# SecureBuild BLENDED TRAINING

## Go Beyond the Code to Reduce Software Risk
Development teams constantly deal with rapid release cycles, dozens of technologies, and relentless threats – making security feel overwhelming. SecureBuild combines online courses with cloud-based cyber ranges to make security approachable and a natural part of the software development process.

- Conduct early phase security activities.
- Reduce flaws and vulnerabilities.
- Mitigate technology specific threats.
- Build Security Champions.

## Achieve any Role-Based Competency
With novice through elite tiers, courses quickly scale knowledge in logical ways. Cyber ranges provide a high-fidelity environment to apply that knowledge in real-world applications.

When teams understand how code flaws propagate into attack vectors, mindsets change from “Why would anyone do that?” to “That’s a problem I need to prevent!”

## Computer-Based Training
**Focus**  
All SDLC Phases, PCI DSS, OWASP, CWE, CVE.

**Platforms**  
Android, iOS, AWS, Azure, Web, Linux, Embedded, IoT, DB, Blockchain.

**Languages & Frameworks**  
AJAX, Django, React.js, .NET, Powershell, GO, API, Angular, jQuery, Ruby, Perl, Bash, C/C++, C#, Web Services, Swift, Ruby, Python, PHP, Node.js, Java, HTML5, Kotlin, and more.

## Cyber Range
**Environments**  
Web & Mobile applications with focus on code/design level vulnerabilities and OWASP Top Ten.

**Attacks**  
Basic to intermediate XSS, SQL Injection, parameter tampering, business logic, and others.

**Gameplay**  
No tools needed. Learning Labs, hints, and cheat sheets ensure all skill levels can compete.

---

*After the cyber range I started approaching code differently. Now my first thought is, How could I hack this? What if I changed the form input here, would we reject it appropriately?*

Molly Struve, Software Engineer, Dev.To
Building Skills that Stick! 3 Step Approach

Most organizations start with fundamentals courses, followed by hands-on cyber range exercises. Reporting baselines skills and provides targeted training recommendations, which may be taking specialized courses, moving on to an advanced range, or building a new skill.

1. **FUNDAMENTALS (COURSES)**
   - Architects
   - Developers
   - Testers/QA
   - Engineers
   - Managers

Learn the Fundamentals (Courses)
Ensure all roles understand key Application, IT and Data security principles.

2. **HANDS-ON ATTACK (CYBER RANGE)**
   - Ecommerce System
   - Single Page App (SPA)
   - Mobile Application
   - Back-office Software

Learn by Doing (Cyber Range)
Thrust teams into immersive environments with poorly implemented security principles. If they can’t find them, they’re likely making the same mistakes.

3. **OPTIMIZE (COURSES & CYBER RANGE)**
   - Attack & Defend Courses
   - Advanced Cyber Ranges

Optimize
Use performance results and industry baselines to identify next role-and technology-specific training steps.

The Power of Accurate Insight

Having a measurable way to assess skills ensures only necessary training is taken. For example, if a developer can’t conduct a basic SQL Injection attack, they likely need training on:

- How databases get exploited
- How to sanitize input
- How to use stored procedures

Cyber Range Results

Recommended Courses

- Designing Secure Software
- Fundamentals of Database Security
- Creating Secure Code – Java
- Creating Secure Code – Web API
- OWASP: Testing for Security Misconfiguration
- OWASP: Testing for Broken Authentication
- OWASP: Testing for Injection
- OWASP: Mitigating Cross-Site Scripting (XSS)