# **+D گام بعدی برای توسعه‌دهندگان**

وظایف مرتبط با ایجاد و نگهداری ایمن از نرم افزارها یا تعمیر نرم افزارهای موجود می‌تواند دشوار باشد و APIها نیز از قضیه مستثنی نیستند.

بر این باوریم که آموزش و آگاه سازی، گامی کلیدی در راستای نوشتن و توسعه نرم افزارهای ایمن هستند. تمامی الزامات دیگر در راستای نیل به هدف فوق به ایجاد و استفاده از فرایندهای امنیتی تکرارپذیر و کنترل‌های امنیتی استاندارد بستگی دارد.

OWASP منابع آزاد و رایگان متعددی برای پاسخ به مسائل امنیتی از ابتدای پروژه ایجاد نموده است. به منظور آشنایی با لیست جامع پروژه‌‌های دردسترس، [صفحه پروژه‌‌های OWASP](https://www.owasp.org/index.php/Category:OWASP_Project) را ملاحظه نمایید.

|  |  |
| --- | --- |
| **آموزش** | برای شروع می‌توان از [پروژه مطالب آموزشی OWASP](https://www.owasp.org/index.php/OWASP_Education_Material_Categorized) بسته به علاقه و نوع حرفه آغاز نمود. برای آموزش عملیاتی، crAPI[[1]](#footnote-1)را نیز به [نقشه راه](https://www.owasp.org/index.php/OWASP_API_Security_Project" \l "tab=Road_Map) خود افزوده‌ایم. تست‌‌های مربوط به WebAppSec را می‌توان با [OWASP DevSlop Pixi Module](https://devslop.co/Home/Pixi) که یک WebApp و سرویس API آزمایشگاهی آسیب‌پذیر است، انجام داد. استفاده از چنین ابزارهایی سبب یادگیری نحوه تست وب اپلیکیشن‌‌ها و APIهای مدرن از منظر مسائل امنیتی و چگونگی توسعه APIهای مدرن در آینده خواهد شد. همچنین امکان شرکت در جلسات آموزشی [کنفرانس AppSec](https://www.owasp.org/index.php/Category:OWASP_AppSec_Conference) و عضویت در [شَعب محلی OWASP](https://www.owasp.org/index.php/OWASP_Chapter) نیز برای علاقه مندان وجود دارد. |
| **الزامات امنیتی** | امنیت باید بعنوان بخشی تفکیک ناپذیر در تمامی پروژه‌‌ها از ابتدا درنظر گرفته شود. در هنگام استخراج الزامات امنیتی، باید معنی واژه «ایمن» برای هر پروژه مشخصا تعریف شود. OWASP استفاده از [استاندارد امنیت سنجی اپلیکیشن (ASVS)](https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project) را بعنوان راهنمایی برای تعیین الزامات امنیتی توصیه می‌کند. در صورت برون سپاری نیز، استفاده از [ضمیمه قرارداد نرم افزار ایمن OWASP](https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex) (که بایستی با قوانین و رگولاتوری‌‌های محلی انطباق یابد) می‌تواند انتخاب مناسبی باشد. |
| **معماری امنیتی** | امنیت بایستی در تمامی مراحل توسعه پروژه‌‌ها اهمیت داشته باشد. [برگه‌‌های راهنمای پیشگیری](https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series) OWASP نقطه شروع مناسبی برای چگونگی طراحی ایمن در خلال فاز طراحی معماری به شمار آید. همچنین [برگه راهنمای امنیت REST](https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/REST_Security_Cheat_Sheet.md) و [برگه راهنمای ارزیابی REST](https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/REST_Assessment_Cheat_Sheet.md) نیز گزینه‌‌های مناسبی در این راستا هستند. |
| **کنترل‌‌های امنیتی استاندارد** | بکارگیری و انطباق با کنترل‌‌های امنیتی استاندارد ریسک ایجاد ضعف‌‌های امنیتی در خلال ایجاد برنامه‌‌ها با منطق سازمانی را کاهش می‌دهد. علیرغم اینکه بسیاری از چارچوب‌های مدرن امروزی با استانداردهای توکار و موثر امنیتی توزیع می‌شوند، اما [کنترل‌‌های پیشگیرانه و فعال OWASP](https://www.owasp.org/index.php/OWASP_Proactive_Controls#tab=OWASP_Proactive_Controls_2018) دید خوبی از کنترل‌‌هایی که باید در پروژه‌‌ها لحاظ شوند بدست می‌دهد. OWASP کتابخانه و ابزارهای متعددی از جمله در حوزه کنترل‌‌های اعتبارسنجی در اختیار عموم قرار می‌دهد که می‌توانند مفید باشند. |
| **چرخه حیات توسعه نرم افزار ایمن** | به منظور بهبود فرایندها در هنگام ایجاد و ساخت APIها می‌توان از [مدل ضمانت کمال نرم افزار OWASP (SAMM)](https://www.owasp.org/index.php/OWASP_SAMM_Project) بهره برد. همچنین پروژه‌‌های متعدد دیگری نیز در OWASP وجود دارند که می‌توانند در فازهای مختلف توسعه API مفید باشند که از جمله آنها می‌توان، [پروژه بازبینی کد OWASP](https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project) را نام برد. |

1. Completely Ridiculous API [↑](#footnote-ref-1)