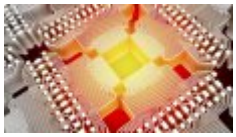
مایکروسافت ابزار رایگان شناسایی آسیب‌پذیری وب‌سایت‌ها را منتشر کرد

مایکروسافت به‌تازگی ابزار بسیار کارآمدی موسوم به سونار (Sonar) را منتشر کرده است که به مالکان سایت‌ها اجازه می‌دهد وب‌سایت خود را به‌منظور شناسایی آسیب‌پذیری‌های احتمالی مورد بررسی قرار دهند. سونار یک ابزار متن باز است که در گروه ابزارهای امنیتی قرار می‌گیرد. این ابزار ضمن آنکه مشکلات مربوط به عملکرد، قابلیت دسترسی و کارایی یک سایت را مورد بررسی قرار می‌دهد، مشکلات امنیتی یک سایت را نیز شناسایی می‌کند. این ابزار از سوی تیم مایکروسافت اج و به شکل متن باز طراحی شده و به بنیاد جاوا اسکریپت اهدا شده است.

در حالی که مایکروسافت ابزار فوق را به این بنیاد اهدا کرده است، اما همچنان از این نرم‌افزار پشتیبانی و قابلیت‌هایی متناسب با تهدیدات امنیتی را به آن اضافه خواهد کرد. تیم سازنده اعلام کرده است که از هرگونه تعاملی با توسعه‌دهندگان ثالث به‌منظور بهتر شدن کیفیت ابزار خود استقبال می‌کند. سونار از رویکردی موسوم به Linting برای ارزیابی یک سایت استفاده می‌کند. Linting به فرآیندی گفته می‌شود که در آن یک برنامه به‌منظور تحلیل کدها ارزیابی شده تا خطاهای بالقوه نرم‌افزار شناسایی شود. سونار طیف گسترده‌ای از مشکلات مرتبط با عملکرد، سطح دسترسی، امنیت و قابلیت همکاری را مورد بررسی قرار داده و به‌خوبی قادر است برنامه‌های وب پیش‌رونده (PWA) (سرنام Progressive Web Apps) را تحلیل کند. مایکروسافت ابزار سونار را در قالب یک پروژه متن باز روی گیت‌هاب قرار داده است تا طراحان با استفاده از آن بتوانند باگ‌های ناپیدای درون یک وب‌سایت را پیدا کنند. در حوزه امنیت، سونار هشت نوع آسیب‌پذیری مهم همچون مشکلات مربوط به پیکربندی SSL را مورد بررسی قرار می‌دهد. در ارتباط با مشکلات مربوط به SSL سونار از ابزار طراحی شده از سوی آزمایشگاه‌های SSL موسوم به SSL Server Test استفاده می‌کند. برای اطلاعات بیشتر در ارتباط با ابزارهای ارائه شده از سوی این آزمایشگاه به نشانی https://ssllabs.com/ مراجعه کنید. آزمایش دیگری که از سوی این ابزار انجام می‌شود در ارتباط با ارتباطات مبتنی بر پروتکل انتقال ابر متن ایمن (HTTPS) است. این ابزار جست‌وجویی انجام می‌دهد تا ارتباطاتی که از مکانیسم ارسال و دریافت اطلاعات با امنیت بالا استفاده نمی‌کنند را شناسایی کند. این ابزار به‌دنبال اتصالات HTTPS می‌گردد که از سرباره Strict-Transport-Security استفاده نمی‌کنند. این کار از آن جهت انجام می‌شود تا به مدیران سایت‌ها اطمینان دهد سایت آن‌ها به‌درستی از پروتکل فوق استفاده می‌کند و در معرض حملات مرد میانی (man-in-the-middle) قرار نخواهد گرفت. یکی از شاخص‌ترین ویژگی‌های ابزار فوق این است که به توسعه‌دهندگان اجازه می‌دهد تا مطلع شوند آیا برنامه‌های کاربردی یا سایت‌های آن‌ها به آسیب‌پذیری‌هایی که درنهایت به پیاده‌سازی حملات شنود MIME منجر می‌شوند آلوده هستند یا خیر.

مطلب پیشنهادی



زبانی ویژه برنامه‌نویسی کوانتومی
مایکروسافت از زبان برنامه‌نویسی کوانتومی کیوشارپ رونمایی کرد

در حالی که برای یک سری کاربردهای خاص و تحلیلی می‌توان از مکانیسم شنود MIME استفاده کرد، اما واقعیت این است که این مکانیسم مخاطرات امنیتی مختلفی را به همراه دارد. اما اگر سایتی از گزینه-X-Content-Type Options: nosniff در پاسخ به سربارها استفاده کند، از شدت این مخاطرات امنیتی کاسته می‌شود. سونار همچنین به بررسی این موضوع می‌پردازد که آیا سرباره تنظیم کوکی (Cookie-set) در خاصیت HttpOnly به‌شکل ایمنی تعریف شده است؟ به طوری که مانع از آن شود تا نشست‌های مربوط به کوکی در حملات تزریق اسکریپت به یک سایت (XSS) مورد سوءاستفاده قرار نگیرد؟ در حالت عادی کوکی‌ها نباید در سراسر پروتکل HTTP انتقال پیدا کنند و همچنین مقادیر مربوط به آن‌ها نیز نباید از طریق جاوا اسکریپت در دسترس قرار گیرد. قابلیت فوق‌العاده مهم دیگری که سونار به آن تجهیز شده است در ارتباط با کتابخانه و چهارچوب‌های جاوا اسکریپتی است که در سمت کلاینت مورد استفاده قرار می‌گیرد. اگر چهارچوب یا کتابخانه‌ای به آسیب‌پذیری‌هایی آلوده باشد و سایتی در سمت کلاینت از آن استفاده کند، سونار قادر است این موضوع را تشخیص دهد. برای این منظور از بانک اطلاعاتی Snky که مشتمل بر آسیب‌پذیری‌های شناسایی شده است و همچنین ابزار js-library-detector استفاده می‌شود. سونار سرباره‌هایی را که ممکن است داده‌های حساس و بالقوه‌ای را منتشر کنند مورد بررسی قرار داده و اجازه نمی‌دهد این سرآیندها اطلاعات حساس سایت‌ها را منتشر کنند. همچنین مانع از آن می‌شود تا تغییر مسیرهای غیرمجازی به وجود آید که درنهایت کاربران را به‌سمت سایت‌های فیشینگ و مخرب هدایت می‌کنند. سونار را می‌توانید به‌شکل محلی و در قالب یک ابزار خط فرمان مورد استفاده قرار دهید، اما یک نسخه آنلاین از آن نیز در دسترستان قرار دارد. این ابزار با محصولات دیگری همچون SSL Labs، snky.io، AMP validator، aXe Core و Cloudinary یکپارچه شده است. ابزار فوق در نشانی https://sonarwhal.com/scanner در اختیارتان قرار دارد.

تاریخ انتشار:

25 دی 1396

نشانی منبع:
https://www.shabakeh-mag.com/security/11326/%D9%85%D8%A7%DB%8C%DA%A9%D8%B1%D9%88%D8%B3%D8%A7%D9%81%D8%AA-%D8%A7%D8%A8%D8%B2%D8%A7%D8%B1-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%B4%D9%86%D8%A7%D8%B3%D8%A7%DB%8C%DB%8C-%D8%A2%D8%B3%DB%8C%D8%A8%E2%80%8C%D9%BE%D8%B0%DB%8C%D8%B1%DB%8C-%D9%88%D8%A8%E2%80%8C%D8%B3%D8%A7%DB%8C%D8%AA%E2%80%8C%D9%87%D8%A7-%D8%B1%D8%A7-%D9%85%D9%86%D8%AA%D8%B4%D8%B1-%DA%A9%D8%B1%D8%AF