امنیت در دنیای وب

تعاریف امنیت

در ایران امروز طیف گسترده‌ای از انواع خدمات بر روی بستر اینترنت در حال خدمات‌دهی هستند. از خرید ساده یک شارژ برای تلفن همراه تا خدمات فروش آنلاین و انجام امور بانکی. امروزه دیگر حتی فرهنگ سفرهای درون شهری در کلان شهرهایی مثل تهران با توجه به گسترش خدمات آنلاین تغییر کرده است. وجود این طیف گسترده از خدمات باعث شده است تا روز به روز اعتماد به خدمات اینترنتی در میان اقشار مختلف جامعه افزایش پیدا کرده و طیف بسیار زیادی از افراد از خدمات متنوع موجود در بستر اینترنت استفاده کنند. در این بین، استفاده از بستر وب برای انجام کارهای روزمره در سازمان‌ها با سرعت بسیار زیادی گسترش یافته است؛ علت این امر هم ایجاد سهولت، همیشه در دسترس بودن، سرعت گرفتن انجام کارها و کاهش بسیار زیاد هزینه‌هاست.

خوشبختانه در حال حاضر، اعتماد خوبی در بین تمامی استفاده‌کنندگان از بستر وب برای دریافت خدمات وجود دارد و شرکت‌ها و سازمان‌ها در بازه 10 سال گذشته در حال انتقال امور به نرم‌افزارهایی هستند که بتوانند با استفاده از آنها امور روزمره خود را انجام دهند.

دنیای وب هم مانند هر دنیای دیگری در کنار مزیت‌هایی که دارد، مجموعه‌ای از تهدیدات را نیز با خود به همراه دارد. وجود هکرهایی که به دنبال اطلاعات سازمان‌ها و یا

شرکت‌ها هستند بزرگترین تهدیدی است که نرم‌افزار های تحت وب با آن روبرو هستند. آن‌ها یا به دنبال اطلاعاتی هستند که در سازمان‌ها وجود دارد و یا برای از بین بردن این اطلاعات تلاش می‌کنند. این افراد واقعا وجود دارند و تقریبا هر روز خبری مبنی بر حمله به یک سایت یا یک شرکت برای سرقت اطلاعات آن منتشر می‌شود؛ اما آیا این به این معنی است که دنیای وب امن نیست؟ پاسخ به این سوال کمی پیچیده است و باید گفت هم بله و هم خیر. پاسخ کوتاه و ساده به سئوال، این است که دنیای وب امن نیست؛ زیرا به صورت واقعی مشاهده می‌کنیم که اطلاعات سرقت می‌شوند و از طرف دیگر، این دنیا امن است چون نمونه‌هایی نیز وجود دارند که تلاش‌های هکرها برای سرقت اطلاعات آن‌ها ناموفق بوده است.

پاسخ بلند این است که بستر وب بر اساس اصول و قواعد مشخصی بنا شده که بخشی از این اصول بر مبنای امنیت ایجاد شده است. شرکت‌های مختلف براساس این اصول و قواعد شروع به تولید نرم افزار می‌کنند و نکته اصلی در رابطه با امن بودن یا نبودن بستر وب بر اساس همین شیوه تولید نرم‌افزار است. در واقع هکرها به دنبال نفوذ با استفاده از اصول وب نیستند؛ بلکه به دنبال نفوذ در نرم‌افزارها با استفاده از اشتباهات تولیدکنندگان آنها هستند. هکرها از اصول وب استفاده می‌کنند و در نرم‌افزارهای مختلف به دنبال بخش‌هایی هستند که اصول امنیتی در آن‌ها وجود ندارد و یا ضعیف است. آنها سعی می‌کنند از طریق این بخش‌ها به اطلاعات ذخیره شده در نرم‌افزار دسترسی پیدا کنند.

بنابراین جدا از مسائل مربوط به مواردی که باید توسط استفاده‌کنندگان رعایت شود در چند مقاله پی‌درپی سعی خواهم کرد مفهوم امنیت و بخش‌های مختلف امنیت را توضیح دهم. سپس شیوه‌های مختلف نگرش به امنیت در نرم‌افزارها در بستر وب توضیح داده

خواهد شد و در هر نگرش استانداردهای موجود در دنیا مورد بررسی قرار خواهد گرفت.

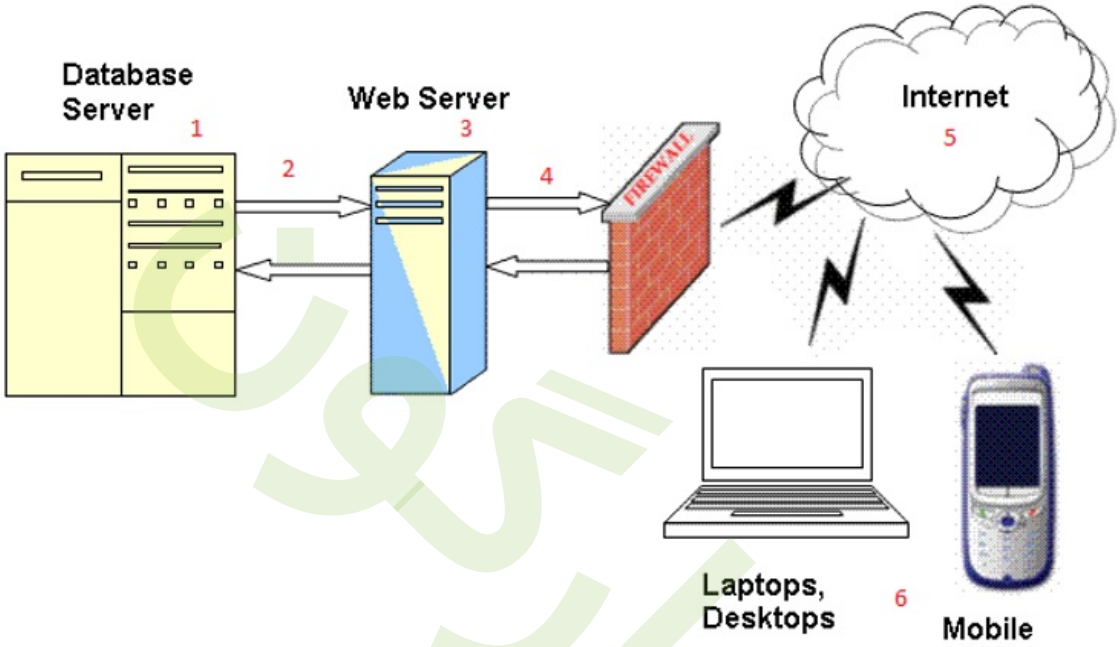
امنیت در بستر وب

برای اینکه به درک مشخصی از امنیت در بستر وب برسیم ابتدا باید تعریفی از امنیت در دنیای وب داشته باشیم و سپس دسته‌بندی کلی تهدیدات موجود برای بخش‌های مختلف بستر وب را ارائه کنیم.

در دنیای آکادمیک علوم کامپیوتر تعریفی مشترک به عنوان امنیت وجود ندارد و دقیقا همانند دنیای واقعی، امنیت از هر منظری تعریف خود را دارد. سعی ما در این مقاله این است که تعریفی جامع و ساده از مفهوم امنیت ارائه کنیم. در دنیای IT مهمترین دارایی، اطلاعات هستند که همه آن‌ها به صورت الکترونیکی تولید، نگهداری و امحاء می‌شوند؛ بنابراین اطلاعات الکترونیکی، نیاز به محافظت دارند. می‌توان گفت در دنیای IT امنیت به معنی جلوگیری از افشا، دسترسی، تولید، تغییر و امحای اطلاعات به صورت غیرمجاز و کشف تلاش‌ها برای دسترسی به اطلاعات است. بستر وب با توجه به اینکه بخشی از دنیای IT است شامل این تعریف می‌شود و نرم افزارهای تولید شده در این بستر باید بتوانند این تعریف را درون خود پیاده‌سازی کنند. این بدین معنی است که باید در بخش های مختلف بستر وب از افشا، دسترسی، تولید، تغییر و امحای اطلاعات به صورت غیرمجاز جلوگیری شود و همچنین بتوان تلاش‌های صورت‌گرفته برای دسترسی غیرمجاز را کشف و گزارش کرد.

به این منظور ابتدا باید در رابطه با تهدیدات مختلف بر روی این بستر صحبت کرد و برای شناسایی تهدیدات نیاز است که بخش‌های مختلف بستر وب در زمان استفاده

کاربران مورد بررسی قرار گیرد. شکل زیر معماری ساده و کلی از شیوه استقرار نرم افزار ها در بستر وب را نمایش می‌دهد:



امنیت وب

شکل 1- معماری ساده‌ای از استقرار نرم‌افزار های تحت وب بر گرفته از سایت **codeproject**

این شکل، نمایش ساده‌ای از معماری استقرار نرم‌افزارهای تحت وب را نمایش می‌دهد و بخش‌های مختلف این بستر را مشخص می‌کند.

1 – سرور پایگاه داده: به صورت ساده، تمامی اطلاعاتی که در نرم‌افزار تولید، ویرایش و در دسترس قرار می‌گیرد در این سرور ذخیره و بازیابی می‌شوند.
2- ارتباط بین سرور وب و سرور پایگاه داده: شبکه‌ای است که درخواست‌های سرور

وب را برای ذخیره یا بازیابی اطلاعات به سرور پایگاه داده، منتقل می‌کند و پاسخ‌های سرور پایگاه داده را نیز به سرور وب انتقال می دهد.

3- سرور وب: مکان استقرار نرم‌افزار بر روی این سرور است. وظیفه این سرور، دادن پاسخ مناسب به هر درخواست دسترسی، ایجاد، ویرایش و یا حذف اطلاعات توسط کاربران است.

4- دیوار آتش: در واقع بر روی بستر وب، محافظت از وب سرور را بر عهده دارد. این دیوار به صورت ساده شبکه بین وب سرور و دیتابیس سرور را از دنیای اینترنت جدا می‌کند و از دسترسی مستقیم از طریق اینترنت به وب سرور و مانع از در اختیار قرار گرفتن آن می‌شود.

5- اینترنت: بستری شبکه‌ای است که وظیفه انتقال اطلاعات و دستورات بین سیستم کاربران و وب سرور را بر عهده دارد.

6- دستگاه کاربران: سیستم‌های شخصی یا موبایل‌ها وظیفه ترجمه اطلاعات و دستورات را از زبان کامپیوتر به اطلاعات قابل درک برای کاربر بر عهده دارند. معمولا کاربران برای انجام این کار در بستر وب از مرورگرهای نصب شده بر روی سیستم استفاده می‌کنند؛ بنابراین به صورت ساده برای نرم‌افزار های وبی، کار اصلی در دستگاه‌های کاربران بر عهده مرورگرهاست.

حال که بخش‌های مختلف این معماری را شناختیم باید این سوال رو بپرسیم که کدام بخش‌ها و به چه صورت ناامن هستند؟ در حقیقت به صورت پیش‌فرض، تمامی بخش‌های بیان شده در بالا ناامن هستند و هکرها سعی می‌کنند از هر یک از این بخش‌ها برای نفوذ به نرم‌افزار ها استفاده کنند. اما چگونه؟

هر یک از این بخش‌ها به خودی خود، قابلیت نفوذ دارد. باید توجه داشت که اطلاعات

به عنوان قلب تپنده استفاده‌کنندگان نرم‌افزار در همه این بخش‌ها وجود دارد؛ بنابراین مهمترین کار هکرها به دست آوردن اطلاعات از یکی از این بخش‌هاست. از این رو شیوه‌های مختلفی از حمله با هدف‌گذاری برای استفاده از هر یک از این بخش‌ها طراحی شده است که در مقاله بعدی در رابطه با هر یک از این شیوه‌ها به تفصیل صحبت خواهد شد. به عنوان مثال هکر ها برای نفود به سرور پایگاه داده سعی می‌کنند از طریق یک کاربر معتبر درخواست‌هایی را برای به دست آوری اطلاعات به سرور دیتابیس ارسال کنند یا با استقرار یک نرم‌افزار در میانه شبکه در بخش‌های 2 و 4 و 5 اطلاعات رد و بدل شده را شنود کنند یا بر روی سرور وب نرم‌افزاری را با استفاده از نرم‌افزار وبی اجرا کرده و با استفاده از آن به اطلاعات سرور پایگاه داده دسترسی پیدا کنند؛ یا حتی از بخش‌های مختلف قواعد مرورگرها بر روی سیستم کاربران استفاده کنند و دستوراتی را از طرف کاربر معتبر به نفع خود به سرور وب ارسال کنند.

با این توضیحات به نظر می‌رسد که نرم‌افزارهای تحت وب اصلا دارای امنیت نیستند؛ اما در حقیقت اینگونه نیست. حقیقت این است که توانایی هکرها برای دستیابی به اطلاعات به 3 موضوع کلی بستگی دارد:

1- حفاظت درست از سرورها بصورت فیزیکی ،از سیستم عامل‌های سرور ها بصورت نرم‌افزاری و از شبکه داخلی بین سرورها بصورت سخت‌افزاری و نرم‌افزاری

2- حفاظت از نرم افزار در مقابل حمله‌های شناخته شده بوسیله کدنویسی صحیح در زمان تولید نرم‌افزار

3- حفاظت کاربران نرم‌افزار از اطلاعات حساس مانند رمز عبور و ...

در رابطه با مورد اول، سیاست‌های مربوط به حفاظت فیزیکی و استفاده از دیواره‌های آتش و نرم افزارهای ضد ویروس می‌تواند از نفوذ هکرها جلوگیری کند. در رابطه با

مورد سوم، آموزش‌های امنیتی به کاربران بسیار راهگشاست و در رابطه با مورد دوم هم در این مجموعه مقالات سعی می‌شود به صورت تفصیلی بیان می‌کنیم که شرکت‌های نرم‌افزاری چگونه می‌توانند امنیت را برای نرم افزارهای تولیدی در بستر وب، برقرار کنند.

امنیت نرم‌افزارها در بستر وب

حقیقت این است که نرم‌افزارهایی که دارای امنیت ضعیف هستند هرچقدر هم کارا باشند غیرقابل استفاده هستند. قطعا هیچ فرد، سازمان یا شرکتی نمی‌تواند از ابزاری غیرمطمئن برای انجام امور خود استفاده کند. با توجه به اینکه برای همه ما اطلاعات، نقشی حیاتی در زندگی ایفا می‌کند باید در هنگام استفاده از ابزارهای مختلف این بررسی را انجام دهیم که آیا استفاده از این ابزار، تهدیدی برای اطلاعات ما ایجاد می‌کند یا خیر؟ از این رو، ابزارهایی که به عنوان نرم‌افزار با هدف تسهیل و تسریع عملیات‌ها به کمک شرکت‌ها و سازمان‌ها می‌آیند باید از این منظر بررسی شوند که آیا تهدیدی برای اطلاعات سازمان یا شرکت هستند یا خیر. برای هر سازمان یا شرکتی این مسئله اهمیت بالایی دارد؛ زیرا وجود یا عدم وجود سازمان و یا شرکت، وابسته به این اطلاعات است.

از این رو، شرکت‌های نرم افزاری باید نرم‌افزارهایی تولید کنند که قابل اعتماد کردن باشند. در کل بر اساس تعریف ارائه شده از امنیت، وظایف شرکت‌های تولیدکننده نرم‌افزار برای ایجاد این اعتماد را به 2 دسته کلی می‌توان تقسیم کرد: «پیشگیری از نفوذ» و «کشف تلاش‌های صورت‌گرفته برای نفوذ».

حدود 10 تا 15 سال پیش در ایران، «کشف تلاش‌های صورت گرفته برای نفوذ» در

شرکت‌های نرم‌افزاری بسیار پر رنگ بود. آنها سعی می‌کردند در هنگام تولید نرم‌افزار قابلیت‌هایی را در اختیار مدیران مشتریان خود قرار دهند تا بتوانند نفوذهای صورت‌گرفته را کشف و اقدامات لازم را برای جلوگیری از ادامه نفوذ، انجام دهند.
مشکل این رویکرد با وجود کشف نفوذ صورت‌گرفته، افشای بیش از حد اطلاعات بود. به مرور زمان، اهمیت افشا نشدن اطلاعات روز به روز افزایش یافت و در حال حاضر برای اکثر سازمان‌ها و شرکت‌ها این فرهنگ واضح و روشن است که پیشگیری بهتر از درمان است. از این رو اکثر شرکت‌ها به استفاده از ابزارهایی روی آورده‌اند که علاوه بر کشف تلاش‌ها برای نفوذ، اصولا از نفوذ پیشگیری کنند. این باعث شده است طی 5 تا 10 سال گذشته شرکت‌های تولید کننده نرم‌افزار، وظیفه پیشگیری را برای خود در اولویت قرار دهند و نرم‌افزارهایی را تولید کنند که پیشگیری از نفوذ در آن، حرف اول را می‌زند.

استانداردسازی نرم‌افزارها

در کنار این رویکردها در دنیا موسساتی ایجاد شده‌اند که به استانداردسازی بحث امنیت در نرم‌افزارهای وبی اقدام کرده‌اند. بعضی از آنها رویکرد پیشگیری را دنبال کرده‌اند و برخی دیگر، رویکرد کشف تلاش‌ها را پی گرفته‌اند. از طرفی، دولت‌ها نیز به این مقوله وارد شده‌اند و از نرم افزارهای امن، تعاریف جدید داده‌اند و بر اساس آنها، گواهینامه‌هایی نیز برای امنیت نرم‌افزارها ارائه می‌کنند.
در حال حاضر برای شرکت‌های تولیدکننده نرم‌افزار ایرانی، شناخته شده‌ترین استانداردهای جهانی در حوزه پیشگیری، استاندارد ASVS است که توسط انجمن

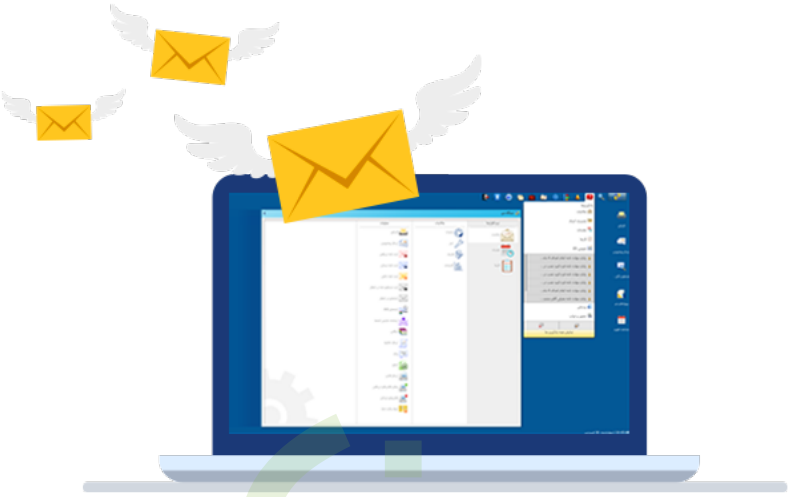
غیرانتفاعی OWASP تولید و منتشر می‌شود و برای بحث رویکرد کشف تلاش برای نفوذ، چارچوبی به نام«معیار مشترک» ایجاد شده است که زیرمجموعه‌ای از استاندارد ISO محسوب می‌شود.

به صورت خلاصه، انجمن OWASP انواع حملات در بستر وب را در 10 دسته‌بندی کلی، تقسیم‌بندی کرده و راههای جلوگیری از این حملات را بیان کرده است و سپس استانداری به نام ASVS ارائه کرده است که طی آن، می‌توان نرم‌افزارها را بر اساس امنیت آن‌ها مورد ارزیابی قرار داد. همچنین چارچوب «معیار مشترک» شرکت‌های نرم‌افزاری را سطح‌بندی کرده است و فرایندی را تدوین کرده است که طی آن شرکت های نرم افزاری می توانند نرم افزار های تولیدی خود را امن نمایند و پس از آن فرایند تولید نرم افزار را نیز امن نمایند. این چارچوب با استفاده از پروفایل‌های حفاظتی مجزا برای هر بستر نرم‌افزاری، الزامات امنیتی معرفی کرده است که بیشتر این الزامات رویکرد مدیریت و کشف نفوذ را دنبال می‌کنند.

در مقاله بعدی به صورت کامل درباره رویکرد پیشگیری با استفاده از تعریف انواع حملات، استاندارد ASVS و وظایف شرکت‌های نرم‌افزاری در این باره، توضیح داده می‌شود. در مقاله سوم نیز در رابطه با چارچوب «معیار مشترک» به تفصیل سخن خواهم گفت.

پایان بخش اول

درخواست دموی نرم‌افزارهای دیدگاه



درخواست دمو
حضوری و آنلاین