# **+DAT متدلوژی و داده**

**بررسی اجمالی**

از آنجا که صنعت AppSec مشخصا بر امنیت اپلیکیشن‌‌های معماری نوین که در آنها API نقشی حیاتی دارد، تمرکز ننموده، ایجاد لیستی از ده ریسک امنیتی بحرانی امنیت API بر مبنای فراخوان عمومی کاری سخت خواهد بود. علیرغم اینکه فراخوانی برای داده‌‌های عمومی داده نشده، اما لیست فعلی بر مبنای داده‌های در دسترس عموم، مشارکت کارشناسان امنیتی و نظرات متخصصان حوزه امنیت، تهیه گردیده است.

**متدلوژی و داده**

در فاز اول، داده‌‌های در دسترس عموم در حوزه رخداده‌‌های مرتبط با امنیت API توسط گروهی از متخصصین امنیت جمع آوری، بازبینی و دسته بندی شدند. این داده‌‌ها از پلتفرم‌‌های شکار باگ[[1]](#footnote-1) و پایگاه‌‌های داده آسیب‌پذیری در یک چارچوب زمانی یک ساله به منظور تحلیل آماری جمع آوری شده اند.

در فاز بعد، از متخصصین امنیت با سویه عملیاتی و تجربه تست نفوذ خواسته شد تا آنان نیز لیست ده ریسک امنیتی بحرانی API از منظر خود را با گروه به اشتراک گذارند.

به منظور انجام فرایند تحلیل ریسک از [متدلوژی رتبه بندی ریسک OWASP](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology) استفاده و نتایج آن نیز توسط متخصصین امنیتی بازبینی قرار گرفت. برای مطالعه بیشتر در این حوزه به بخش ریسک‌‌های امنیتی API مراجعه نمایید.

پیش نویس اولیه ده ریسک امنیتی بحرانی APIها در 2019 از منظر OWASP از اجماع بین نتایج آماری فاز اول و لیست مدنظر متخصصین بدست آمده است و سپس به منظور بازبینی مجدد در اختیار گروه دیگری از متخصصین (با تجربه مرتبط در حوزه امنیت API) قرار گرفته است.

مستند ده ریسک امنیتی بحرانی APIها در 2019 از منظر OWASP اولین بار در رویداد جهانیOWASP AppSec در تل‌آویو (می 2019) ارائه شده و پس از آن برای بحث و مشارکت عموم در GitHub قرار گرفت.

لیست مشارکت کنندگان در بخش سپاسگزاری‌‌ها قابل مشاهده است.

1. Bug Bounty [↑](#footnote-ref-1)