

نیازمند سراسر منیتی برنامه‌هاست تحت وب

تهیه و گردآوری

آمنه پور سمیرا

محمود رضا فردوسی

سرشناسه : فردوسی، محمودرضا، ۱۳۵۴ -  
 عنوان و نام پدیدآور : نیازمندیهای امنیتی برنامه‌های تحت وب / محمودرضا فردوسی - آمنة پورسرپرست .  
 مشخصات نشر : تبریز: ماراویا، ۱۳۹۶ .  
 مشخصات ظاهری : ۲۸۸ ص.: مصور(رنگی)، جدول .  
 شابک : ۹۷۷۳۸-۶۰۰-۹۷۸-۲۳۰۰۰۰ : ۲۳۰۰۰۰ ریال  
 وضعیت فهرست نویسی : فیبا  
 موضوع : شبکه های کامپیوتری -- تدابیر ایمنی -- برنامه های کامپیوتری  
 موضوع : Computer networks -- Security measures -- Computer program .  
 موضوع : وب -- شبکه ها -- تدابیر ایمنی  
 موضوع : Web servers -- Security measures .  
 موضوع : کامپیو ها -- امنیتی اطلاعات  
 موضوع : Computer security .  
 شناسه افزوده : پورسرپرست، آمنه ۱۳۵۴ -  
 رده بندی کنگره : ۱۳۹۶ ن ۹۷۷۳۸/۶۰۰/۲۳۰۰۰۰  
 رده بندی دیویی : ۰۰۵/۸  
 شماره کتابشناسی ملی : ۴۸۴۴۷۳۱



عنوان کتاب : نیازمندیهای امنیتی برنامه‌های تحت وب  
 تألیف : محمودرضا فردوسی - آمنة 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 : ۹۷۸-۶۰۰-۹۷۷۳۸-۲-۴

نشانی: تبریز، یاغچیان، خیابان نور، جنب فضای سبز. تلفن: ۳۳۸۵۷۶۴۰

دفتر تهران: میدان انقلاب، خیابان ۱۲ فروردین، خ شهدای ژاندارمری. تلفن: ۶۶۴۹۳۷۹۰

## مقدمه

یک بررسی ساده نشان می‌دهد که زندگی بدون اینترنت یا «رایاتار» در دنیا و حتی در کشورهای در حال توسعه به سرعت ناممکن می‌گردد و دسترسی به شبکه به تدریج علاوه بر آنکه یک الزام برای زندگی فردی و انسانی تلقی می‌شود، در سطح سازمانی و ملی نیز تعیین کننده و پیش نیاز است به طوری که در سطح شرکت‌ها هیچ کسب و کاری بدون بهره‌گیری از شبکه شکل نمی‌گیرد، و در سطح ملی هیچ اقدامی 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، محیط زیست، توسعه دانش و تکنولوژی، بهره‌وری، حمل و نقل 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 کرده است به طوری که امنیت شبکه با امنیت زندگی فردی و اجتماعی و امنیت جهانی پیوند خورده و به رعایت 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 کسب و کار 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 به صورت 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.

ما اینم به ویژه بر این نکته تأکید کنم که سلامت، شفافیت و ضرورت فراهم نمودن دسترسی برابر برای افراد جامعه در مقولات اقتصادی و کارآفرینی به طور 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 بی‌شمار را برای آن ایجاد نموده است.

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

ارزیابی این کتاب از سوی نخبگان حوزه امنیت، منجر 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.....                              | ۱۹         |
| فصل اول - شبکه گسترده جهانی و ب.....       | ۲۵         |
| وب چیست ؟ .....                            | ۲۶         |
| برنامه‌های وب چه هستند؟ .....              | ۲۹         |
| برنامه‌های وب چگونه کار می‌کنند؟ .....     | ۳۱         |
| سرویس‌های وب چه هستند؟ .....               | ۳۳         |
| ریسک‌ها، تهدیدها، آسیب‌پذیری و حمله .....  | ۳۵         |
| ارزیابی ریسک .....                         | ۳۶         |
| مشکلات امنیتی وب .....                     | ۳۷         |
| به چه میزان امنیت نیاز است؟ .....          | ۴۰         |
| امنیت برنامه‌های وب .....                  | ۴۱         |
| ما یک فایروال داریم پس ما ایمن هستیم ..... | ۴۲         |
| امنیت چیست؟ .....                          | ۴۳         |
| اصول امنیتی برنامه‌ها .....                | ۴۵         |
| اعتبار سنجی ورودی و خروجی .....            | ۴۶         |
| احراز هویت .....                           | ۴۶         |
| رمزنگاری اطلاعات .....                     | ۴۹         |
| پشتیبانی از امضاء دیجیتال .....            | ۵۰         |

|                                                                      |           |
|----------------------------------------------------------------------|-----------|
| مدیریت ثبت فعالیت‌ها.....                                            | ۵۱        |
| شکست ایمن (بسته).....                                                | ۵۳        |
| سادگی.....                                                           | ۵۴        |
| استفاده دوباره از اجزای امن.....                                     | ۵۴        |
| دفاع در عمق.....                                                     | ۵۴        |
| امنیت وابسته به ضعیف‌ترین نقاط است.....                              | ۵۵        |
| پنهان‌سازی در امنیت، در طولانی مدت خطرناک است.....                   | ۵۵        |
| حدائل حق دسترسی.....                                                 | ۵۵        |
| بخش‌بندی (محرر سازی).....                                            | ۵۶        |
| تعریف راهبرد تست و تست برنامه.....                                   | ۵۶        |
| چگونه یک برنامه وب را امن سازی کنیم؟.....                            | ۶۱        |
| شبکه امن، میزبان و برنامه.....                                       | ۶۱        |
| تأمین امنیت شبکه.....                                                | ۶۳        |
| تأمین امنیت میزبان.....                                              | ۶۴        |
| دسته‌بندی پیکربندی میزبان.....                                       | ۶۴        |
| تأمین امنیت نرم‌افزار.....                                           | ۶۸        |
| دسته‌بندی آسیب‌پذیری برنامه.....                                     | ۶۸        |
| خلاصه.....                                                           | ۷۱        |
| <b>فصل دوم- نیازمندی‌های امنیتی برنامه‌ها.....</b>                   | <b>۷۳</b> |
| نیازمندی‌های امنیتی برنامه‌ها.....                                   | ۷۴        |
| نیازمندی‌های امنیتی چه هستند؟.....                                   | ۷۵        |
| گام اول: اهداف خود را برای اتخاذ نیازمندی‌های امنیتی تعریف کنید..... | ۷۷        |

|                                                                                 |     |
|---------------------------------------------------------------------------------|-----|
| گام دوم (الف): برای نیازمندی‌هایی که قابلیت استفاده مجدد دارند مخزن ایجاد کنید. | ۷۸  |
| گام دوم (ب): مشخص کردن منبع برای نیازمندی‌ها.                                   | ۸۰  |
| گام سوم: افزودن نیازمندی‌ها به مخزن.                                            | ۸۰  |
| گام چهارم: ساخت فهرستی از ویژگی‌های برنامه.                                     | ۸۱  |
| گام پنجم: تعریف الزامات مورد نیاز تیم‌های توسعه.                                | ۸۲  |
| سند نیازمندی‌های امنیتی برنامه در پروژه‌ها.                                     | ۸۲  |
| الف (هدف)                                                                       | ۸۲  |
| ب (استانداردهای قانونی و تیر)                                                   | ۸۳  |
| ج (محدوده نیازمندی)                                                             | ۸۳  |
| د (نیازمندی‌های امنیتی برنامه)                                                  | ۸۴  |
| د - ۲ (نظارت‌های فنی و عملیاتی)                                                 | ۹۰  |
| د - ۳ (راه‌حل‌های معماری)                                                       | ۹۳  |
| د - ۴ (مستندسازی راه‌حل)                                                        | ۱۰۳ |
| خلاصه                                                                           | ۱۰۵ |
| فصل سوم - پیوست امنیتی برنامه                                                   | ۱۰۷ |
| پیوست امنیتی برنامه                                                             | ۱۰۸ |
| پیوست امنیتی قرارداد                                                            | ۱۱۰ |
| فرم پیوست امنیتی سامانه‌های اطلاعاتی                                            | ۱۲۳ |
| فصل چهارم - تهدیدهای برنامه و اقدامات متقابل                                    | ۱۳۱ |
| تهدیدها و اقدامات متقابل                                                        | ۱۳۲ |
| بررسی و ارزیابی                                                                 | ۱۳۳ |
| بهره‌برداری و نفوذ                                                              | ۱۳۴ |

|          |                                     |
|----------|-------------------------------------|
| ۱۳۴..... | افزایش سطح دسترسی                   |
| ۱۳۵..... | حفظ دسترسی                          |
| ۱۳۵..... | عدم ارائه سرویس                     |
| ۱۳۵..... | درک طبقه‌بندی تهدیدها               |
| ۱۳۶..... | STRIDE                              |
| ۱۳۸..... | تهدیدهای STRIDE و اقدامات متقابل    |
| ۱۴۰..... | تهدیدها، شبکه و اقدامات متقابل      |
| ۱۴۰..... | جمع‌آوری اسنادات                    |
| ۱۴۱..... | جاسوسی                              |
| ۱۴۲..... | جعل                                 |
| ۱۴۲..... | سرقت جلسه                           |
| ۱۴۳..... | عدم ارائه سرویس                     |
| ۱۴۴..... | تهدیدهای میزبانی و اقدامات متقابل   |
| ۱۴۵..... | ویروس‌ها، اسب‌های تروجان و کرم‌ها   |
| ۱۴۶..... | ردیابی                              |
| ۱۴۷..... | هک کردن پسورد                       |
| ۱۴۸..... | عدم ارائه سرویس                     |
| ۱۴۹..... | اجرای کد دلخواه                     |
| ۱۴۹..... | دسترسی غیرمجاز                      |
| ۱۵۰..... | تهدیدهای برنامه‌ای و اقدامات متقابل |
| ۱۵۱..... | اعتبارسنجی ورودی                    |
| ۱۵۲..... | سرریز بافر                          |

- ۱۵۴..... تزریق کد
- ۱۵۵..... تزریق SQL
- ۱۵۶..... متعارف سازی
- ۱۵۶..... احراز هویت
- ۱۵۷..... شنود شبکه
- ۱۵۸..... تهاجم‌های بوجرمانه
- ۱۵۸..... تهاجم‌های دیک شری
- ۱۵۹..... تهاجم‌های دست‌کارت
- ۱۶۰..... سرقت اعتبارنامه
- ۱۶۱..... مجوز دسترسی
- ۱۶۱..... افزایش سطح دسترسی
- ۱۶۲..... افشای داده‌های محرمانه
- ۱۶۲..... دست‌کاری داده
- ۱۶۳..... تهاجم‌های فریبکارانه
- ۱۶۳..... مدیریت پیکربندی
- ۱۶۴..... دسترسی غیرمجاز به رابط‌های مدیریتی
- ۱۶۵..... دسترسی غیرمجاز به مخازن پیکربندی
- ۱۶۵..... بازیابی موارد محرمانه پیکربندی متن
- ۱۶۶..... عدم پاسخگویی فردی
- ۱۶۶..... حساب‌های سرویس و برنامه با امتیازات (دسترسی) بیش‌ازحد
- ۱۶۷..... داده‌های حساس
- ۱۶۷..... دسترسی به داده‌های حساس در مخزن

|          |                                                              |
|----------|--------------------------------------------------------------|
| ۱۶۸..... | شنود شبکه.....                                               |
| ۱۶۸..... | دست کاری داده.....                                           |
| ۱۶۹..... | مدیریت جلسه (نشست).....                                      |
| ۱۶۹..... | سرقت جلسه.....                                               |
| ۱۷۰..... | تکرار جلسه.....                                              |
| ۱۷۱..... | تهاجم های واسط انسانی.....                                   |
| ۱۷۲..... | رمزنگاری.....                                                |
| ۱۷۲..... | تولید با مدیریت ضعف کلید.....                                |
| ۱۷۳..... | رمزگذاری ضعف با سوم.....                                     |
| ۱۷۴..... | جمل checksum.....                                            |
| ۱۷۴..... | دست کاری پارامتر.....                                        |
| ۱۷۵..... | دست کاری رشته Query.....                                     |
| ۱۷۶..... | دست کاری فیلد فرم.....                                       |
| ۱۷۶..... | دست کاری کوکی.....                                           |
| ۱۷۷..... | دست کاری سرآیند HTTP.....                                    |
| ۱۷۷..... | مدیریت خطا.....                                              |
| ۱۷۸..... | مهاجم، جزئیات پیاده سازی را برملا می سازد.....               |
| ۱۷۸..... | عدم ارائه سرویس.....                                         |
| ۱۷۹..... | بازرسی و ثبت.....                                            |
| ۱۷۹..... | انکار کاربر در اجرای یک عملیات.....                          |
| ۱۸۰..... | بررسی یک برنامه توسط مهاجمان، بدون گذاشتن ردپایی از خود..... |
| ۱۸۰..... | پنهان سازی ردپای مهاجمان توسط آن ها.....                     |

|                                                              |     |
|--------------------------------------------------------------|-----|
| خلاصه.....                                                   | ۱۸۱ |
| فصل پنجم - طراحی امن برنامه‌های وب.....                      | ۱۸۳ |
| معماری و مسائل مربوط به طراحی امن برنامه‌های وب.....         | ۱۸۴ |
| اعتبار سنجی ورودی.....                                       | ۱۸۷ |
| فرض اینکه تمام ورودی‌ها مخرب هستند.....                      | ۱۸۸ |
| انتخاب یک رویکرد متمرکز.....                                 | ۱۸۹ |
| عدم اتکا بر اعتبار سنجی سمت سرویس‌گیرنده (کاربر).....        | ۱۸۹ |
| در نظر گرفتن مسائل متفاوت سازی.....                          | ۱۹۰ |
| محدود، رد، و پاک‌سازی ورودی‌ها.....                          | ۱۹۰ |
| مثال‌های اجرایی.....                                         | ۱۹۳ |
| احراز هویت.....                                              | ۱۹۴ |
| جداسازی مناطق عمومی و محدود.....                             | ۱۹۶ |
| استفاده از سیاست‌های قفل حساب برای حساب‌های کاربر نهایی..... | ۱۹۷ |
| پشتیبانی از دوره‌های انقضای رمز عبور.....                    | ۱۹۷ |
| داشتن قابلیت غیرفعال کردن حساب‌ها.....                       | ۱۹۷ |
| ذخیره نکردن کلمات عبور در اطلاعات کاربر.....                 | ۱۹۷ |
| نیاز به کلمات عبور قوی.....                                  | ۱۹۸ |
| ارسال نکردن کلمات عبور در شبکه به صورت متن شفاف.....         | ۱۹۸ |
| محافظت از کوکی‌های احراز هویت.....                           | ۱۹۸ |
| مجوز دسترسی (اختیارات).....                                  | ۱۹۸ |
| استفاده از دروازه‌های کنترلی متعدد.....                      | ۱۹۹ |
| محدود کردن دسترسی کاربر به منابع در سطح سیستم.....           | ۱۹۹ |

|          |                                                                                            |
|----------|--------------------------------------------------------------------------------------------|
| ۲۰۰..... | اعطاء مجوز به صورت دانه دانه .....                                                         |
| ۲۰۱..... | مدیریت پیکربندی.....                                                                       |
| ۲۰۲..... | ایمن سازی رابط های مدیریت برنامه.....                                                      |
| ۲۰۲..... | ایمن سازی محل ذخیره پیکربندی برنامه.....                                                   |
| ۲۰۳..... | اعطاء امتیازات مدیریتی به صورت جداگانه.....                                                |
| ۲۰۳..... | استفاده از حساب های فرایند و سرویس با حداقل امتیاز.....                                    |
| ۲۰۳..... | داده های حساس.....                                                                         |
| ۲۰۴..... | داده های حساس (مجموعه).....                                                                |
| ۲۰۴..... | تا حد امکان داده های حساس ذخیره سازی نشوند.....                                            |
| ۲۰۵..... | ذخیره نکردن داده های حساس در کد برنامه.....                                                |
| ۲۰۵..... | نگهداری نکردن رشته های اتصال به پایگاه داده، کلمات عبور، و یا کلیدها به صورت متن شفاف..... |
| ۲۰۵..... | استفاده از DPAPI برای رمزنگاری داده های حساس.....                                          |
| ۲۰۶..... | داده های حساس کاربر.....                                                                   |
| ۲۰۷..... | عدم استفاده از پروتکل HTTP- GET برای انتقال داده حساس.....                                 |
| ۲۰۷..... | مدیریت جلسه.....                                                                           |
| ۲۰۸..... | استفاده از SSL برای محافظت از کوکی های احراز هویت.....                                     |
| ۲۰۸..... | رمزنگاری محتویات کوکی های احراز هویت.....                                                  |
| ۲۰۸..... | محدود سازی طول عمر جلسه.....                                                               |
| ۲۰۸..... | محافظت وضعیت جلسه از دسترسی غیرمجاز.....                                                   |
| ۲۰۹..... | رمزنگاری.....                                                                              |
| ۲۱۰..... | استفاده از پروتکل های رمزنگاری استاندارد.....                                              |

- ۲۱۰..... رمزنگاری و رمزگشایی به‌موقع داده‌ها
- ۲۱۰..... استفاده از الگوریتم درست و اندازه کلید صحیح
- ۲۱۱..... ایمن‌سازی کلیدهای رمزنگاری
- ۲۱۱..... دست‌کاری پارامتر
- ۲۱۲..... رمزگذاری حالت کوکی حساس
- ۲۱۲..... اطمینان از اینکه کاربران کنترل‌های برنامه را دور نمی‌زنند
- ۲۱۲..... اعتبارسنجی تمام مقادیر ارسال شده از سرویس‌گیرنده (کاربر)
- ۲۱۲..... عدم اعتماد به الملاء اسراند HTTP
- ۲۱۳..... مدیریت خطا
- ۲۱۳..... جلوگیری از نشت اطلاعات به کاربر
- ۲۱۴..... ثبت دقیق جزئیات خطاها
- ۲۱۴..... درک و تحلیل خطاهای به وجود آمده
- ۲۱۴..... حسابرسی و ثبت وقایع
- ۲۱۵..... حسابرسی و ثبت دسترسی‌ها در تمام لایه‌های برنامه
- ۲۱۵..... جریان اطلاعات هویت شناسایی شود
- ۲۱۵..... ثبت وقایع کلیدی
- ۲۱۵..... ایمن‌سازی فایل‌های ثبت وقایع
- ۲۱۶..... پشتیبان‌گیری و تجزیه و تحلیل فایل‌های ثبت وقایع به‌طور منظم
- ۲۱۶..... خلاصه
- ۲۲۱..... فصل ششم - بازبینی معماری و طراحی برنامه برای امنیت
- ۲۲۲..... بازبینی معماری و طراحی برنامه برای امنیت
- ۲۲۳..... ملاحظات استقرار (توسعه) و زیرساخت

|          |                                                                                        |
|----------|----------------------------------------------------------------------------------------|
| ۲۲۴..... | آیا شبکه ارتباط امن را فراهم می کند؟                                                   |
| ۲۲۴..... | آیا توپولوژی انتخاب شده برای نحوه استقرار برنامه شامل فایروال درونی می شود؟            |
| ۲۲۴..... | آیا توپولوژی انتخاب شده برای نحوه استقرار برنامه شامل سرور راه دور برای برنامه می شود؟ |
| ۲۲۵..... | سیاست های امنیتی زیرساخت چه محدودیت هایی را تحمیل می کند؟                              |
| ۲۲۷..... | آیا مشکلات Web Farm را بررسی شده اند؟                                                  |
| ۲۲۷..... | محیط یوزبان چه سطوح امنیتی را پشتیبانی می کند؟                                         |
| ۲۲۹..... | اعتبارسنجی برای ورودی.....                                                             |
| ۲۳۱..... | اعتبار ورودی چگونه سنجیده می شود؟                                                      |
| ۲۳۳..... | ورودی چه کاری انجام می دهد؟                                                            |
| ۲۳۵..... | احراز هویت.....                                                                        |
| ۲۴۱..... | مجوز دسترسی (اختیارات).....                                                            |
| ۲۴۵..... | مدیریت پیکربندی.....                                                                   |
| ۲۴۹..... | داده حساس.....                                                                         |
| ۲۵۲..... | مدیریت جلسه (نشست).....                                                                |
| ۲۵۵..... | رمزنگاری.....                                                                          |
| ۲۵۸..... | دست کاری پارامتر.....                                                                  |
| ۲۶۱..... | مدیریت خطا.....                                                                        |
| ۲۶۳..... | ثبت وقایع و حسابرسی.....                                                               |
| ۲۶۵..... | خلاصه.....                                                                             |
| ۲۶۷..... | فصل هفتم - اقدامات برنامه نویسی ایمن OWASP.....                                        |
| ۲۶۸..... | اقدامات برنامه نویسی ایمن OWASP.....                                                   |

|          |                                      |
|----------|--------------------------------------|
| ۲۷۰..... | بازبینی قواعد ریسک و امنیت نرم‌افزار |
| ۲۷۲..... | اعتبارسنجی ورودی                     |
| ۲۷۵..... | رمزنگاری خروجی                       |
| ۲۷۵..... | احراز هویت و مدیریت رمز عبور         |
| ۲۸۰..... | مدیریت جلسه                          |
| ۲۸۲..... | کنترل دسترسی                         |
| ۲۸۵..... | اقدامات رمزنگاری                     |
| ۲۸۶..... | مدیریت خطا و ورز به سیستم            |
| ۲۸۸..... | محافظت از داده                       |
| ۲۸۹..... | امنیت ارتباطات                       |
| ۲۹۰..... | پیکربندی سیستم                       |
| ۲۹۲..... | امنیت پایگاه داده                    |
| ۲۹۴..... | مدیریت فایل                          |
| ۲۹۵..... | مدیریت حافظه                         |
| ۲۹۶..... | اقدامات برنامه‌نویسی عمومی           |
| ۲۹۸..... | خلاصه                                |

|          |                                                    |
|----------|----------------------------------------------------|
| ۳۰۱..... | فصل هشتم - استاندارد OWASP برای تأیید امنیت برنامه |
| ۳۰۲..... | استاندارد OWASP برای تأیید امنیت برنامه            |
| ۳۰۳..... | سطوح تأیید امنیت برنامه                            |
| ۳۰۸..... | معماری، طراحی و مدل‌سازی تهدید                     |
| ۳۱۱..... | نیازمندی‌های تأیید احراز هویت                      |

|          |                                                  |
|----------|--------------------------------------------------|
| ۳۱۵..... | نیازمندی‌های تأیید مدیریت جلسه.....              |
| ۳۱۸..... | نیازمندی‌های تأیید کنترل دسترسی.....             |
| ۳۲۰..... | نیازمندی‌های تأیید بررسی ورودی مخرب.....         |
| ۳۲۴..... | نیازمندی‌های تأیید رمزنگاری.....                 |
| ۳۲۶..... | نیازمندی‌های تأیید رفع خطا و ثبت وقایع.....      |
| ۳۲۸..... | نیازمندی‌های تأیید حفاظت از داده‌ها.....         |
| ۳۳۱..... | نیازمندی‌های تأیید امنیت ارتباطات.....           |
| ۳۳۳..... | نیازمندی‌های تأیید پیکربندی امنیتی HTTP.....     |
| ۳۳۵..... | نیازمندی‌های تأیید کنترل‌های مخرب.....           |
| ۳۳۶..... | نیازمندی‌های تأیید کنترل‌های سوءکار.....         |
| ۳۳۷..... | نیازمندی‌های تأیید فایل‌ها و منابع.....          |
| ۳۴۰..... | نیازمندی‌های تأیید کاربردهای همراه.....          |
| ۳۴۳..... | نیازمندی‌های تأیید خدمات وب.....                 |
| ۳۴۵..... | نیازمندی‌های تأیید پیکربندی.....                 |
| ۳۴۷..... | نیازمندی‌های تأیید اینترنت اشیاء.....            |
| ۳۵۱..... | خلاصه.....                                       |
| ۳۵۳..... | در پایان.....                                    |
| ۳۵۷..... | پیوست یک - استاندارد OWASP.....                  |
| ۳۶۷..... | پیوست دو - انواع حملات به برنامه‌های تحت وب..... |
| ۳۸۷..... | منابع و مآخذ.....                                |

# 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. این سایت‌ها طبیعتاً بیشتر در معرض مسائل امنیتی هستند. هر سیستمی با چندین پورت باز 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 امنیتی 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 نفر ساعت 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 خواهند ماند.

در مقابله و تلاش برای از بین بردن هرگونه سودآوری در سرمایه‌گذاری بر روی هک، صدها و شاید هزاران نهاد امنیتی، 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. اعدام گسترده 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 بهانه‌ای 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 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 ساده‌سازی هر یک از مکانیزم‌های 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 نرم‌افزاری 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، برده‌نویسی، آلودگی 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 تأییدیه‌های 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.