# امنیت وب چیست؟

امنیت وب چیست؟ امنیت وب که به عنوان امنیت سایبری نیز شناخته می شود به امنیت وب سایت‌ها و سرورها در برابر خطرات آنلاین مربوط می‌شود. هدف آن حفاظت از داده‌های حساس با محدود کردن، کشف و پاسخ به حملات است. بررسی امنیت وب سایت شامل اسکن آدرس‌های اینترنتی برای آسیب پذیری‌های احتمالی و بدافزارها از طریق نرم افزار امنیتی وب سایت است. یک بررسی امنیت وب، خطرات آنلاین را به کاربر اطلاع می‌دهد و راه حل‌هایی برای رفع آن‌ها توصیه می‌کند. این اولین قدم برای اطمینان از ایمنی، جلوگیری و تشخیص خطرات است. از سوی دیگر، آگاهی از هکرها، هک، کرم‌ها، ویروس‌ها، تروجان‌ها، جاسوس افزارها، اکسپلویت کیت‌ها و غیره نیز به همان اندازه مهم است که می‌تواند به کامپیوترها و شبکه‌های میزبان حمله و آسیب رسانده و آنها را غیرفعال یا مختل کند. تهدیدات ویروس بدافزار بسیار آلوده هستند و به اندازه کافی قادرند اطلاعات شما را خراب کرده و به امنیت شبکه و وب شما آسیب برسانند. ویروس‌های مخرب بی سر و صدا از سیستم شما تجاوز می‌کنند و بسیاری از فعالیت‌های مخرب را انجام می‌دهند که باعث می‌شود وب سایت و شبکه شما پاسخگو نباشد.

### ابزارهای امنیت وب چیست؟

ابزار امنیتی، وب سایت‌ها را در فواصل دوره‌ای اسکن می‌کند تا متوجه شود آیا فعالیت مشکوکی وجود دارد یا خیر. هنگامی که فعالیت مشکوک ردیابی می‌شود، ابزارهای امنیتی وب سایت بلافاصله آن را به اطلاع کارشناسان امنیتی می‌رساند. علاوه بر این، افراد کلیدی در سازمان نیز هشدار دریافت می‌کنند. به سادگی، ابزارهای امنیتی وب سایت در شناسایی و حذف بدافزارهایی که سعی دارند بر وب سایت تجاری تأثیر بگذارند کمک می کند.

### ابزار امنیتی برنامه وب

شبکه جهانی هنوز باید راه طولانی را پیش از تبدیل شدن به یک اکوسیستم کاملاً امن که برای تنظیم و کنترل خود برنامه ریزی شده است، طی کند. تصمیم گیرندگان باید اطمینان حاصل کنند که کلیه سیستم های شرکت خود، از آخرین استانداردهای با امنیت بالا پیروی می کنند. کارمندان همچنین باید در پروتکل های اولیه امنیت سایبری آموزش ببینند. این به ویژه در مورد کارمندان غیر فناوری صادق است. به عنوان مثال، همه باید بدانند چگونه یک ایمیل فیشینگ صورت می پذیرد و چگونه باید از آن جلوگیری کرد.

بدون استراتژی امنیتی صحیح، ممکن است اتفاقات غیر قابل جبرانی رخ دهد. مهاجمان می دانند که چگونه نقاط ضعف را بیابند و از آنها بهره برداری کنند، شکاف‌هایی را باز می‌کنند که باعث می‌شود سیستم‌های قوی از بین بروند. در همین راستا ما یکی از بهترین سرویس‌های مجزا به نام Acunetix به معرفی میکنیم:

## امنیت وب و وب اسکنAcunetix

سرویس مجزا Acunetix محصول شرکت Acunetix در سال ۲۰۰۴ و برای مبارزه با حملات وب تاسیس گردید و در حال حاضر یکی از بزرگان در حوزه تکنولوژی‌های امنیت برنامه‌های تحت وب می‌باشد. محصول شاخص این شرکت Acunetix Vulnerability Scanner طراحی شده تا آسیب پذیری‌های مختلف را در وب سرویس یا وب سایت شما را شناسایی و اطلاعات کاملی را جهت شناخت، بررسی و رفع آن‌ها به شما ارائه می‌کند. این برنامه از تکنولوژی‌های بسیار پیشرفته و منحصر بفردی استفاده می‌کند که به عنوان نمونه می‌توان به موارد زیر اشاره کرد:

- AcuSensor
- AcuMonitor

- Webkit Engine
- و...

## ویژگی‌های اصلی

Acunetixشامل یک موتور Acusensor است که کدها را به محض ورود اسکن می‌کند که این امر باعث ضریب بالای کشف و همچنین کاهش ضریب خطا می‌شود AcuSensor .حتی قادر است که راه‌های نفوذ در کد ها را شناسایی کرده و در Debug گزارش کاملی از این راه‌های نفوذ را ارائه کند AcuSensor .نه تنها راه‌های نفوذ را می‌یابد، بلکه زمان ارزشمند را برای شما ذخیره می‌کند.

حملات لایه اپلکیشین، روی پورت ۴۴۳/۸۰ انجام می‌شوند و با عبور از فایروال، امنیت در سطح شبکه و سیستم عامل مستقیم به قلب برنامه و اطلاعات حساس شرکت می‌رسند. پس شما نیاز به برنامه‌ای دارید که قبل از هکرها شما را از راه‌های نفوذ مطلع کند. با ابزارهای متنوع Acunetix شما به راحتی این امکان را دارید که در عمیق‌ترین سطح راه‌های نفوذ را کشف و رفع نمایید.

**Acunetixشامل ۳ نسخهOnline ، Standard و Enterprise است که نسخه Online به صورت سرویس آنلاین بر روی سرورهای Acunetix است و دو نسخه دیگر قابلیت نصب روی هر سیستمی را خواهند داشت.**

**خرید محصول امنیت وب و وب اسکنAcunetix**

منبع cwatch

لطفا جهت مشاوره در انتخاب آنتی ویروس مناسب خود با این شماره **09224971053** تماس بگیرید.

**مارو در شبکه های اجتماعی خودتان به اشتراک بگذارید.**