



GUIDE

Quickstart to Secure Coding Training

In this eBook, we guide you through the steps required to ensure a smooth rollout of your organization's secure coding training program using the SecureFlag platform. Along the way, we will help you clarify your goals, define your strategy, identify the necessary actions, and set key criteria and metrics, all of which will set you up for long-term success.

Step 1: Define Program Objectives

One of the key objectives of your organization's Secure Coding training program should be to strengthen your developers' defensive programming skills, taking into account their current capacities, knowledge, or speciality. A solid secure coding training program enables organizations to:

- **Reduce issues and the time to fix them**
- **Identify and empower Security Champions.**
- **Achieve Compliance..**

A developer's security maturity level can be tracked by multiple properties, including:

- **Competency score**
- **Certifications/Badges**
- **Training time**
- **Number of labs completed**
- **Points earned**

Here's how maturity levels are defined in the SecureFlag program:



Novice

Where every developer starts their skill-building journey.



Security Squire

Able to identify and fix all OWASP Top issues.



Expert Defender

Able to identify and fix complex security issues. Candidates at this level or above should be considered Security Champions.



Cyber Commander

Able to identify and fix security issues beyond the OWASP Top 10. They also mentor others at lower levels to improve security awareness and promote interest in learning across the organization.

Quickstart Guide to Secure Coding Training

The SecureFlag platform has been designed for you to structure a customizable learning journey that continuously engages and rewards your developers, empowering them to complete a variety of achievements along the way.

These include:

- **Badges:** maps to the participant's maturity level
- **Trophies:** awarded for completing Labs without using hints
- **Tournament Placements:** awarded for completing a Tournament
- **Certifications:** awarded for completing a Learning Path. Each certification must be renewed every year by taking refresher exercises

You can combine these elements to create your own certification program. Consider adding elements like "mentoring" (e.g., X hours of mentoring provided) as part of the certification journey from one level to the next. Not all your developers need to achieve the highest level of certification. Give them the option to choose how and when to build their skills; those at higher levels could be good candidates for your Security Champions program.

For example, your certification levels might look something like this:

	Novice	Security Squire	Expert Defender	Cyber Comander
Hours Spent on Training	<6 hrs	6-20 hrs	21-40 hrs	40+ hrs
Number of Labs Completed	<15	16+	35+	55+
Points Earned	500+	750+	1800+	2800+
Competency Score	55%	>60%	>65%	>75%
Badges (Certifications, Trophies, Tournament Placements)		1 Trophy 1 Certification	3+ Trophies 2+ Certifications 1 Tournaments	5+ Trophies 3+ Certifications 2+Tournaments

Based on your specific objectives, your Customer Success Manager (CSM) will help you create a Training Plan for your organization and support you in achieving set objectives.

Quickstart Guide to Secure Coding Training

Step 2: Setup Single Sign-On

Ask your Customer Success Manager (CSM) to set up Single Sign-On (SSO) for your organization before diving into the training program. SecureFlag supports any SSO solution based on SAML 2.0 or OAuth 2.0 protocols and has native integrations with many IAM providers. User provisioning can be fully automated through the SCIM 2.0 protocol.

Step 3: Onboard Users

After setting up Single Sign-On (SSO) and sending your communications for the launch of the program, ask your CSM to onboard your users via one of the following options:

- **Use SCIM or SecureFlag APIs (automated user onboarding):**

Automate provisioning of Users/Teams using the SCIM 2.0 protocol

- **Create and import users in bulk (we onboard your users):**

You provide us with a spreadsheet, and we will create the Users in bulk

- **Send an invitation code (users onboard themselves):**

Users self-signup through an invitation link

- **Create Users from the Management Interface (you onboard your users):**

You can add new Users from the Management Interface

Step 4: Kick-Off the Program

Now that you have set up the system and added users to it, you are ready to launch your secure coding training program! Importantly, a good program is a fun program! Rally the troops, synchronize with Executive Sponsors and Team Managers to light the coding candles.

Quickstart Guide to Secure Coding Training

To generate enthusiasm, we've thrown together some ideas that may help you:

- Invite **executive leadership** to convey the importance of the training program
- For a few weeks prior to kick-off day, **generate hype** and build excitement by sending out newsletters, posting notices, hanging banners, etc.
- Identify a theme for the event and make it part of the program "brand", with unique colors, icons, logos, stickers, etc. To **promote the event** quickly and simply, use the posters, email and social templates available as part of the Communication Pack
- Invest in branded merchandise and rewards and make sure people know about what's up for grabs (or ask your Customer Success Manager for **SecureFlag swag**)

Team Managers should talk about the new program at team meetings and encourage developers to ask questions. This will heighten the sense of enthusiasm and get the developer buy-in you need to make the training program a success.

Step 5: Assign Training Activities

SecureFlag groups Labs and other learning resources into a sequence of logically linked secure coding journeys called **Learning Paths**. A Learning Path allows a learner to become an expert in a topic in small and easy-to-manage steps.

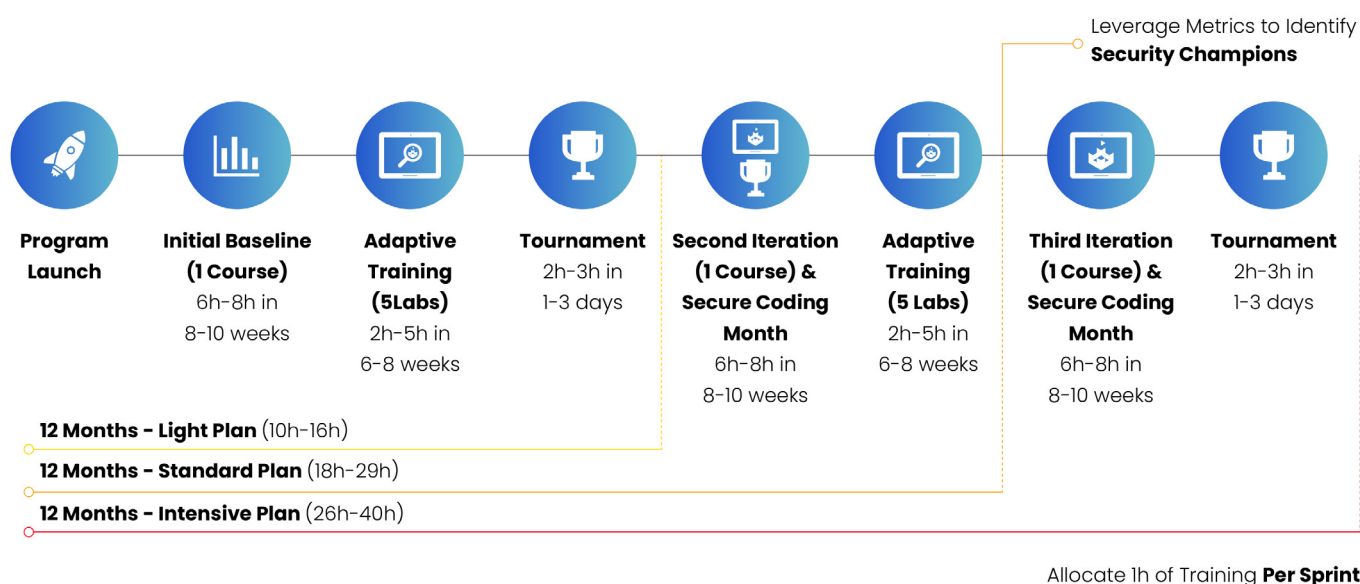
Each Learning Path includes labs, videos and knowledge-base articles. These elements work together and guide developers towards increasing their secure coding competency in a specific area. When a developer completes a SecureFlag Learning Path, they receive a certificate.

Certificates have an expiration date, but they can be renewed by taking some **refresher exercises** during the year. By doing this, developers can keep their learning up-to-date and continuously add to their skillset in that area. Work with your Customer Success Manager to identify topics and personas, and then assign Labs/Learning Paths to the entire Organization, a Team, or Individual users.

We recommend building a **Training Plan** with one or more Training Iterations in order to plan and **automatically assign** activities to participants **throughout** the year.

Quickstart Guide to Secure Coding Training

Work with your Customer Success Manager to create a tailored Plan based on the training program's objectives.



A common pattern that our clients frequently adopt is to assign an OWASP Top 10 Learning Path to all participants (for their specific technology speciality) and use the results as the initial baseline to identify the competency level in the organization across the main classes of security vulnerabilities.

After the initial baseline is completed, we can continue with an Adaptive Training strategy and assign participants topics based on the areas in which they scored the worst. This allows to bring everyone to the same level of competency in a shorter time.

You can also use data from vulnerability management processes to identify patterns of issues to focus on during training.

In SecureFlag, on top of our vast catalog, you can also create custom Learning Paths to address specific concerns identified.

Quickstart Guide to Secure Coding Training

Step 6: Measure Program Effectiveness

As you focus on continuous learning and development to promote a positive security culture in your organization, make sure you refer to the metrics provided by the platform to measure the effectiveness and ROI of your secure coding training program.

You can gauge the security maturity of your program based on key success metrics like:

- **Program adoption** (number of developers/teams trained).
- **Competency scores** (developers' ability to identify and fix security vulnerabilities)
- Reduction in the **number of new security vulnerabilities introduced** in development
- **Reduction in the time taken to fix security vulnerabilities**
- Reduction in the **number of security retests** to consider a security defect as fixed



Number of security tickets

Identified for teams participating in the secure coding program.



Rework due to security tickets

Based on time allocated in sprints for teams participating in the program.



Time to fix security tickets

For teams participating in the secure coding program.

Quickstart Guide to Secure Coding Training

Keep Engagement High **Through Tournaments**

Regular tournaments are a great way to promote a stronger security mindset without making the process feel burdensome to developers. Discuss with your Customer Success Manager how many events you want to run during the year. Make it a themed event using our ready-made promotional material, and display prizes so participants can see tangible proof of what they stand to win if they do well. Use multiple channels to promote it, including email, posters, instant messaging, company Intranet, etc.

After the tournament, hand out prizes: we can provide you with Digital Gift Cards that can be redeemed for thousands of popular brands, products, and experiences. Motivating executive and leadership stakeholders to message their congratulations to the winners also goes a long way to reinforcing the importance of building a healthy security culture.

Finally, send out a short survey to give developers a voice in helping to improve future tournaments.

Next **Steps**

Ask your Customer Success Manager or Account Manager for our complete Guide for Program Managers which includes many additional details on how to run a secure coding training program using SecureFlag.



Contact us to get started

www.secureflag.com