



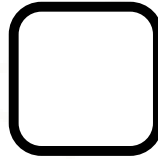
مقایسه SAST و DAST

بررسی ایستا امنیت اپلیکیشن یا Static Application Security Test و بررسی پویا امنیت اپلیکیشن یا Dynamic Application

Security Test در فرآیند بررسی آسیب پذیری ها در لایه اپلیکیشن مورد استفاده قرار میگیرند.

تست نفوذ جعبه سیاه چیست

شناسایی و کشف آسیب پذیری در اپلیکیشن اجرا شده کشف و گزارش میگردد.

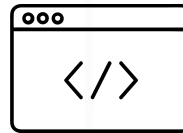
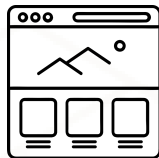


تست نفوذ جعبه سفید چیست

شناسایی و کشف آسیب پذیری در سورس کد کشف و گزارش میگردد.

نیاز به اپلیکیشن در حال اجرا

برای بررسی نیاز به دسترسی به اپلیکیشن اجرا شده در نسخه مورد نظر می باشد.



نیاز به سورس کد

برای بررسی نیاز به دسترسی به کد بر اساس مرحله یا stage تست می باشد.

هزینه فنی زیاد تر برای رفع باگ

میزان و عمق آسیب پذیری های کشف شده با توجه به مرحله تست شامل تغییرات گسترده در لایه اپلیکیشن میگردد.

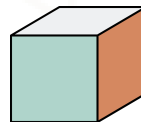
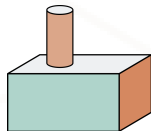


هزینه فنی کم تر برای رفع باگ

میزان و عمق آسیب پذیری های کشف شده با توجه به مرحله تست اغلب شامل تغییرات کم تر در لایه اپلیکیشن می باشد.

امکان اجرا پس از بررسی Static

پیشنهاد میگردد پس از بررسی static و با توجه به معماری اپلیکیشن، بررسی پویا انجام گیرد.



امکان اجرا پس از بررسی Dynamic

پیشنهاد میگردد بررسی static در مراحل ابتدایی توسعه و پیش از بررسی dynamic صورت گیرد.

میزان آسیب پذیری کشف شده کمتر به نسبت بررسی Static

با توجه به دسترسی به اپلیکیشن از سمت کاربر و همچنین امکان بهره برداری از آسیب پذیری، میزان کشف آسیب پذیری های false-positive در این بخش کم تر می باشد.



امکان ایجاد Noise بیشتر

با توجه به الگوهای آسیب پذیری و همچنین معماری و توسعه نادرست بخش های مختلف اپلیکیشن، میزان کشف آسیب پذیری در این بخش بسیار زیاد تر می باشد.