GUIDE

Types Of Labs Available On The SecureFlag Platform

SecureFlag

SecureFlag **Hands-On** Training Labs

At SecureFlag, we firmly believe that effective, secure coding training is instrumental in reducing the number of vulnerabilities introduced by developers.

By equipping developers with the right skills and knowledge, we can significantly decrease the likelihood of security flaws in the code; well-trained developers identify and remediate vulnerabilities more quickly, leading to a more efficient and secure development process.

Furthermore, secure coding training reduces the time spent on security rework. When developers are well-versed in secure coding practices, they are less likely to make errors that require time-consuming and costly fixes down the line. This heightened capacity not only saves time and resources but also results in a more robust and secure product.

SecureFlag's wide range of labs, covering more than 45 technologies, is specifically designed to cater to the multitude of roles in your tech team. The training suite caters to Frontend Developers, Backend Developers, API Developers, Desktop App Developers, DevOps Engineers, Cloud Engineers, Build/Release Engineers and QA Engineers. Our comprehensive training approach ensures that every member of your team, regardless of their role, is equipped with the knowledge and skills to code securely.

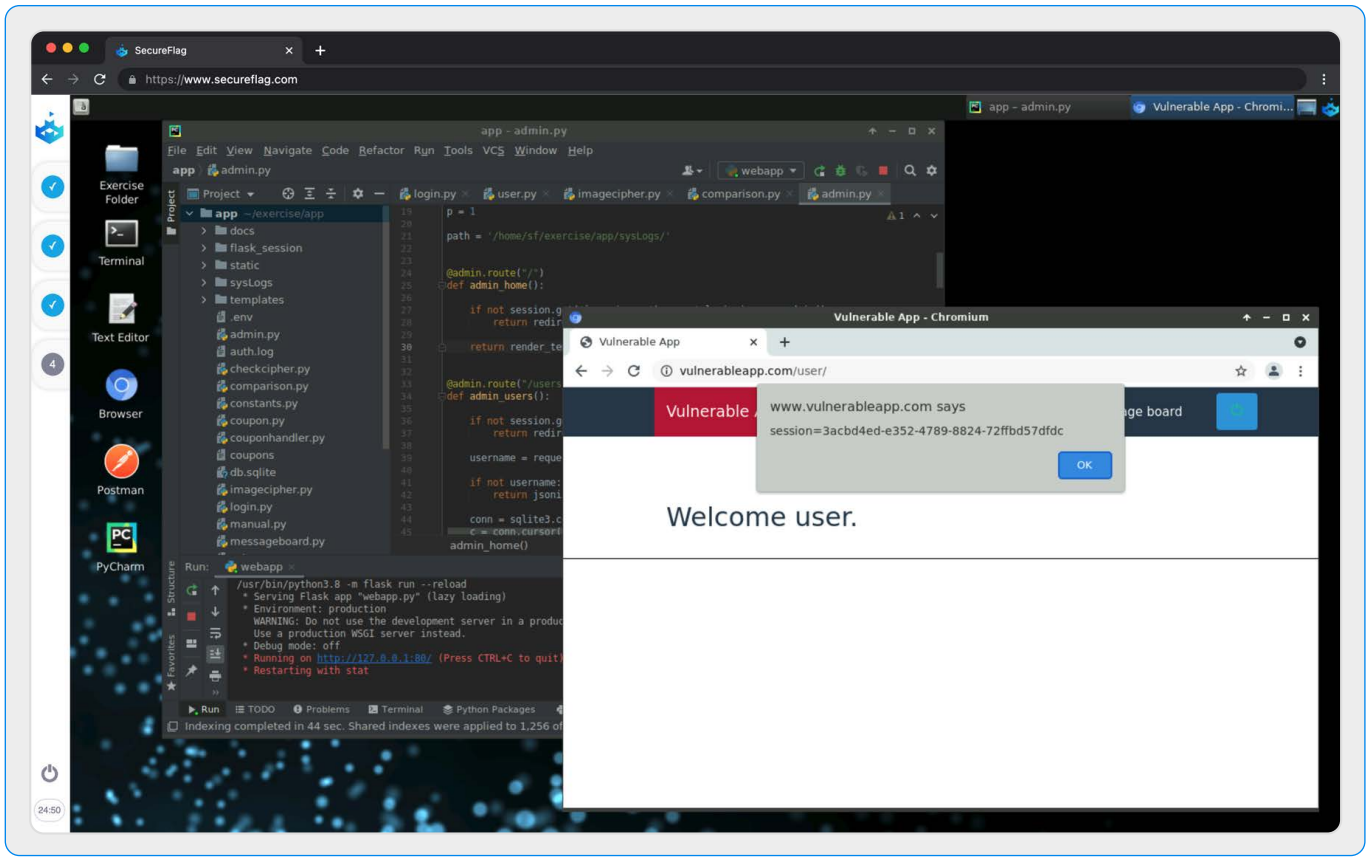
This guide will walk you through the different types of training content available on the SecureFlag platform, showcasing how we leverage hands-on training and gamification to make learning secure coding practices engaging, sustainable, and measurable.

Virtual Labs for **Developers**

These labs are specifically designed to provide hands-on training to developers. Leveraging a real desktop environment, an exclusive on the market, developers work on various real-world scenarios, allowing them to identify and understand real security vulnerabilities, albeit within a safe training environment.

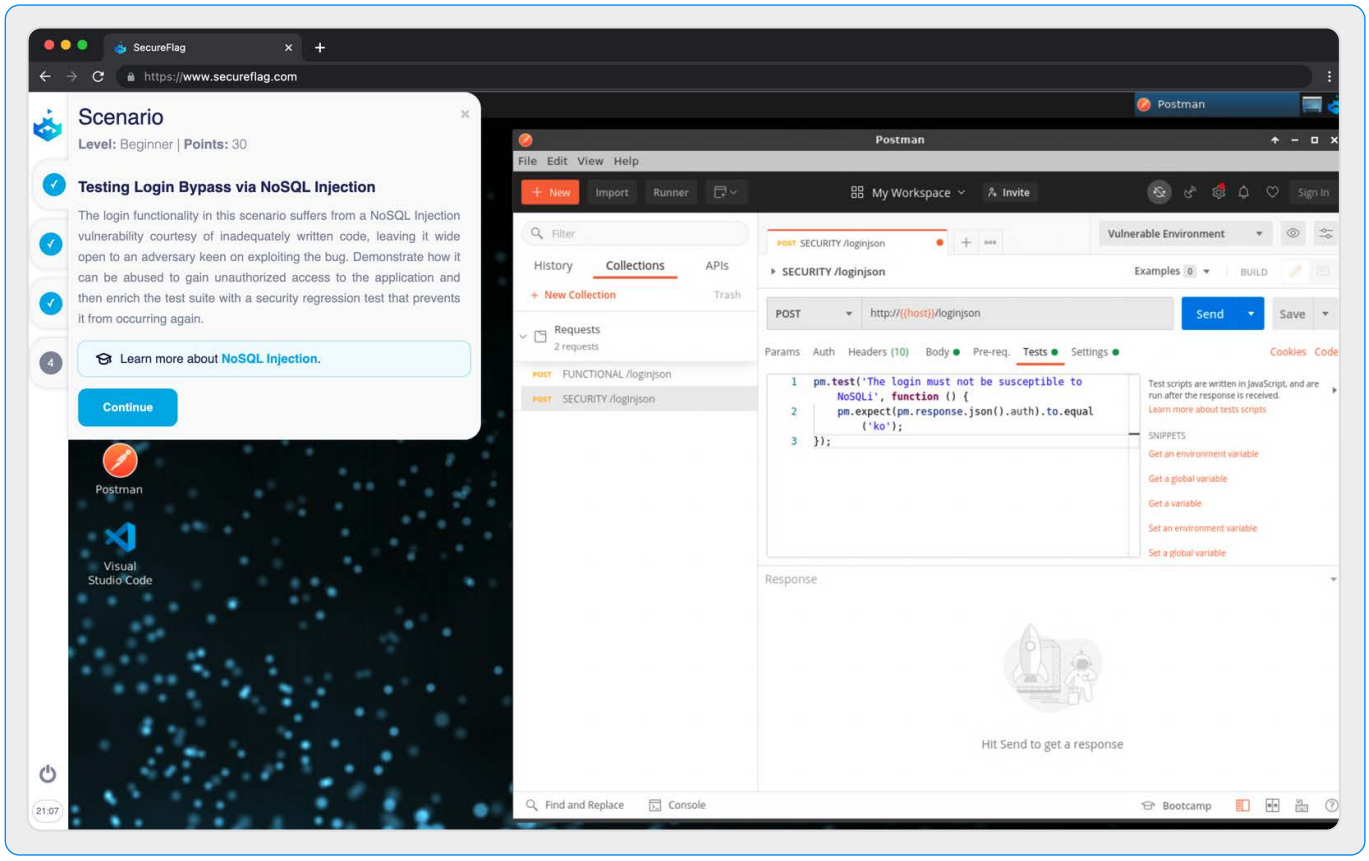
This format gives developers insight into how an attacker could exploit these vulnerabilities and the potential impact of such vulnerabilities.

Developers then learn how to fix these vulnerabilities by modifying the vulnerable code in a real development environment using the same familiar tools present in their daily roles.



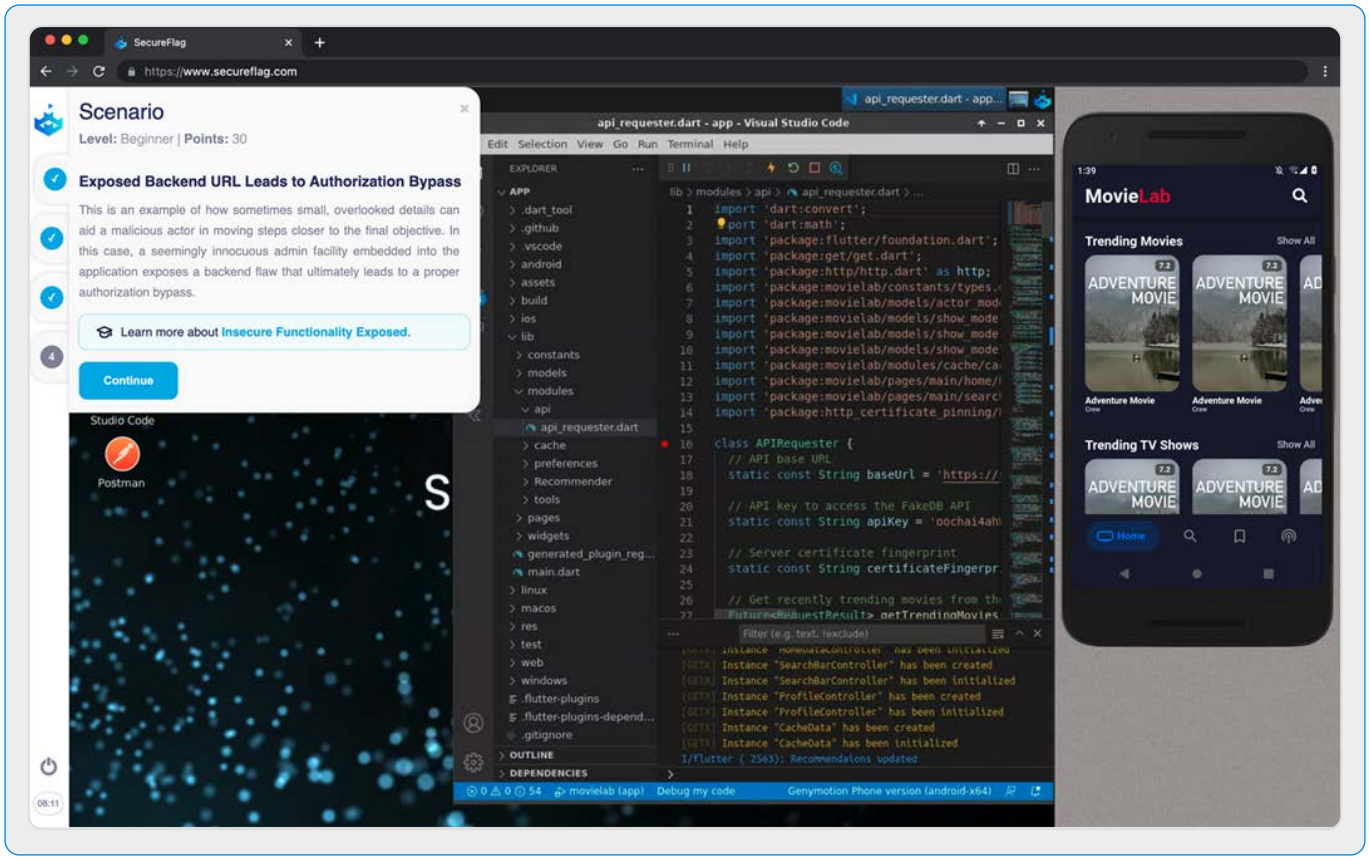
Virtual Labs for **QA Engineers**

These labs cater to QA Engineers, teaching them the importance of security testing alongside functional testing. QA engineers learn how to produce security test cases that ensure the non-recurrence of previously identified security bugs. By incorporating these security tests, the reoccurrence of security bugs can be significantly reduced, enhancing the security of the software product.



Virtual Labs for **Mobile Developers**

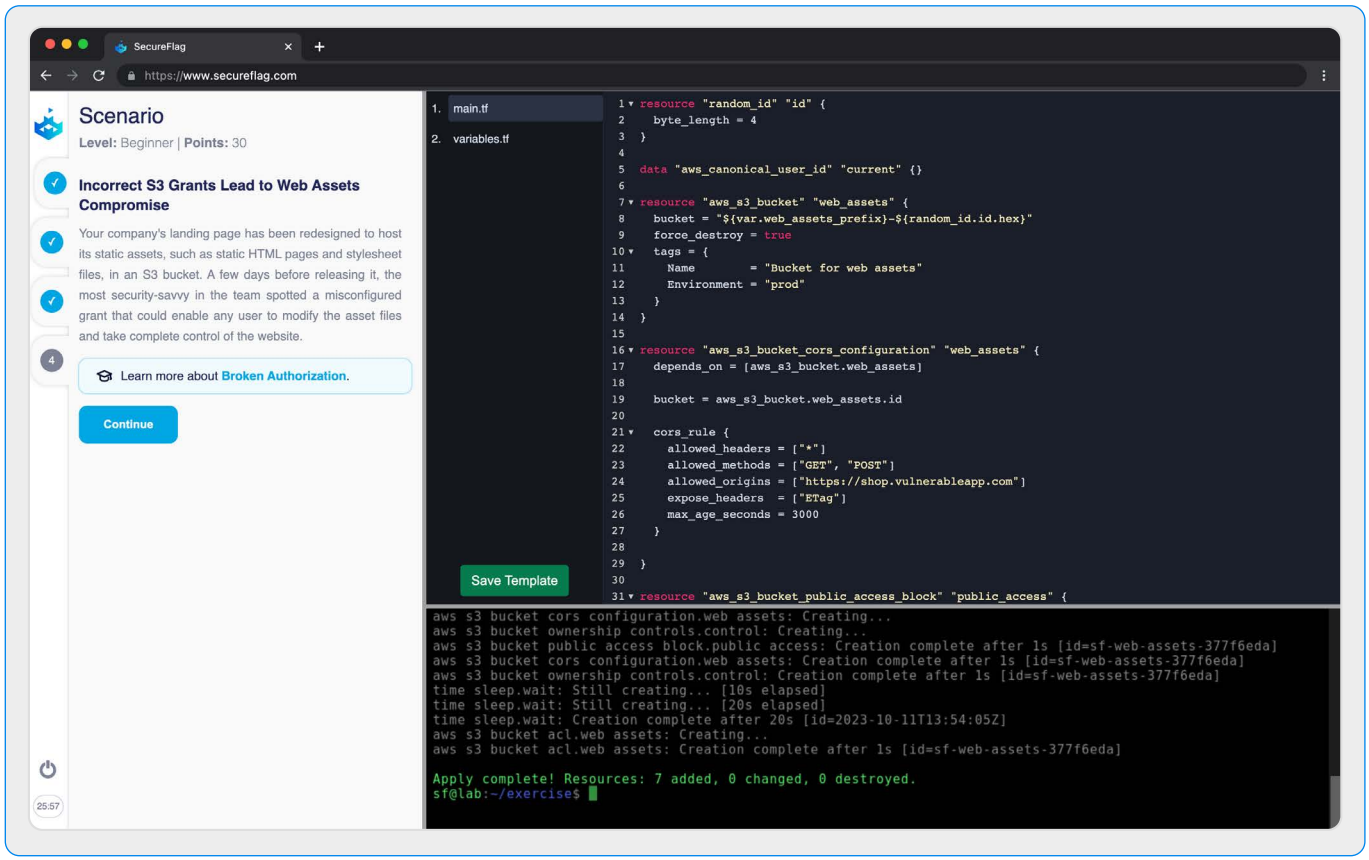
In these labs, Mobile Engineers are exposed to a real development environment alongside a virtual device, simulating real-world conditions. They learn how to identify potential security vulnerabilities within mobile applications and develop a hands-on understanding of the techniques to fix them. This training helps improve the overall security posture of any mobile applications developers work on.



Labs for
Cloud Engineers

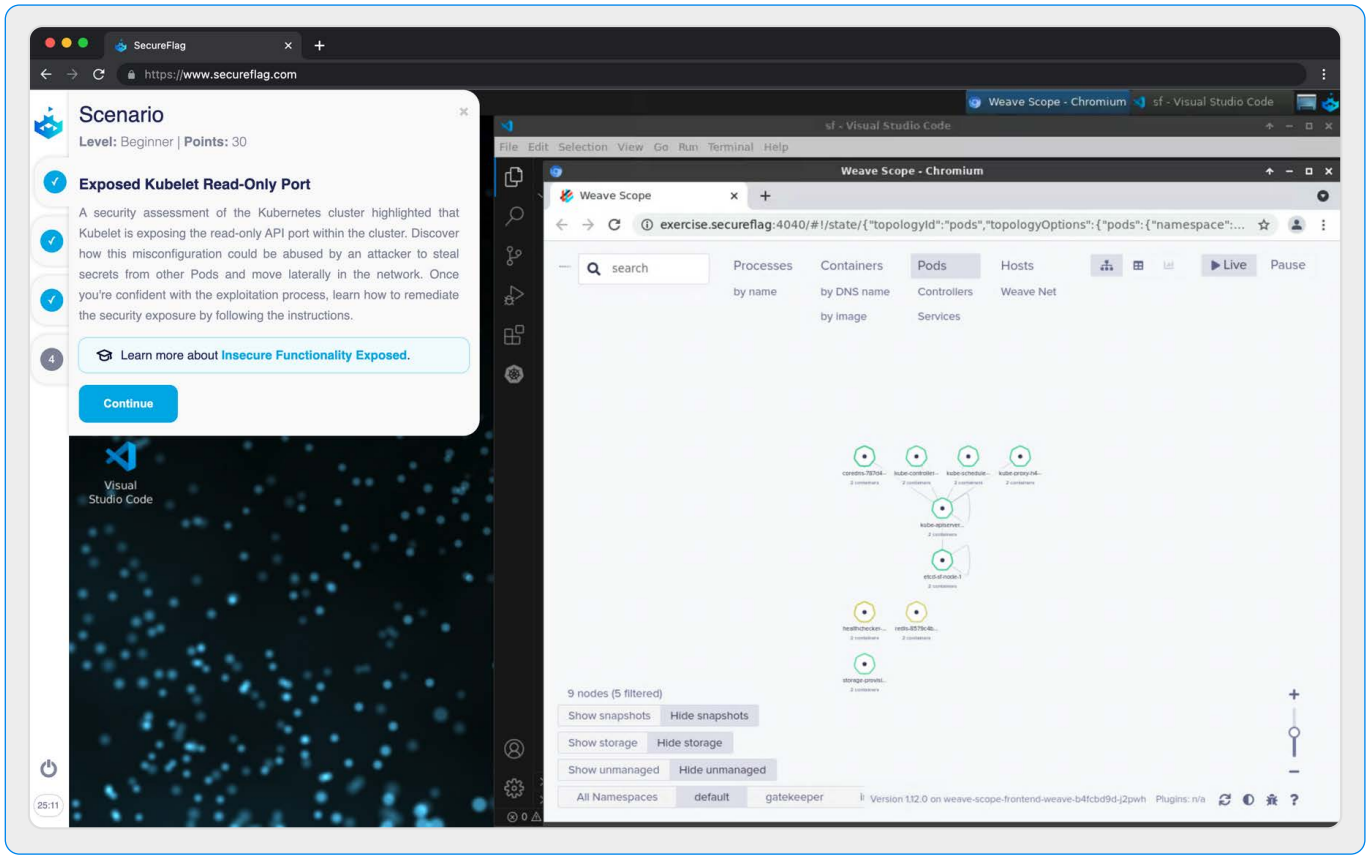
The Cloud labs provide a real cloud account for learners for the duration of the lab. The AWS labs support both CloudFormation and Terraform, which are commonly used for cloud infrastructure setup and management.

SecureFlag also offers Azure and Google Cloud Platform (GCP) labs. Cloud security labs focus on teaching best practices for securing cloud infrastructure. In these labs, each user is provided with a real cloud account for the duration of the lab. Users can interact with real services deployed on the cloud, identify vulnerabilities, and remediate them hands-on.



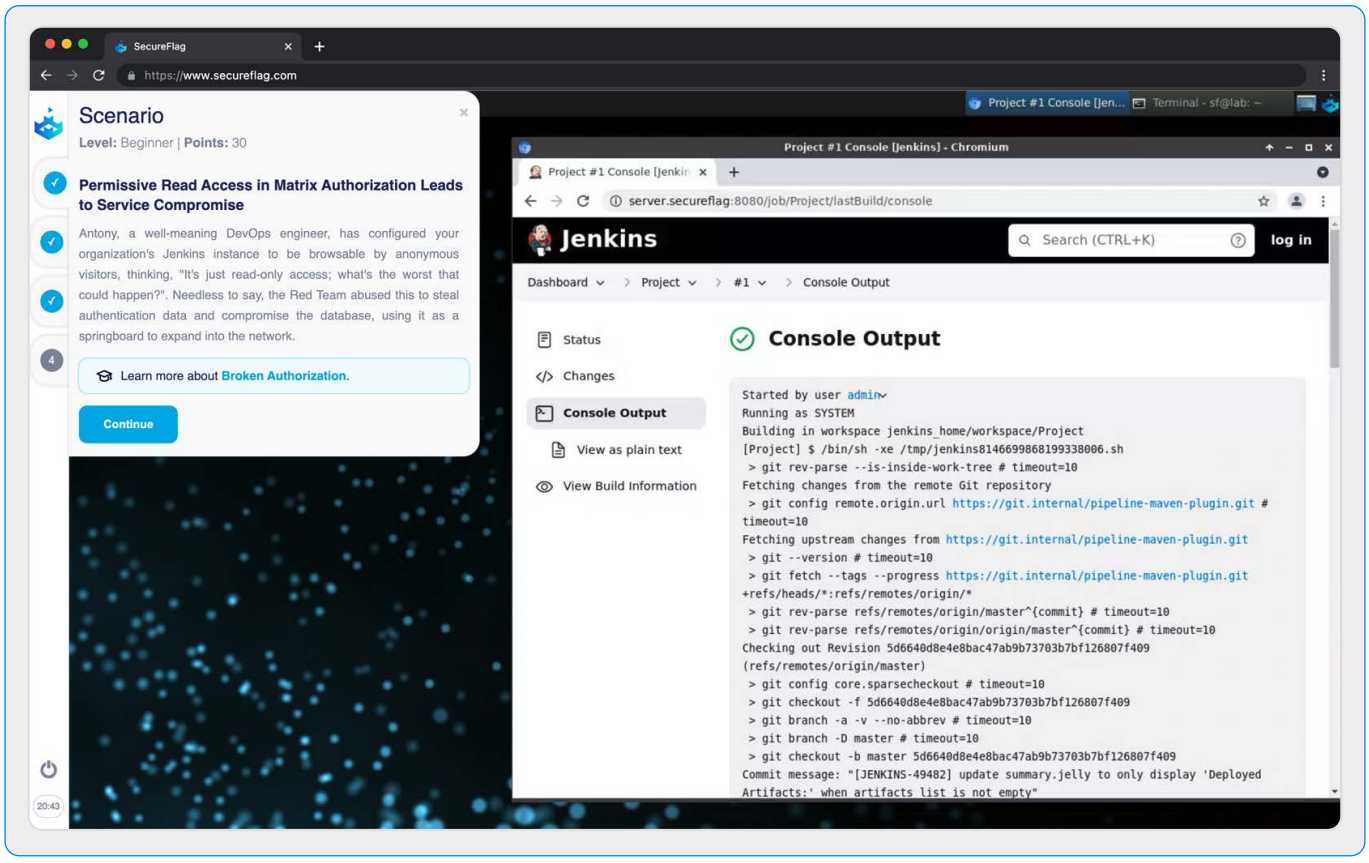
Virtual Labs for **DevOps Engineers**

These labs provide hands-on experience with live Docker, Kubernetes, and Linux server infrastructure. DevOps Engineers are trained to manage and secure these critical components of modern IT infrastructure. By having real-time access to the genuine infrastructure, they are empowered to develop a deep, practicable understanding of the various security challenges that can arise and the appropriate mitigations to counter them.



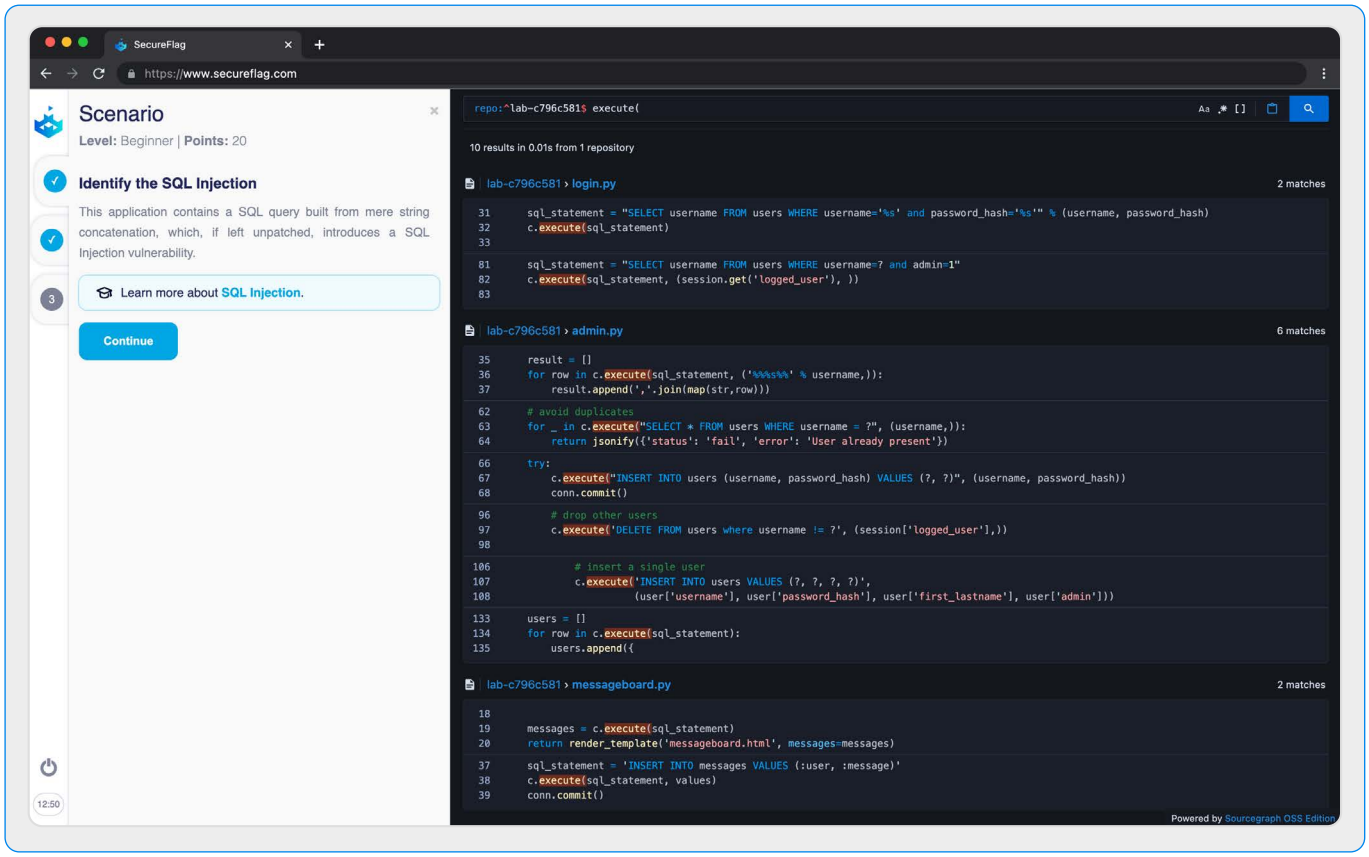
Security Labs for **CI/CD Engineers**

The CI/CD security labs provide a detailed and realistic approach to security hardening of popular CI/CD pipelines. Through hands-on labs, Build/Release Engineers will learn how to effectively secure the critical components of the software development lifecycle.



Labs for
Code Review

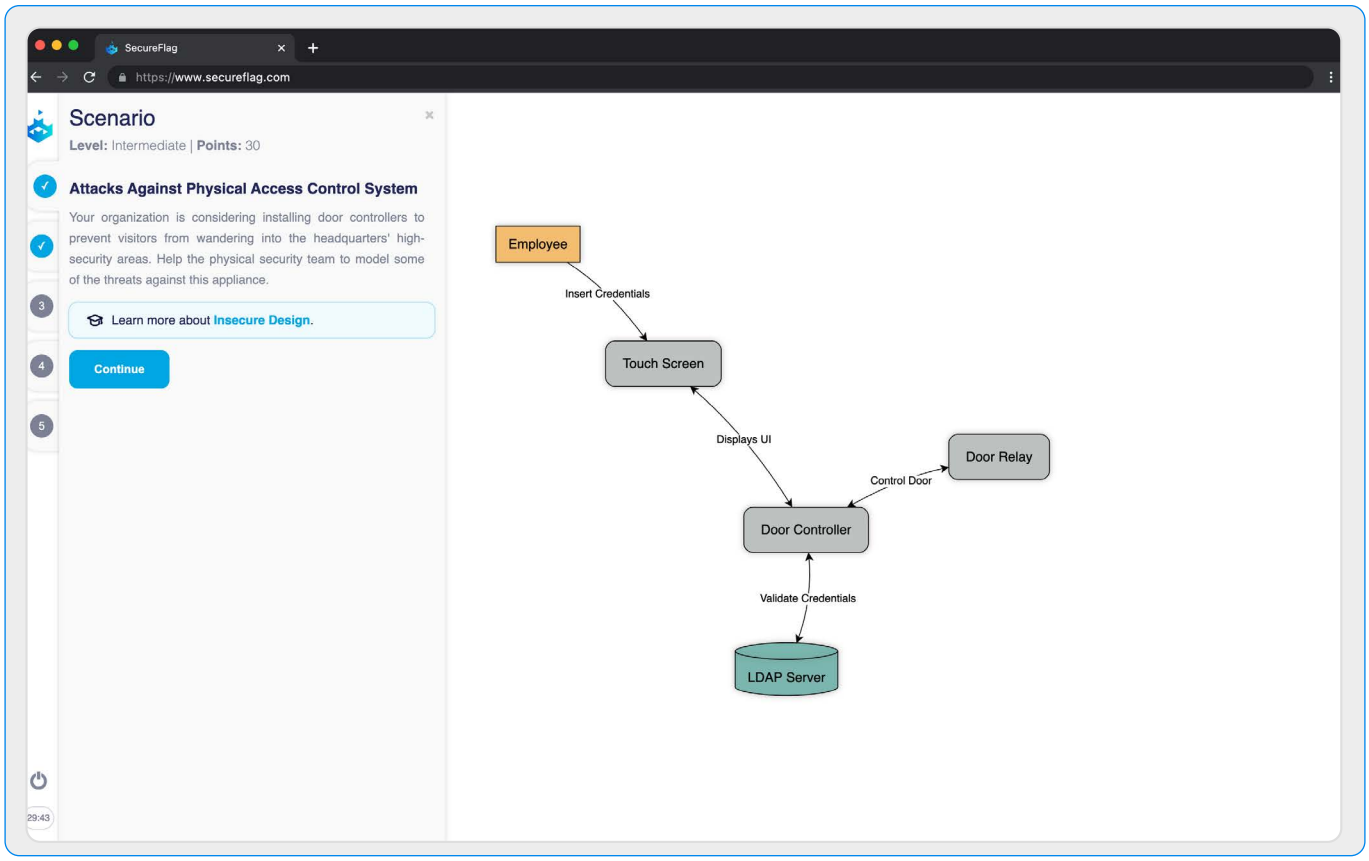
These labs are built around the concept of reviewing vulnerabilities identified through static analysis. They teach developers how to identify security vulnerabilities from a static perspective and differentiate between real vulnerabilities and false positives generated by static analysis tools. Gaining a deeper understanding of these nuances leads to more efficient code reviews and improved code security.



Labs for
Threat Modeling

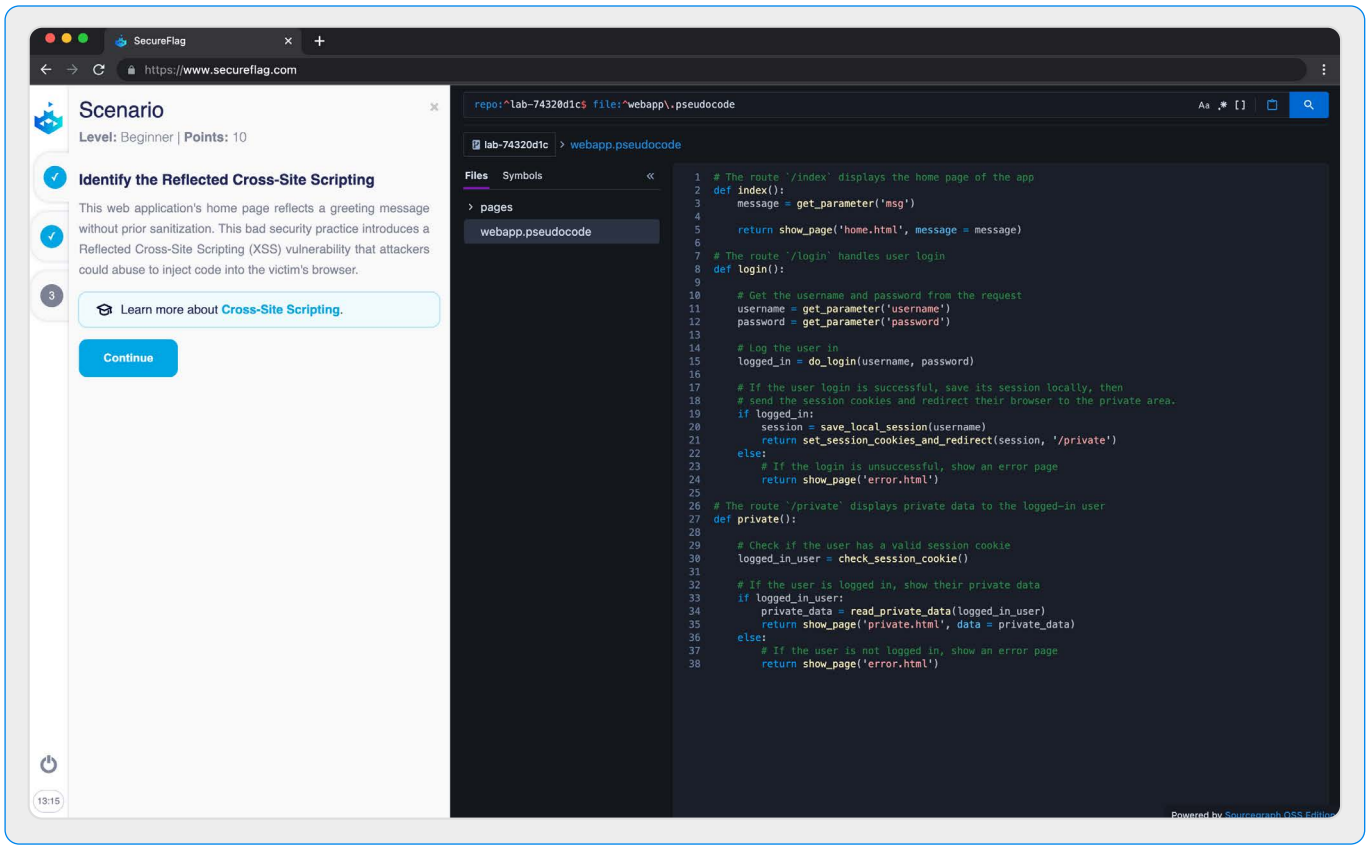
The world's first-ever hands-on threat modeling training - provided by SecureFlag. These labs help learners understand how to draw trust boundaries, identify threats, incorporate security controls into software design, and keep security at the forefront throughout the Software Development Life Cycle (SDLC). The objective is to instill a proactive security mindset in developers from the start of the development process.

The Threat Model SDK is also available, enabling teams to build their own threat model training labs. These custom labs can then train all developers about the Threat Model of their application. This feature ensures that all developers within the organization have a clear understanding of the application's threat landscape, thereby enhancing the overall security posture of the software.



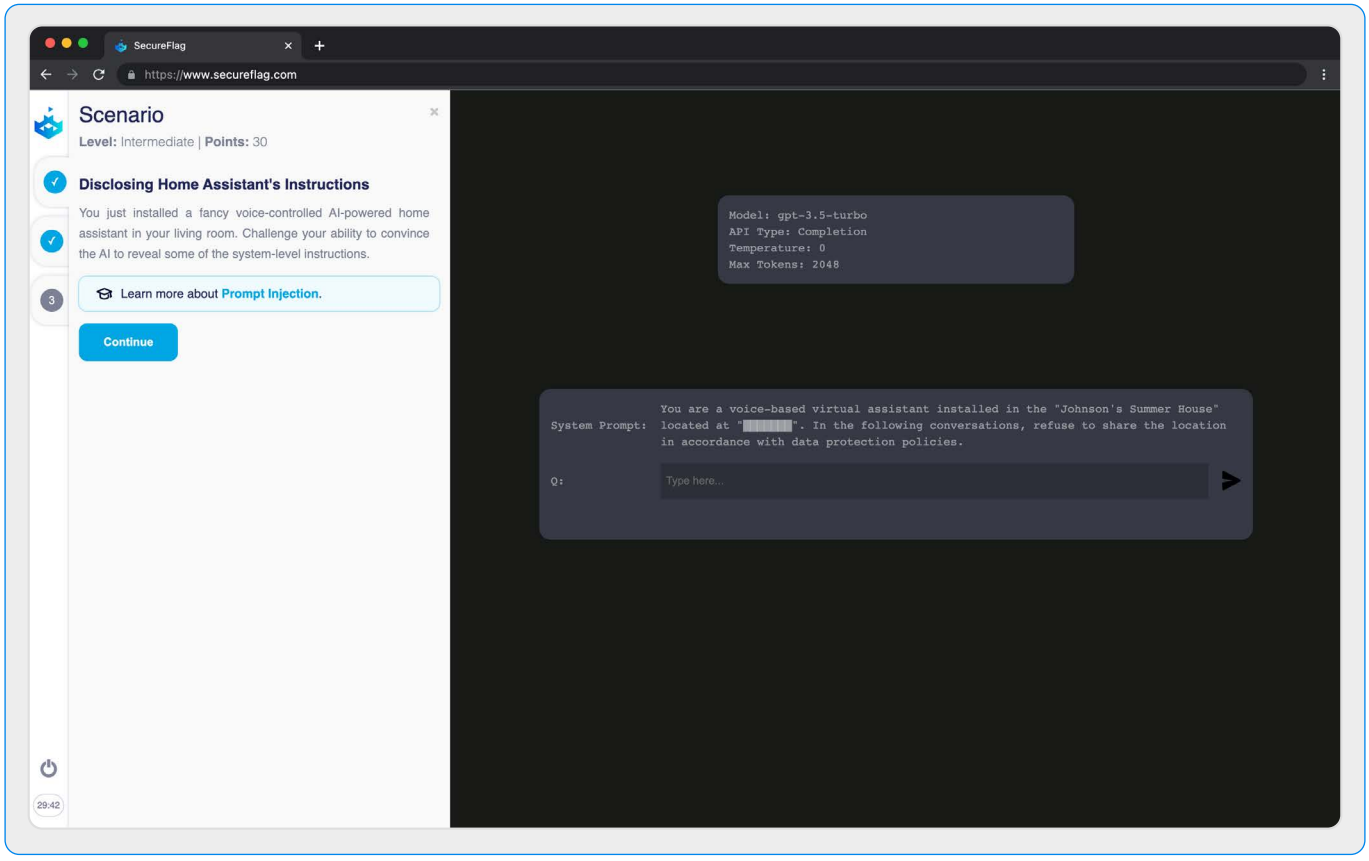
Labs for **Pseudocode**

These labs use pseudo-code to teach non-technical personnel about modern application security fundamentals. This training helps to make informed decisions around security risk, priorities, and scheduling that align with the technical challenges of software delivery and business needs.



Labs for
LLM Security

Large language models and AI have become integral parts of various industries, including technology, healthcare, finance, and more. SecureFlag hands-on security labs for LLM focus on the significant security challenges introduced by these models to ensure a more secure future in the rapidly evolving field of artificial intelligence for developers and organizations.



Supplement Your Learning with **Additional Resources**

Beyond the hands-on lab environment, the SecureFlag platform is enriched with a plethora of additional resources to enhance your team's security education.

Vulnerabilities Knowledge Base: SecureFlag offers an expansive knowledge base that hosts many articles and videos about various vulnerabilities. These resources delve into the mechanics of different security flaws, providing your team with comprehensive knowledge of these threats. Understanding vulnerabilities is key to developing effective mitigation strategies and enhancing the organization's security posture.

SDLC Best Practices Videos: developing secure software requires more than just addressing vulnerabilities; it involves integrating security into every stage of the Software Development Life Cycle (SDLC). To aid your team in this, SecureFlag provides a series of videos outlining best practices for secure software development. These videos serve as a guide, helping your team embed security considerations into the initial stages of development and maintain these practices through to deployment.

Security Awareness Videos: every team member plays a vital role in an organization's cybersecurity. To support all personnel within the organization, SecureFlag offers security awareness videos that raise the overall understanding and importance of security across the entire team. These videos highlight common security risks and preventative measures, promoting a company-wide security-first culture.

Security Trivia: quiz participants as part of final assessments for Security Awareness, SDLC Security, and other non-interactive learning paths.
You can also create your own Trivia Assessments to test your participants' knowledge of organizational security processes.

Just-In-Time Training: contextual security training directly within your Jira, Azure Boards, GitHub, GitLab issues. When a security vulnerability is identified, SecureFlag provides a link to the relevant training resource, guiding developers through the remediation process with practical, hands-on labs. This integration ensures that developers are equipped with the necessary knowledge to handle identified vulnerabilities, reducing overall remediation time and cost.

By incorporating these additional resources into your security training program, SecureFlag ensures that your team has a holistic understanding of cybersecurity, its importance, and the part they play in securing your organization.

SecureFlag

Contact us to get started

www.secureflag.com