نیازمندی‌های امنیتی برنامه‌های تحت وب

تهیه و گردآوری

محمودرضا فردوسی　　آمنه پورسرمست

سرشناسه : فردوسی، محمودرضا، ۱۳۵٤ -
عنوان و نام پدیدآور : نیازمندیهای امنیتی برنامه‌های تحت وب/ محمودرضا فردوسی - آمنه پورسرپرست .
مشخصات نشر : تبریز: ماراویا، ۱۳۹٦ .
مشخصات ظاهری : ۳۸۸ ص.: مصور(رنگی)، جد ول.
شابک : ٤-۲-۹۷۷۳۸-٦۰۰-۹۷۸:۲۳۰۰۰۰ ریا ل
وضعیت فهرست نویسی : فیپا
موضوع : شبکه های کامپیوتری -- تدابیر ایمنی -- برنامه‌های کامپیوتری
موضوع : Computer networks -- Security measures -- Computer progra...
موضوع : وب -- سرورها -- تدابیر ایمنی
موضوع : Web servers -- Secu...t/ me...ures
موضوع : کامپیوترها -- ایمنی اطلاعات
موضوع : Com...ter security
شناسه افزوده : پورسرپرست، آمنه، ۱۳۶۱ -
رده بندی کنگره : ۱۳۹٦ ۹ن٤/...۱۰۵/۸ TK
رده بندی دیویی : ۰۰۵/۸
شماره کتابشناسی ملی : ٤۸٤٤۷۳۱

عنوان کتاب : نیازمندی‌های امنیتی برنامه‌های تحت وب
تألیف : محمودرضا فردوسی - آمنه پورسرپرست
صفحه‌آرا : فرشته زند
نوبت چاپ : اول ۱۳۹۶
شمارگان : ۱۰۰۰ نسخه
انتشارات : ماراویا
قیمت : ۲۳۰۰۰ تومان
چاپ و صحافی : خدمات چاپ و نشر آنلاین
شابک : ۹۷۸-٦۰۰-۹۷۷۳۸-۲-٤

نشانی: تبریز. باغچیان . خیابان نور. جنب فضای سبز. تلفن: ۳۳۸۵۷٦٤۰

دفتر تهران: میدان انقلاب. خیابان ۱۲ فروردین . خ شهدای ژاندارمری .تلفن:٦٦٤۹۳۷۹۰

مقدمه

یک بررسی ساده نشان می‌دهد که زندگی بدون اینترنت یا «رایاتار» در دنیا و حتی در کشورهای درحال‌توسعه به‌سرعت ناممکن می‌گردد و دسترسی به شبکه به‌تدریج علاوه بر آنکه یک الزام برای زندگی فردی تلقی می‌شود، در سطح سازمانی و ملی نیز تعیین کننده و پیش نیاز است به‌طوری‌که در سطح شرکت‌ها هیچ کسب‌وکاری بدون بهره‌گیری از شبکه شکل نمی‌گیرد، و در سطح ملی هیچ اقتصادی برای اداره کشور بدون آن متصور نیست. اضافه بر آن ارتباطات بین‌المللی نیز موکول به بهره‌مندی از آن است.

امروزه مقولات دموکراسی، ارتباطات انسانی، صلح، رشد اقتصادی، بهداشت عمومی، مقابله با فساد، عدالت، محیط‌زیست، توسعه دانش و تکنولوژی، بهره‌وری، حمل‌ونقل بین‌المللی و حتی محلی و داخلی، حقوق شهروندی، رفاه اجتماعی، هنر و حتی تفریح و سرگرمی مردم و افزایش ایمان مذهبی و آرامش نیز به بهره‌برداری بهتر از شبکه اینترنت منوط است.

این وابستگی، مقوله امنیت شبکه را واجد اهمیت فوق‌العاده نموده است به‌طوری‌که امنیت شبکه با امنیت زندگی فردی و اجتماعی و امنیت جهانی پیوند خورده و به سرعت با توسعه سخت‌افزار و نرم‌افزارها پیچیده‌تر می‌شود.

دیگر؛ رقابت‌های فردی و تجاری و رقابت در سطح کشورها به افزارهای سخت و شگردهای سنتی و فیزیکی گذشته نیاز ندارد، بلکه می‌توان از طریق نفوذ و اختلال در شبکه با هزینه‌ای اندک، خسارات فوق‌العاده را ایجاد کرده یا هراس از این اتفاق را به کسب‌وکار پررونقی برای متخصصان مقابله با آن تبدیل نمود.

مخاطرات ممکن است از ناحیه ارزیابی نادرست ریسک‌ها، طراحی برنامه‌ها، مدیریت داده‌ها، آسیب‌های ناشی از معماری، پیاده‌سازی و نگهداری اپلیکیشن‌ها (برنامه‌های کاربردی)، احراز هویت، دسترسی، رمزنگاری و نظایر آن رخ دهد و به فاجعه‌ای فردی، اجتماعی، اقتصادی و ملی و حتی جهانی منجر شود.

ارزش احتمال این مخاطره که اینک از سوی هکرهای (مهاجمین) حرفه‌ای به‌صورت تیمی دنبال می‌شود موجب گردیده به مطالعاتی که در این زمینه توسعه می‌یابد بهای بیشتری داده و تبادل تجربیات در مقوله امنیت، قدر دانسته شود.

مایلم به ویژه بر این نکته تأکید کنم که سلامت، شفافیت و ضرورت فراهم نمودن دسترسی برابر برای اعضای جامعه در مقولات اقتصادی و کارآفرینی به‌طور اعم، و فرصتی که برای مهاجمین در این عرصه به وجود آمده ویژگی خاصی به اهمیت مقوله امنیت داده و ارزش اجتماعی، اقتصادی و حقوقی بی‌بدیلی را برای آن ایجاد نموده است.

همکاران گرامی اینجانب؛ آقای محمودرضا فردوسی و خانم آمنه پورسرپرست که سالهاست به‌طور تخصصی در مقوله امنیت فعالیت دارند با تألیف و انتقال تجربیات ذی‌قیمت خود طی چند کتاب باارزش، همپای توسعه دانش جهانی در این مورد، سعی دارند که گامی در مسیر ارتقاء کیفیت امنیت در کشور بردارند و مسؤولیت علمی و اجتماعی خود را در این زمینه ایفا نمایند که زکاه العلم نشره.

ارزیابی این کتاب از سوی نخبگان حوزه امنیت قطعا به بهبود اثربخشی این امر کمک می‌کند و دانش این حوزه را ارتقاء می‌دهد.

انشا الله این خدمت مأجور باد.

سیدمصطفی رضوی

دانشیار دانشکده مدیریت دانشگاه تهران

و معاون امور حقوقی و مجلس وزارت امور اقتصادی و دارایی

فهرست مطالب

صفحه | شماره صفحه

پیشگفتار

ایمن‌ترین وب سرور جهان وب سروری است که خاموش باشد. وب سرورهای ساده‌ای که دارای تعداد کمی پورت باز و خدمات اندکی بر روی این پورت‌ها هستند، در سطح بعدی ایمنی قرار دارند که این‌ها گزینه‌های مناسبی برای اکثر سازمان‌ها نیستند. برای اجرای سایت‌های پیچیده به برنامه‌های قدرتمند و انعطاف‌پذیری نیاز است و این سایت‌ها طبیعتاً بیشتر در معرض مسائل امنیتی هستند. هر سیستمی با چندین پورت باز و چندین سرویس و چندین زبان برنامه‌نویسی، به این دلیل که نقاط ورود زیادی برای نفوذ دارد، در معرض آسیب است. هر برنامه تحت وب جدید می‌تواند یک حفره امنیتی جدید و متعاقب آن احتمال دسترسی به داده‌های سازمان را به وجود آورد. مهاجمین (هکرها) از طریق جاسوسی پورت‌هایی که ظاهراً پشت فایروال پنهان هستند، به داده‌ها دسترسی پیدا می‌کنند. هیچ راهی برای تضمین اینکه یک برنامه تحت وب ۱۰۰ درصد ایمن باشد وجود ندارد. اگر یک برنامه هیچ‌گاه مورد حمله هکرها قرار نگرفته است، احتمالاً آن‌ها هیچ‌گونه علاقه‌ای به آن برنامه ندارند.

افراد زیادی در دنیا وجود دارند که خود را هکر می‌نامند که مسلماً مهارت‌های آن‌ها به یک اندازه نیست. درواقع تعداد اندکی از هکرها قادر به کشف راهی جدید برای غلبه بر موانع امنیتی وب هستند. با در نظر گرفتن کار انجام‌شده توسط ده‌ها هزار نفر از برنامه‌نویسان سراسر جهان برای بهبود امنیت، کشف روشی جدید برای حمله آسان نخواهد بود. ممکن است صدها و گاهی هزاران نفرساعت صرف به وجود آوردن یک بهره‌برداری از یک آسیب‌پذیری جدید شود. گاهی این کار توسط افراد انجام می‌شود، اما اغلب توسط تیم‌هایی انجام می‌گیرد که مورد حمایت جرائم سازمان‌یافته هستند. در هر دو حالت آن‌ها خواهان این هستند که بازگشت سرمایه خود را از لحاظ زمانی و انرژی به حداکثر برسانند و بنابراین خیلی بی‌سروصدا بر سرمایه‌های سازمانی بسیار ارزشمند متمرکز می‌شوند و تا زمانی که تکنیک جدید آن‌ها کشف شود، ناشناخته خواهد ماند.

در مقابله و تلاش برای از بین بردن هرگونه سودآوری در سرمایه‌گذاری بر روی هک، صدها و شاید هزاران نهاد امنیتی در وب وجود دارد. این گروه‌های خصوصی و عمومی به دنبال اطلاعات مربوط به بهره‌برداری‌های تازه کشف‌شده و به اشتراک‌گذاری آن‌ها هستند، تا بتوان به‌موقع و سریع در مورد آن‌ها هشدار داده و اقدامات دفاعی در مقابل این بهره‌برداری‌های ناشناخته را سریعاً به مرحله عمل آورد. اعلام کشف یک بهره‌برداری جدید، آن را تبدیل به یک بهره‌برداری شناخته شده می‌کند.

برنامه‌های تحت وب سازمانی باید در یک محیط ایمن اجرا شوند. تنها این حقیقت که برنامه در پشت فایروال‌ها و تجهیزات امنیتی اجرا می‌شود، ایمنی آن را تضمین نمی‌کند. اگر حداقل یک پورت به دنیای خارج باز شود، کدهای مخرب می‌توانند پنهانی از آن به درون برنامه نفوذ کنند. و یک «کارمند ناراضی» یا صرفاً یک «برنامه‌نویس کنجکاو» در درون سازمان می‌تواند کدی ناخواسته را به آن تزریق کند. برنامه‌های تحت وب همواره مستعد ریسک‌ها و آسیب‌های امنیتی هستند و بنابراین هر شبکه‌ای که وب سرورها به آن متصل هستند نیز شامل این ریسک‌ها و آسیب‌ها می‌شود. با در نظر نگرفتن ریسک‌های ایجاد شده توسط کارمندان، کاربران و مهاجمین که از منابع شبکه‌ای سوءاستفاده می‌کنند، وب سرور و برنامه‌ای که آن

سرور میزبانی آن را انجام می‌دهد، مهم‌ترین منابع ریسک‌های امنیتی سازمان خواهند بود. وب سرورها بر اساس طراحی خود، پنجره‌ای بین شبکه سازمان و جهان باز می‌کنند. سیاست‌های اعمال شده از طریق نگهداری سرور، به‌روزرسانی برنامه تحت وب و کد نویسی وب‌سایت، ابعاد آن پنجره را تعریف خواهند کرد، اطلاعاتی که می‌تواند از طریق آن عبور کند را محدود خواهد کرد و بنابراین سطح امنیت برنامه را تعیین خواهد نمود.

کتاب‌ها و مقالات و استانداردهای بسیاری وجود دارند که مبحث امنیت را پوشش می‌دهند، و سازمان‌ها معمولاً تیم‌هایی را به مدیریت امنیت فناوری اطلاعات سازمان اختصاص می‌دهند که کنار آمدن با تهدیدهای امنیتی، وظیفه اصلی آن‌هاست. این کتاب حاوی مطالب الهام بخشی برای متخصصین امنیتی به‌ویژه در حوزه برنامه‌های کاربردی تحت وب است و توسعه دهندگان نرم‌افزاری می‌توانند اطلاعات مفیدی را در این کتاب پیدا کنند.

اگر یک توسعه دهنده نرم‌افزار نیاز به دسترسی به یک برنامه داخلی داشته باشد، باز کردن این مسئله برای تیم پشتیبانی فنی می‌تواند امتیازات دسترسی مورد نیاز را برایش فراهم کند. اما توسعه دهندگان نرم‌افزاری باید حداقل در سطح وسیعی از آنچه که یک برنامه تحت وب را ایمن‌تر یا غیر ایمن‌تر می‌سازد، و اینکه برنامه‌های تحت وب با چه تهدیدهایی روبرو می‌شوند داشته باشند؛ این مبحث، موضوع اصلی این کتاب است. برای پیاده‌سازی هر یک از مکانیزم های امنیتی اشاره شده در این کتاب، لازم است که بررسی و تحلیل‌های دقیقی در مراحل مختلف توسعه یک برنامه کاربردی (چرخه حیات برنامه) انجام شود. همچنین با توجه به رشد بسیار زیاد شبکه‌های ارتباطی و اجتماعی و متعاقب آن برنامه‌های تعاملی تحت شبکه، این کتاب بر روی برنامه‌های کاربردی تحت وب متمرکز گردیده ولیکن بسیاری از مباحث مطرح شده قابل استفاده در تمامی معماری‌های ترم افزاری و برنامه‌نویسی (کد نویسی) می‌باشد.

در این کتاب سعی شده با استفاده از سیاست‌ها و استانداردهای مطرح شده در برخی از سازمان‌های بزرگ حوزه فناوری اطلاعات و با تمرکز بر استانداردهای شرکت مایکروسافت (Microsoft) و سازمان OWASP ، اقدامات امنیتی مورد نیاز برنامه‌های کاربردی تحت وب

در تمامی مراحل معماری و طراحی، برنامه‌نویسی، پیاده‌سازی و اجرا و توسعه و نگهداری معرفی و مورد بررسی قرار گیرند.

آنچه که در این کتاب خواهیم آموخت:

- درک اهمیت طراحی و پیاده‌سازی برنامه‌های ایمن‌تر و تفکر در مورد امنیت و به کارگیری آن در سراسر چرخه حیات برنامه.
- درک اهمیت مسائل مربوط به امنیت برنامه‌های تحت وب و ریسک‌های احتمالی مربوط به این مسائل.
- عواقب عدم مدیریت مناسب داده‌های نامطمئن، مانند از دسترس خارج شدن سرویس، برنامه‌نویسی نالایق در سایت و غیره.
- درک و استفاده از بهترین اقدامات مربوط به ایمنی برنامه‌ها.
- آسیب‌پذیری‌های معماری، طراحی، پیاده‌سازی و نگهداری برنامه‌ها.
- آسیب‌پذیری‌های مربوط به اعتبارسنجی ورودی، احراز هویت، اعطاء مجوز دسترسی، مدیریت پیکربندی، داده‌های حساس، مدیریت جلسه، رمزنگاری، دست‌کاری پارامتر و مدیریت خطا.

- تکنیک‌ها و استانداردهایی که می‌توان برای ایمنی برنامه‌های وب، سرورهای میزبان و سایر مؤلفه‌های مرتبط با آن‌ها مورد استفاده قرار داد.
- شناسایی نیازمندی‌های امنیتی برنامه و تدوین پیوست امنیتی.
- تهدیدهای برنامه و مقابله با آن‌ها.
- معماری، طراحی و برنامه‌نویسی امن برنامه.
- نیازمندی‌های تائیدیه های استاندارد OWASP.

اگر سازمان شما دارای سرمایه‌های مهم اطلاعاتی است و تعامل با آن‌ها از طریق شبکه‌های رایانه‌ای و برنامه‌های کاربردی تحت وب، امنیت اطلاعات و سازمان را در معرض مخاطره قرار می‌دهد و چالشی بزرگ برای سازمان می‌باشد، امیدواریم که مطالب ارائه شده در این کتاب، موجب بهبود سطح امنیت برنامه‌ها در سازمان شده و از بسیاری از خطرات ناشی از آسیب‌پذیری‌های موجود در برنامه‌ها جلوگیری به عمل آورد.