# **+DSO گام بعدی برای DevSecOps**

با توجه به اهمیت APIها در معماری اپلیکیشن‌های جدید، ایجاد APIهای ایمن امری حیاتی می‌باشد. مقوله امنیت را نمی‌توان نادیده گرفت و باید آن را جزئی از کل چرخه توسعه اپلیکیشن در نظر گرفت. انجام اسکن و تست‌ نفود، آن هم به صورت سالیانه به هیچ عنوان کافی نمی‌باشد.

DevSecOps باید به فرایند توسعه افزوده شده و در تمام زمان‌های توسعه نرم افزار، انجام تست‌های امنیتی مداوم را تسهیل کند. هدف آنها بهره‌گیری از خودکارسازی‌ فرایندهای امنیتی در جهت بهبود فرایند تولید نرم افزار بوده به شکلی که تاثیری بر سرعت توسعه نداشته باشد. اگر شک دارید، [مانیفست DevSecOps](https://www.devsecops.org/) را بررسی کنید تا در جریان باشید.

|  |  |
| --- | --- |
| **درک مدل تهدیدات[[1]](#footnote-1)** | اولویت‌ تست‌ها از مدل تهدیدات بدست می‌آید. اگر شما مدل تهدیدات ندارید می‌توانید از [OWASP Application Security Verification Standard (ASVS)](https://owasp.org/www-project-application-security-verification-standard/) و [OWASP Testing Guide](https://owasp.org/www-project-web-security-testing-guide/) به عنوان ورودی استفاده کنید. همچنین مشارکت دادن تیم توسعه می‌تواند باعث شود آنها نسبت به موضوعات امنیتی آگاه‌تر شوند. |
| **درک چرخه توسعه نرم افزار** | تیم توسعه را به فرایند اضافه کنید تا آنها نیز درک بهتری از چرحه توسعه نرم افزار پیدا کنند. مشارکت شما در انجام تست‌های مداوم امنیتی باید همراستا با افراد، فرایند‌ها و ابزارها باشد. همه باید با فرایند موافق باشند تا هیچ گونه اصطکاک و مقاومتی وجود نداشته باشد. |
| **راهبرد انجام تست** | با توجه به اینکه کار شما نباید تاثیری بر سرعت توسعه داشته باشد. بنابراین باید خیلی آگاهانه بهترین تکنیک (ساده، سریع‌ترین و دقیق‌ترین)‌ را برای تایید الزامات امنیتی انتخاب کنید. [OWASP Security Knowledge Framework](https://owasp.org/www-project-security-knowledge-framework/) و [OWASP Application Security Verification Standard](https://owasp.org/www-project-application-security-verification-standard/) می‌توانند منابع خوبی برای الزامات عملکردی و غیر عملکردی باشند. منابع خوب دیگری از [پروژه‌ها](http://devsecops.github.io/) و [ابزارها](https://github.com/devsecops/awesome-devsecops) مشابه با مواردی که توسط [DevSecOps community](file:///C:\\Users\\Neo\\Downloads\\devsecops.org) پیشنهاد می‌شود، وجود دارد. |
| **دستیابی به جامعیت و دقت** | شما پلی هستید بین تیم‌ توسعه دهنده و ‌‌‌پیاده‌سازی، برای اینکه به این مهم دست یابید نه تنها باید بر روی عملکرد و قابلیت‌ها تمرکز کنید بلکه باید به هماهنگی نیز توجه کنید. از ابتدا به صورت نزدیک با هر دو تیم توسعه و ‌‌‌پیاده‌سازی کار کنید تا بتوانید زمان و تلاش‌تان را بهینه نمایید. شما باید برای حالتی که الزامات امنیتی به صورت مداوم بررسی شوند، هدف گذاری کنید. |
| **به وضوح یافته‌‌‌ها را به اشتراک بگذارید** | با کمترین اصطکاک یا بدون اصطکاک مشارکت داشته باشید. یافته‌‌ها را در بازه زمانی مشخص و در قالب ابزارهای مورد استفاده توسط تیم توسعه (نه فایل‌های PDF) تحویل دهید. به تیم توسعه اضافه شوید تا یافته‌ها را به آن‌ها نشان دهید. از این فرصت برای آموزش آنها استفاده کنید، به صورت شفاف در مورد نقطه ضعف و روش‌های سوء استفاده از آن (که شامل سناریو‌های حملات می‌باشند) توضیح دهید تا واقعی به نظر برسد. |

1. Threat Model [↑](#footnote-ref-1)