acunetix

WEB APPLICATION SECURITY

گروه شرکت های کارنما

شرکت کارنما رایانه ارائه کننده نرم افزار

acunetix

acunetix

آیا وب سایت شما قابل هک شدن است؟

بررسی امنیت و آسیب پذیری وب با اسکنر Acunetix

بررسی امنیت و آسیب پذیری وب با اسکنر Acunetix

بر اساس برآوردهای انجام گرفته در حدود ۷۰ درصد از وب سایت ها دارای آسیب پذیری هایی هستند که ممکن است روزی سرانجام منجر به سرقت داده های حساسشان شود . این اطلاعات طیف گسترده ای را در برمی گیرند، از اطلاعات مربوط به کارت های اعتباری گرفته تا فهرست مشتریان همگی در زمره این اطلاعات جای می گیرند.

چندی است که هکرها تلاش ها و فعالیت هایشان را روی برنامه های تحت وب متمرکز نموده اند؛ سبدهای خرید اینترنتی، فرم ها، صفحات ورود به وب سایت های مختلف، محتوی پویا و بسیاری دیگر بخشی از دایره فعالیت های نفوذی هکرها را تشکیل می دهند. امروزه برنامه های اینترنتی ناایمنی وجود دارند که به صورت شبانه روزی و در هر نقطه ای از جهان قابل استفاده می باشند و همین مسأله دسترسی هکرها به پایگاه های داده ای حساس و نهفته شرکت ها و امکان انجام فعالیت های غیرقانونی با استفاده از آن سایت را در اختیار تبهکاران قرار می دهد.

فایروال ها، SSL و سرورهای خارج از سرویس، ناتوان در برابر هک برنامه‌های مبتنی بر وب

حملاتی که از طریق پورت ۸۰/۴۴۳ علیه برنامه های تحت وب انجام می گیرند، مستقیما به فایروال، سیستم عامل های قدیمی و امنیت شبکه و در یک کلام قلب برنامه و داده های شرکت شما نفوذ می کند. برنامه هایی که به صورت سفارشی ساخته می شوند معمولا به خوبی تست نمی شوند و برخی آسیب پذیری هایشان کشف نشده باقی می ماند و به همین دلیل نفوذ به آنها برای هکرها بسیار ساده است.

بنابراین توصیه ما به شما این است که پیش از آنکه هکرها بتوانند به داده های حساس شرکت شما دست پیدا کرده و از طریق وب سایت شما مرتکب جرائم خطرناکی شده و در نهایت کسب و کارتان را به مخاطره بیاندازند، از بابت ایمنی و امنیت وب سایت خود اطمینان کامل را حاصل نمایید. اسکنر Acunetix (برای کشف آسیب پذیری های وب) وب سایت شما را زیر و رو کرده و پس از بررسی دقیق برنامه های موجود در آن هرگونه تزریق مشکوک دستورات SQL، حملات XSS و دیگر آسیب پذیری هایی که ممکن است کسب و کار آنلاین شما را به خطر بیاندازد پیدا می کند . این برنامه با ارائه گزارشات دقیق مشخص می کند که برنامه های اینترنتی در چه قسمت هایی نیاز به رفع اشکال دارند و به این ترتیب وب سایت شما را در برابر حملات احتمالی هکرها حفظ خواهند کرد.

اکیونتیکس؛ ابزار مطرح جهانی برای حفظ امنیت برنامه‌های وبی

فناوری اسکن ابزار اکیونتیکس در سطح جهانی مطرح می باشد: مهندسین سازنده این ابزار از مدت ها پیش (۱۹۹۷) به فکر امنیت وب افتادند و با توسعه این ابزار، به جایگاه نخست در تحلیل وب سایت و تشخیص آسیب پذیری دست پیدا کردند.

این اسکنر از بخش های مبتکرانه بسیاری تشکیل شده است که در ادامه به ذکر برخی از آن ها خواهیم پرداخت:

- فناوری مبتکرانه AcuSensor که با ترکیب نمودن فناوری های اسکن جعبه سیاه (Black Box) با بازخوردهای موجود، حسگرهای خود را داخل کد منبع قرار داده و به این ترتیب امکان اسکن دقیق وب سایت با پایین ترین نرخ تشخیص نادرست را فراهم می کند.
- تحلیل گر خودکار دستورات جاوا از دیگر مشخصه های این ابزار است که امکان تست امنیتی برنامه های مبتنی بر آژاکس (Ajax) و Web 2.0 را فراهم میکند.
- پیشرفته ترین قابلیت تست حملات XSS و تزریق دستورات SQL از دیگر قابلیت های مهم این برنامه محسوب می شود.
- ثبت کننده بصری که کار تست فرم های اینترنتی و بخش های حفاظت شده (از طریق کلمات عبور) آن را راحت تر می کند، از دیگر امکانات این برنامه است.
- اسکنر پر سرعت و مالتی ترد (پردازش همزمان یک کد در مراحل مختلف اجرای یک دستور) با قابلیت بررسی صدها هزار صفحه مختلف و بدون بروز هرگونه اختلال.
- پویشگر آسیب پذیری وب اکیونتیکس قابلیت درک و تشخیص فناوری های پیچیده وب نظیر Json, Ajax, XML, Soap را دارد.

Acunetix Customers:

NASA, U.S. AIR FORCE, THE PENTAGON, U.S. DEPARTMENT OF ENERGY, U.S.ARMY, AMERICAN EXPRESS, NORWEGIAN ARMED FORCES, CISCO, London Stock Exchange, ING, BANK OF CHINA, CREDIT SUISSE, SONY, Deloitte., HSBC, KPMG, PRICEWATERHOUSECOOPERS, Deutsche Bank, CERN, BARCLAYS, Panasonic, FUJITSU, WALT DISNEY PICTURES, france telecom

از دیدگاه مطبوعات:

ابزار Acunetix WVS علاوه بر آنکه آسیب پذیری های وب سایت شما را نشان می دهد، ابزارها و اطلاعات لازم برای تست برنامه های تحت وب را نیز در اختیارتان قرار خواهد داد. اکیونتیکس ابزاری بسیار مهم برای توسعه دهندگان وب خواهد بود؛ چراکه امکان اعمال تنظیمات متعددی در آن وجود دارد و از همین روی بهترین راهکار برای انجام تستهای دقیق محسوب می شود.

بررسی دقیق تزریق SQL و آسیب پذیری‌های موجود دربرابر حملات XSS

Acunetix WVS تمامی آسیب پذیری های اینترنتی از جمله تزریق SQL، حملات XSS و بسیاری دیگر را به دقت بررسی می کند. تزریق کدهای SQL یکی از تکنیک های هک کردن است که درخواست های SQL را با هدف دسترسی به داده های موجود در پایگاه های داده ای اصلاح می کند. حملات XSS هم به هکرها امکان می دهند که یک دستور مخرب را روی مرورگر بازدیدکنندگان آن سایت اجرا کنند.
تشخیص این آسیب پذیری ها نیز مستلزم دراختیار داشتن یک موتور تشخیص بسیار پیشرفته است. باید در نظر داشت که تعداد حملاتی که یک اسکنر می تواند تشخیص دهد اهمیتی در فرایند اسکن آسیب پذیری ها ندارد، بلکه مسأله مهم پیچیدگی و دقتی است که اسکنر از طریق آن فرایند تزریق کدهای SQL و دیگر حملات نظیر XSS را انجام میدهد.

فناوری مبتکرانه AcuSensor با نرخ خطای پایین

اکیونتیکس از نوعی موتور بسیار پیشرفته برای تشخیص آسیب پذیری برخوردار است که به همراه فناوری اکوسنسور (Acusensor) بهترین عملکرد را از خود به نمایش می گذارد. اکوسنسور نوعی فناوری امنیتی بسیار پیشرفته و بی مانند است که در کوتاه ترین زمان ممکن و با پایین ترین نرخ خطا آسیب پذیری های موجود در وب سایت شما را پیدا می کند و محل دقیق آن آسیب پذیری را در کد مورد نظر تشخیص داده و اطلاعات مربوط به رفع خطاها را گزارش می دهد. این فناوری همچنین تزریق CRLF، کدهای اجرایی، مشاهده دایرکتوری، دخول فایل، آسیب پذیری های سندیت و بسیاری موارد دیگر را با تعیین موقعیت دقیق تشخیص می دهد.

فناوری‌های اسکن Ajax و Web 2.0 برای یافتن آسیب‌پذیری ها

موتور بسیار پیشرفته CSA (تحلیل گر کدهای کلاینت) به شما امکان می دهد که جدیدترین و پیچیده ترین برنامه های اینترنتی Ajax و Web 2.0 را به صورت کامل و همه جانبه اسکن نمایید؛ لازم به ذکر است که زبان مجازی اکیونتیکس موسوم به(Acunetix WVS) قابلیت درک SOAP، XML، AJAX و JSON را نیز دارد.

تست قسمت‌های محافظت شده در برابر پسورد و فرم‌ها با پرکننده خودکار فرم‌های اینترنتی

اسکنر اکیونتیکس قادر است که به صورت خودکار فرم های اینترنتی را پرکرده و سندیت ورود به برنامه های مختلف را بررسی نماید. اغلب اسکنرهای موجود توانایی انجام این کار را ندارند یا برای تست چنین صفحاتی به کدهای بسیار پیچیده ای نیاز دارند. اما اکیونتیکس اینگونه نیست: با استفاده از ابزار ثبت ماکروی این برنامه موسوم به Login Sequence Recorder می توان مراحل مختلف Log in یا ورود به وب سایت را از فرایند پر کردن فیلدها ثبت نمود یا اینکه صرفا به ثبت و ضبط یک فرایند خاص اکتفا نمود. آنگاه اسکنر این سکانس را در طول فرایند اسکن از نو پخش می کند و فرمهای اینترنتی را پر کرده و به صورت خودکار به بخش های حفاظت شده از طریق کلمه عبور دسترسی پیدا می کند.

در هر زمان و از هر مکانی، وب سایت‌های مختلف را اسکن کنید

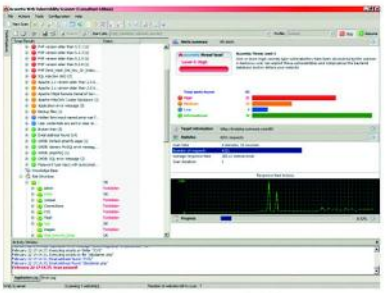
ابزار اکیونتیکس قادر است به طور همزمان تا ۱۰ وب سایت مختلف را تنها از یک رایانه اسکن نماید. از این رو می توان گفت که عملکرد و شتاب این ابزار در اسکن نمودن به میزان قابل توجهی بهبود یافته است. ممکن است بخواهید در مواقعی که وب سایت بازدیدکنندگان کمتری دارد برای مثال شب هنگام فرایند اسکن نمودن را انجام دهید که برای این منظور می توانید برنامه ریزی های لازم را با استفاده از این برنامه انجام دهید. به علاوه با استفاده از یک پرتال مشخص می توانید در هر نقطه ای از جهان و در هر ساعتی از شبانه روز به وب سایت مورد نظرتان Log in کرده، آن را اسکن کنید و در نهایت نتایج کار را دریافت نمایید.

گزارش‌های دقیق

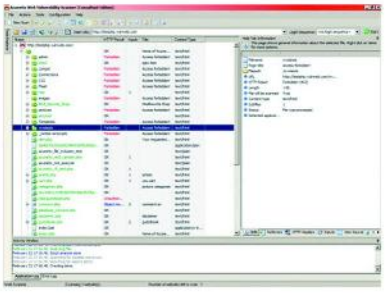
ابزار اسکن اکیونتیکس شامل یک ماژول اعلام گزارش فراگیر و گسترده می باشد که می تواند نشان دهد که آیا برنامه شما مطابق با استاندارد امنیت داده ایDSS PCI هست یا خیر. این ماژول همچنین شما را از وجود هریک از آسیب پذیری های ذکر شده در لیست ده گانه OWASP باخبر میکند که در واقع نوعی سازمان امنیت برنامه های اینترنتی است که هرچند وقت یک بار لیستی متشکل از ۱۰ آسیب پذیری اینترنتی جهانی را در اینترنت منتشر میکند. ابزار اکیونتیکس همچنین بررسی های لازم در رابطه با مطابقت برنامه اینترنتی مورد نظر شما با نشریه ویژه NIST ۵۳-۸۰۰ و همچنین دستورالعمل های توسعه و امنیت برنامه DISA موسوم به STIG (یا دستورالعمل فنی اجرای امنیت) بررسی می کند. علاوه بر این ها گزارشی در باب وجود هریک از خطاهای موجود در لیست ۲۵ گانه خطرناک ترین خطاهای نرم افزاری CWE/SANS نیز در اختیارتان قرار خواهد گرفت.

تحلیل وب سایت شما دربرابر پایگاه داده هک گوگل

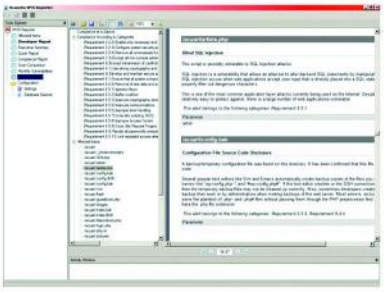
پایگاه داده ای هک گوگل از درخواست هایی تشکیل می شود که توسط هکرها برای شناسایی اطلاعات حساس موجود در وب سایتها ارائه می شوند و از آن جمله می توان به صفحات پورتال های Log in، گزارشات مربوط به امنیت شبکه، و غیره اشاره نمود. اکیونتیکس این درخواست ها را در محتوی وب سایت شما اجرا کرده و سپس پیش از آنکه دست هکرها به داده های حساس و یا اهداف قابل سوء استفاده برسد، آن ها را شناسایی می کند.



این برنامه در آشکارسازی حملات خودکار و آسیب پذیری ها به شما کمک می کند.



اسکن خودکار وب سایت سازمان و نمایش ساختار آن



ارائه گزارش‌های کامل و بر اساس PCI VISA

اسکن ها به سرعت و آسانی انجام می شود.

نمونه‌ای از گزارش اسکن