TRAINING MODULES

WE HACK PURPLE

TRAINING@WEHACKPURPLE.COM

TANYA JANCA

AppSec, Securing Coding, DevSecOps, and Azure Security Training

Tanya Janca, also known as SheHacksPurple, is the best-selling author of 'Alice and Bob Learn Application Security'. She is also the founder of We Hack Purple, an online learning academy, community and podcast that revolves around teaching everyone to create secure software. Tanya has been coding and working in IT for over twenty years, won countless awards, and has been everywhere from startups to public service to tech giants (Microsoft, Adobe, & Nokia). She has worn many hats; startup founder, pentester, CISO, AppSec Engineer, and software developer. She is an award-winning public speaker, active blogger & streamer and has delivered hundreds of talks and trainings on 6 continents. She values diversity, inclusion and kindness, which shines through in her countless initiatives.

Application Security Foundations program – 2 days for the complete program
Secure Coding program
DevSecOps with GitHub Actions program
Azure Security program

"The engaging presentation skills of Tanya as instructor keep it fun, light, and almost conversational. The exercises compel you to think aspects of appsec which one might have not thought of. Case studies really help strengthen understanding and open the doors of perception to new possibilities"

- Ronald

"We decided to work with Tanya to jumpstart our AppSec program; we are happy we did. Tanya took our development and security leadership team through her two-day foundations workshop, and we left feeling empowered to begin our journey. Tanya is an engaging presenter and thoughtful sounding board, and her expertise in this field shines through. We look forward to continuing to work with her."

- Gerrit

"Tanya is both extremely knowledgeable, and a fantastic teacher of the knowledge. This course both brought excitement, and guided my curiosity into safe learning and cultivated even more curiosity. It was all things engaging, fun, helpful, and a healthy balance of convergent and divergent learning. Just fantastic! Loved every moment of it. I should also add, that I will be revisiting the contents of this course, to stay sharp and to continue improving (there's just so much to keep coming back to)."

- Kellen

ABOUT OUR TRAINING MODULES

The following live training modules can be selected for training during live remote sessions with We Hack Purple. Each session has an approximate amount of time it will take, we are unable to deliver them in less time. Choose as many as you wish to add up to the amount of time for your desired session.

APPLICATION SECURITY FOUNDATIONS

2 DAYS TO COMPLETE FULL PROGRAM

WRITTEN EXERCISES AND DISCUSSION

NO HANDS-ON-KEYBOARD EXERCISES

Lectures on types of AppSec activity: • Includes one written exercise	2 hr
Lectures on creating an application security program: • Includes one written exercise and discussion	1 hr
Lectures on all types of AppSec tools: • Includes one written exercise	1.5 hr
Lectures on scaling your team, developer advocacy, and developer education: • Includes 3 written exercises and discussion.	2.5 hr
Lectures on gathering metrics and improve: • Includes written exercises and cases studies	2 hr
Securing modern technologies (best practices) and advanced application security activities: • Includes written exercises	2 hr
Incident Response: • Includes case study, templates and assignment	1.5 hr
Policies, standards and guidelines: • Includes 2 assignments, several PDFs of templates	1.5 hr

- We Hack -
PURPLE

SECURE CODING

6.5 HOURS TO COMPLETE FULL PROGRAM

WRITTEN EXERCISES AND DISCUSSION

LONGER SESSIONS INCLUDE BREAKS

Your security policies and secure system development life cycle: — 1 hr

- content to be discussed in advance with client

The 17 secure coding commandments: — 3 hr

How to make code safe enough to put on the internet

- Includes code review exercises and breaks

PCI Compliance for devs — 1 hr

Only what they need to know, and how to ensure they are compliant

---

The OWASP Top Ten and other well-known web app pitfalls, as well as how to avoid them — 1.5 hr

---

Secure Design Concepts — 1hr

Covers 8 secure design concepts - Assume Breach, Zero Trust, Defense in Depth, Least Privilege, Supply Chain Security, Security by Obscurity, Attack Surface Reduction, and Usable Security

---

Incident Response — 30-60 min, End of day

What we need Devs to know during and incident. Covers the concept of 'need to know' and Developer / IR Team communications

- Includes story telling of past incidents that stress the importance of several of the previous lessons delivered in the training, such as having an application inventory and SBOM, input validation, parameterized queries, etc.

- We Hack - PURPLE

DEVSECOPS WITH GITHUB ACTIONS

ADDITIONAL TOOLS CAN BE ADDED TO THIS PROGRAM WITH ADVANCE NOTICE, ASSUMING:
1) THE DEVELOPMENT TIME IS COVERED AT $1000 PER TOOL
2) A GITHUB ACTION IS PROVIDED BY THE TOOL VENDOR AND
3) A LICENSE IS PROVIDED TO THE TRAINING IN ADVANCE.

Lecture: What is CI/CD? What is DevOps? What is DevSecOps? DevSecOps tool options. Why GitHub Actions. Advantages.	30 min
Azure setup, adding to pipeline and publish (optional)	1 hr
GitHub actions setup, forking a report, secret manager, and running a pipeline (not optional)	1 hr
Adding any of the following tools to your pipeline and running, 30-45 minutes each: a. Snyk b. Dependency check c. Dependency graph and Dependabot d. TruffleHog (secret scanning) e. OWASP Zap (headless mode) f. NeuraLegion NexDAST	30-45 min each
Any of the Azure security items from the Azure course can easily be added here.	TBD

- We Hack -
PURPLE

AZURE SECURITY

OTHER AZURE FEATURES CAN BE ADDED TO THIS TRAINING ASSUMING:
1) THE LICENSING FEE IS CARRIED BY THE CLIENT AND
2) THE TRAINER IS GIVEN TIME TO PRODUCE THE CONTENT.
$500 PER NEW SECURITY TOOL THAT IS PART OF AZURE

Discussion and lecture while training templates load into Azure/training setup (mandatory): • What is cloud native? How is cloud native security different?	1 hr
How to load ARM templates into Azure (mandatory).	15 min
Forcing HTPS.	15 min
Enabling Azure Defender.	15 min
Reviewing and remediating Azure Security Center Recommendations.	1 hr min
Implementing automated policy.	1 hr
Implementing Just in Time Access Control (JIT).	30 min
Implementing File Integrity Monitoring.	30 min
Implementing Application Adaptive Controls.	30 min
Implementing Threat protection and reviewing results.	30 min
Implementing DOS protection.	30 min
Complete tour of Azure Security Center and Security Blades.	1 hr

- We Hack -
PURPLE

QUESTIONS?

Contact Us

training@wehackpurple.com