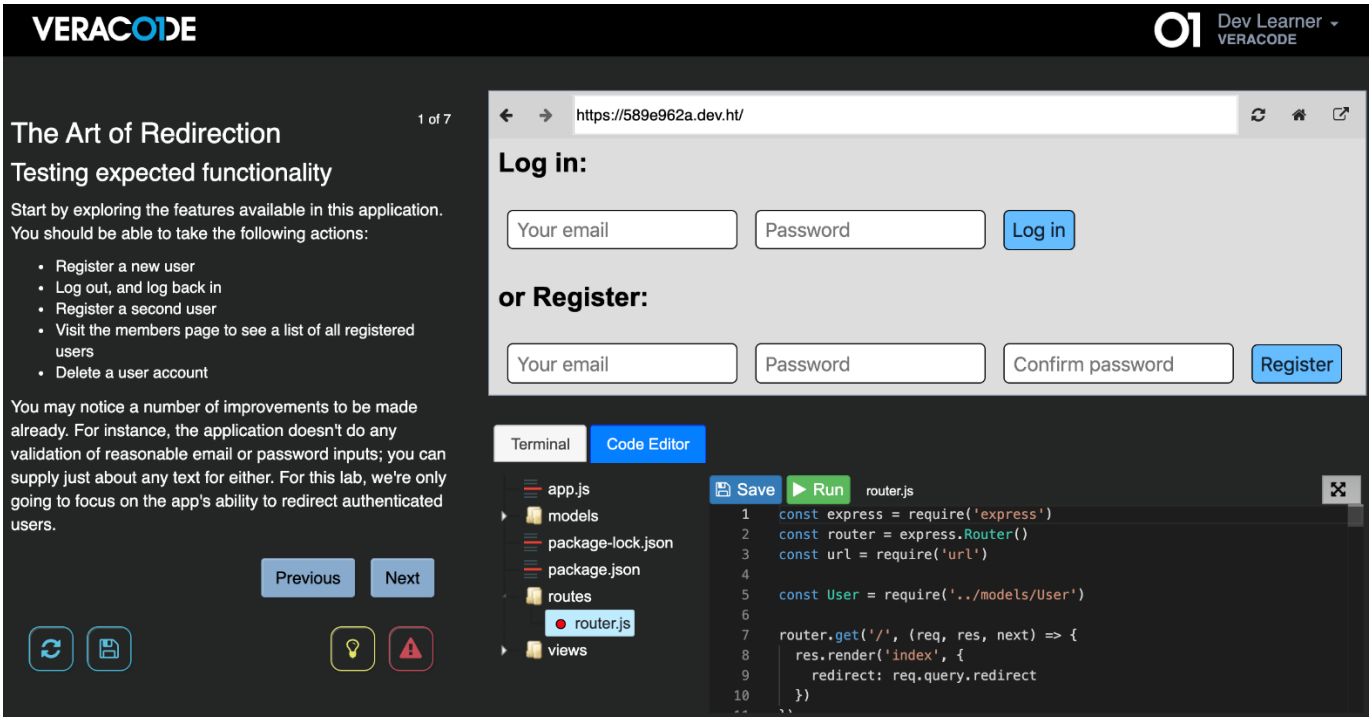
PLATFORM OVERVIEW

Guided Interactive Labs

Developers are automatically provisioned individual, containerized servers and web applications, accessible through their browser. From the lab interface, users can interact with real web apps, exploiting vulnerabilities and patching code by writing their own fixes.

Lessons guide users through each step, automatically checking user progress along the way. Additional practice challenges serve as extra practice to reinforce learned skills.

Users can save their place in each lab to pick up where they left off and access optional hints to guide them as needed.

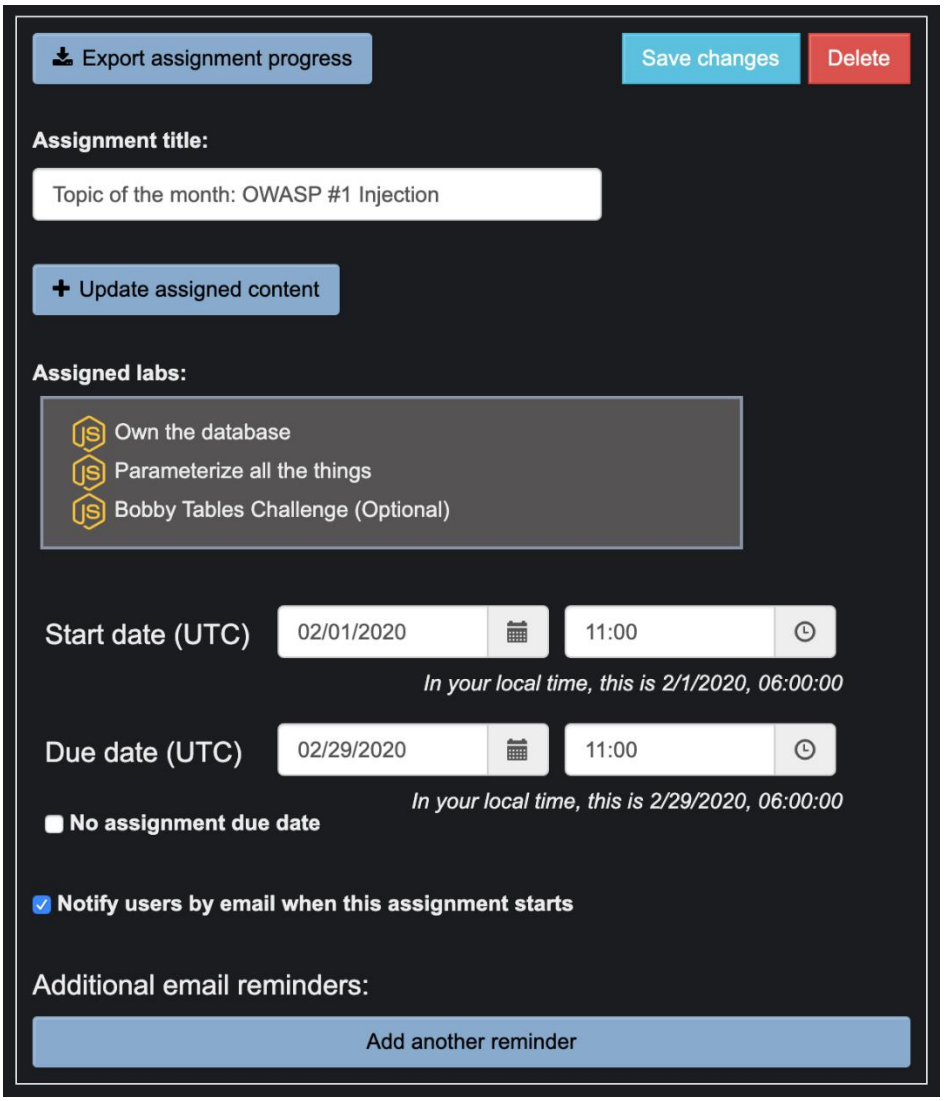


VERACODE

Assignments and Progress Tracking

Admins and managers can assign required labs with due dates, define user roles, and select languages for different sets of developers. Customizable email reminders help keep users on track.

Progress at the team and individual level is reported on within the platform, via CSV file exports, and via API requests for teams with their own internal dashboards.



VERACODE

Customizable Content and Competitions

Relevant training content can be assigned at a per-language and per-topic level to groups of developers. Written training content itself can be customized to your organization's specific approach—for instance, by linking a team back to internal reference documentation related to a particular security topic.

Configurable leaderboards track user progress within teams. Admins can set up timed competitions to host an internal *Capture the Flag* or one-time workshop.