ارتبط امن
Ertebate Amn

acunetix

آیا وب سایت شما قابل هک است؟

آن را با اسکنر آسیب پذیری های وب Acunetix بررسی نمایید.

بیش از ۷۰ درصد از وبسایت ها آسیب پذیری هایی دارند که می تواند به سرقت اطلاعات حساس شرکت منجر شود. مانند اطلاعات کارت اعتباری و لیست مشتریان شرکت. هکرها تلاش خود را روی برنامه های تحت وب متمرکز می کنند مانند نرم افزارهای سبد خرید، فرم ها، صفحات ورود به سیستم، محتوای یوپا و غیره. با قابلیت دسترسی از هر نقطه جهان در ۲۴ ساعت شبانه روز و هفت روز هفته، برنامه های تحت وب نا امن امکان دسترسی آسان به بخش مدیریت پایگاه داده های شرکت را فراهم می کنند و همچنین به هکرها اجازه می دهند تا فعالیت های غیر قانونی را با استفاده از سایت قربانی انجام دهند.

فایروال ها، SSL و شبکه های امن شده در برابر هک برنامه های تحت وب بی فایده هستند!

حملات برنامه های وب که روی پورت ۸۰/۴۴۳ انجام می شود، از فایروال عبور کرده، از سیستم عامل و امنیت سطح شبکه گذشته و درست به سمت قلب برنامه و داده های شرکت شما نفوذ می کنند. برنامه های کاربردی سفارشی تحت وب اغلب به اندازه کافی تست نمی شوند و دارای آسیب پذیری های کشف نشده ای هستند که در نتیجه طعمه های آسان برای هکرها می باشند.

قبل از اینکه هکرها اطلاعات حساس شما را دانلود کنند و از طریق وبسایت شما فعالیت های مجرمانه انجام دهند و کسب و کارتان را به خطر بیندازند، از امن بودن وبسایت خود مطلع شوید. سامانه Acunetix به صورت خودکار وب سایت وبرنامه های تحت وب شما را پویش کرده و وب سایت های تولید انبوه و سفارشی و برنامه های کاربردی وب را برای جستجوی حفره های امنیتی مانند SQLInjection، Host Header Attacks، SSRF، XXE، XSS و بیش از ۵۰۰ آسیب پذیری دیگر وب، اسکن می کند.

پویش و اسکن

چیزی را که قابل پویش نباشد را نمی توانید اسکن کنید . Acunetix می تواند در معماری برنامه های تحت وب پیچیده از جمله برنامه های HTML5 سنگین جاوا اسکریپت پویش کند در حالی که با سهولت قادر به اسکن خودکار مناطق محدود شده نیز می باشد.

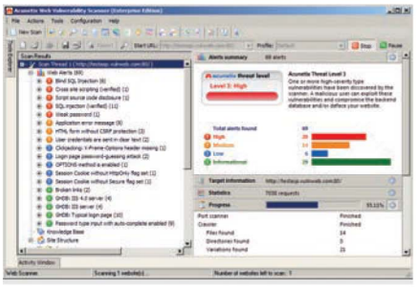
تشخیص و اخطار

با کشف آسیب پذیری، دقت نرم افزار سنجیده میشود. Acunetix بیش از ۵۰۰ آسیب پذیری برنامه تحت وب را تشخیص داده و طبق اهمیت آنها هشدار می دهد، اما توانایی منحصر بفرد آن در اسکن با دقت بالا، میزان پایین مثبت های کاذب، آن را برترین راهکار در این حوزه می نماید.

گزارش و اصلاح

طیف گسترده ای از گزارشات هم به توسعه دهندگان و هم به صاحبان کسب و کار کمک می کند تا به سرعت سطح تهدید یک برنامه تحت وب را شناسایی کنند، و تشخیص دهند چه چیزی نیاز به تعمیر دارد، و انطباق با استاندارد های مختلف را تضمین می کند.

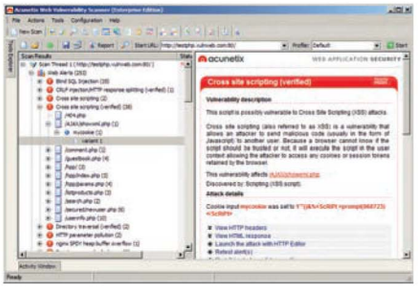
Acunetix پرچم دار فن آوری در امنیت برنامه تحت وب



رابط کاربری اصلی

Acunetix از پیشگامان در تست خودکار امنیت برنامه تحت وب و مهندسی پیشرو درتجزیه و تحلیل ساختار وب سایت و تشخیص آسیب پذیری است. فناوری های نوآورانه Acunetix شامل موارد زیر می باشد :

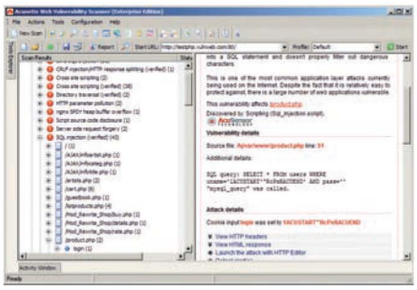
- فناوری Deep Scan امکان پویش دقیق برنامه های تک صفحه سمت سرویس گیرنده و سنگین SOAP را فراهم می کند که فناوری های پیچیده ای مانند SPAs/JSON،XML،WADL Google Web Toolkit، WDSL، SOAP/WCF، و عملیات CRUD را تحت نفوذ قرار می دهد
- پیشرفته ترین و قوی ترین تست SQL و Cross-site Scripting در صنعت از جمله تشخیص پیشرفته اسکریپت Cross-site مبتنی بر DOM.
- Login Sequence Recorder که امکان پویش و اسکن خودکار صفحات محافظت شده با رمز های پیچیده را فراهم میکند مانند multi-step, Single Sign-On و وب سایت های مبتنی بر OAuth.
- فناوری AcuSensor امکان اسکن دقیق بیشتر را با کاهش میزان مثبت کاذب و با ترکیب تکنیک های اسکن جعبه سیاه با دریافت بازخورد از حسگرهای آن که در داخل کد منبع قرار دارند،فراهم می کند.
- بالاترین تشخیص اسکن آسیب پذیری وردپرس (WordPress) -اسکن وردپرس برای بیش از ۱۲۰۰ آسیب پذیری شناخته شده در هسته،تم ها و پلاگین های وردپرس.
- پویشگر و اسکنر فوق سریع با قابلیت اسکن چند وب سایت بطور همزمان که می تواند بدون وقفه در صدها هزار صفحه پویش کند.
- به راحتی طیف گسترده‌ای از گزارشات فنی و انطباق را برای توسعه دهندگان وب و صاحبان کسب و کار تولید می کند.



آسیب پذیری های XSS

چک کردن دقیق آسیب پذیری های SQL Injection و Cross-Site Scripting به اختصار (XSS)

Acunetix با دقتی بسیار بالا صدها آسیب پذیری برنامه های تحت وب از جمله SQL Injection و Cross-site Scripting تست می کند. SQL Injection یکی از قدیمی ترین و شایع ترین اشکالات یا باگ های نرم افزاری است: این باگ به حمله کنندگان اجازه می دهد تا Query های مربوط به SQL را به منظور به دست آوردن دسترسی به داده ها در پایگاه داده تغییر دهند. حملات Cross-site Scripting به حمله کنندگان اجازه می دهد تا اسکریپت های مخرب را در داخل مرورگر بازدید کنندگان اجرا کنند: که احتمالاً منجر به جعل هویت کاربران می شود؛ Acunetix در صنعت پیشرو در زمینه تشخیص بزرگترین انواع آسیب پذیری های XSS و SQL Injection است: از جمله Out-of Band SQL Injection و XSS بر اساس DOM می باشد.



نمایش Query های SQL (با تشکر از Acu Sensor)

فناوری AcuSensor ، مثبت های کاذب بسیار پایین را تضمین می کند

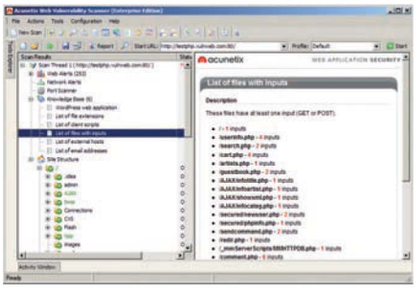
Acunetix شامل فناوری منحصر به فرد AcuSensor است که فقط همان کدی را تجزیه و تحلیل می کند که اجرا می شود. این قابلیت منجر به نرخ تشخیص بالاتر و به طور قابل توجهی باعث حذف مثبت های نادرست می شود. علاوه بر این، فناوری AcuSensor قادر به نشان دادن محل آسیب پذیری در کد و گزارش اطلاعات اشکال زدایی است AcuSensor. نه تنها آسیب پذیری های بیشتری را پیدا می کند، بلکه زمان با ارزشی را برای تیم های امنیت و توسعه خود حفظ می کند.

تست برنامه های تحت وب تأیید شده با (Login Sequence Recorder)

تست صفحات تأیید شده ای از برنامه های کاربردی تحت وب شما برای اطمینان از پوشش کامل تست ، کاملا مهم است. اسکنر آسیب پذیری Acunetix می تواند به طور خودکار نواحی تأیید شده را با استفاده از Login Sequence Recorder تست کند. بدین ترتیب Login Sequence Recorder امکان ضبط مراحل انجام کار را راحت می کند که اسکنر Acunetix می تواند برای تایید صفحه مورد نظر به این اقدامات ضبط شده رجوع کند.همچنین Login Sequence Recorder می تواند مجموعه ای از محدودیت ها را ضبط کند که برای کاستن از دامنه اسکن تنها با چند کلیک به راحتی انجام پذیر خواهد بود.

فناوری Deep Scan محتوای بیشتری را اسکن می کند

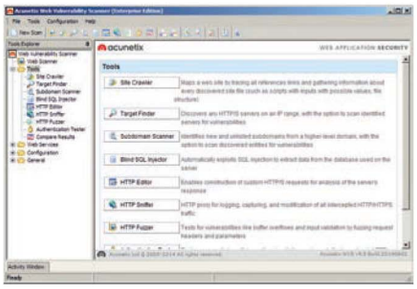
فرایند اساسی در طول هر اسکن این است که اسکنر بتواند بدرستی یک برنامه را پویش کند صرف نظر این که از کدام فناوری برای ساخت وب استفاده شده است. اسکنر آسیب پذیری Acunetix با استفاده از فناوری Deep Scan موتور اسکن و پویشگر HTML5 بطور کامل عملکرد تعاملی یک بازدید کننده از سایت شما را با اجرا و تجزیه و تحلیل جاوا اسکریپت شبیه سازی می کند. DEEP SCAN این امکان را فراهم می کند که عملیات پویش به دقت در AJAX-heavy client side single Page Application انجام شود که از فناوری هایی مانند Google Web Toolkit و AngularJs,EmberJS استفاده می کند. همچنین می تواند فناوری های پیچیده وب را درک کرده و با آنها تعامل کند مانند WDSL/SOAP، WCF/SOAP، WADL، XML، AJAX GWT و عملیات CRUD . علاوه بر این DEEP Scan برای تجزیه و تحلیل وب سایت ها و برنامه های کاربردی وب توسعه یافته در Ruby On Rails و فریم ورک های جاوا از جمله Java Server Faces (JSF) Spring و Struts به نحو مطلوبی بهینه شده است.



پایگاه دانش نشان دهنده لیستی از فایل ها با ورودی

اسکن پیشرفته سطح شبکه

بازرسی های امنیتی جامع نیاز به بازرسی دقیق محیط و دارایی های شبکه عمومی شما دارد. Acunetix با یکپارچه سازی اسکنر Open VAS با اسکنر آنلاین خود امکان انجام یک اسکن جامع و همه جانبه از سطح شبکه را مهیا کرده است که بطور کامل با تست امنیت برنامه های کاربردی تحت وب شما یکپارچه شده است به گونه ای که یک راهکار ساده پردازش ابری برای شما فراهم می کند. Acunetix کلمات عبور ضعیف، پیکربندی نا امن وب سرور، دایرکتوری هایی با مجوز ضعیف، آسیب پذیری های سرور DNS، تست های دسترسی FTP، سرورهای پروکسی که نامناسب پیکربندی شده اند، رمزهای SSL ضعیف و بسیاری دیگر از بررسی های امنیتی پیچیده را تست خواهد کرد.



ابزارهای تست دستی Acunetix

گزارشات دقیق و با جزئیات شما را قادر می سازد تا الزامات قانونی و مقررات را پیاده سازی نمایید

به منظور ثبت و پیگیری آسیب پذیری های شناسایی شده در برنامه های کاربردی وب شما، اسکنر Acunetix گزارش های گسترده ای برای کمک به مدیریت و تسریع روند اصلاح آسیب پذیری ارائه می کند در حالی که الویت بندی اقدامات اصلاحی را نیز مشخص می نماید. این گزارشات همچنین شامل طیف وسیعی از گزارشات انطباق پذیری و طبقه بندی است از جمله OWASP Top 10؛ PCI DSS؛ ISO 27001؛ Sarbens؛NIST Special Publication 800-53(for FISMA); Mitre: HIPAA Oxley: SANS 25Most Dangerous /Mitre CWE Software Error– و ...

اسکن آسیب پذیری وردپرس

Acunetix نسخه های مختلف از وردپرس را شناسایی می کند و تست های امنیتی را برای بیش از ۱۲۰۰ پلاگین محبوب وردپرس و همچنین چند تست آسیب پذیری دیگر را برای آسیب پذیری های هسته وردپرس انجام می دهد. علاوه بر این، Acunetix سایر تست های پیکربندی خاص وردپرس را نیز انجام خواهد داد: مانند کلمات عبور ضعیف مدیریت وردپرس ،تعیین شماره نام کاربری وردپرس ،فایل های پشتیبان wp-config.php نرم افزار مخرب (بدافزار) پنهان شده به عنوان پلاگین ها و نسخه های قدیمی پلاگین ها.

گزارشگر

ابزارهای پیشرفته تست نفوذ

اسکنر Acunetix شامل ابزارهای پیشرفتهای برای اجرای تست نفوذ (Pen Test) می باشد که امکان اجرای تست های خود کار و یکپارچه سازی با ابزار های خارجی و ابزارهایی که برای کمک در تست رویه های منطقی برنامه های کاربردی تحت وب بکار می رود را فراهم می سازد .مانند:

- ویرایشگر HTTP - ایجاد درخواست های HTTP/HTTPS به منظور تجزیه و تحلیل پاسخ وب سرور.
- HTTP Sniffer - رهگیری، ثبت و اصلاح ترافیک HTTP/HTTPS ارسال شده از برنامه تحت وب.
- HTTP Fuzzer - بررسی دقیق درخواست های HTTP/HTTPS به منظور اعتبار سنجی و کنترل اطلاعات غلط و یا تصادفی.
- انجام استخراج اطلاعات پایگاه داده خودکار با استفاده از آسیب پذیری Blind SQLi.

ویژگی های پیشرفته تر

- تنظیمات انعطاف پذیر اسکن- اسکن وب سایت ها و برنامه های کاربردی وب با تنظیمات مختلف اسکن و توالی های ورود
- سهولت در تعیین محدوده اسکن - به منظور سفارشی سازی محدوده اسکن می توان پروفایل عملیات اسکن و فیلترهای فایل و دایرکتوری را شخصی سازی کرد. (قابل استفاده برای فیلترهای Wildcard و فیلترهای مبتنی بر عبارات منظم)
- زمانبندی اسکن به آسانی - تکرار اسکن مورد نیاز در زمان مناسب به راحتی انجام پذیر است و یا در ساعات مشخصی عملیات اسکن متوقف می گردد.
- وارد کردن داده های به دست امده توسط نرم افزار های اسکن دیگر - نرم افزارهایی مانند: Telerik Fiddler, HAR , Portswigger BurpSuite
- برنامه ریزی پویش خودکار - امکان برنامه ریزی انجام پویش داینامیک با استفاده از ابزار ها یا اسکریپت های خارجی یا شخصی ساز
- تست منطق کسب وکار با Selenium IDE - پشتیبانی از پویش و اسکن برنامه های کاربردی منطق محور پیچیده کسب و کار از طریق موارد آزمون Selenium IDE
- پیکربندی خودکار فایروال های برنامه کاربردی وب

ارائه راهکار Acunetix هم تحت وب و هم نصب بر روی سرور مشتری

اسکنر Acunetix هم به صورت آنلاین و هم بصورت نصب روی دستگاه قابل استفاده است. در نسخه آنلاین می توانید در هر سال به دلخواه خود هر تعداد اسکن مورد نیاز را انجام دهید. در نسخه نصبی که به عنوان نسخه Enterprise است امکان اسکن نامحدود از وب سایت های متعلق به سازمان را فراهم می نمایند. همچنین نسخه مشاور Consultant امکان استفاده از Acunetix جهت انجام تست نفوذ برای اشخاص ثالث را فراهم می آورد. در هر دو نسخه می توانید بطور همزمان تا ۱۰ وب سایت را اسکن کنید.

درباره Acunetix

Acunetix در سال ۲۰۰۴ برای مبارزه با روند رو به رشد ونگران کننده حملات وب تأسیس شد و تا کنون پرچم دار بازار فناوری امنیت برنامه های وب است. محصول شاخص آن، Acunetix Vulnerability Scanner است که با استفاده از روش یک هکر حرفه ای که به دنبال یافتن آسیب پذیری های وب سایت است، تمامی آسیب پذیری ها و حفره های امنیتی وب سایت شما را پیدا کرده و راهکار برطرف کردن مشکل را نیز ارایه می کند.

نظرات مشتریان

"Acunetix WVS نقش بسیار مهمی در شناسایی و کاهش آسیب پذیری های برنامه های تحت وب ایفا کرده است. Acunetix خود را ثابت کرده است و ارزش هزینه کردن دارد."

Mr Rodgers
IT Security Team
U.S. Air Force

"Acunetix نقطه کلیدی در استراتژی امنیت برنامه های ما است، با فرآیند QA یکپارچه می شود، روش مقرون به صرفه برای ما فراهم می کند که برای تشخیص نقص هایی که می توانند در اوایل چرخه توسعه حل شوند کاربرد دارد"

Petro Anduja
ING Direct, Spain

"استفاده از Acunetix WVS به ما اجازه داده تا اسکن خودکار را به طور منظم بر روی Host سایت های تحت کنترل گروه Betfair زمانبندی کنیم، ارائه دید ارزشمندی در ضبط آسیب پذیری ها در اوایل SDLC فراهم می کند."

Jan Ettles
Betfair.com, UK

بعضی از مشتریان Acunetix

آدرس:
تهران - خیابان ولیعصر - نرسیده به سه راه توانیر -
برج طلوع - طبقه ۱ - واحد ۱۰۴

www.ertebateamn.com
www.acunetix.com