



انتشارات احمیل روز

امنیت در تجارت الکترونیکی

E-Business security

سارنگ قربانیان

سید مهدی عمادی استر آبادی

مجید رضا اخوان

یوسف عطاری

www.ketab.ir



سرشناسه:	سازنگ قربانیان، ۱۳۵۳
عنوان و نام پدیدآور:	امنیت در تجارت الکترونیکی (E-Business security) / سازنگ قربانیان... [و دیگران]
مشخصات نشر:	تهران: ادیبان روز، ۱۳۹۴
مشخصات ظاهری:	۴۳۲ ص: مصور
شابک:	۹۷۸-۶۰۰-۹۵۲۸۱-۴-۱
وضعیت فهرست نویسی:	فیا
یادداشت:	نویسندگان سازنگ قربانیان، سید مهدی عمادی استرآبادی، مجیدرضا اخوان، یوسف عطاری
یادداشت:	کتابنامه: ص. ۴۳۱ - ۴۳۲
موضوع:	بازرگانی الکترونیکی
موضوع:	بازرگانی الکترونیکی - تدابیر ایمنی
رده بندی کنگه:	۱۳۹۴ الف/۳۲/HF۵۵۴۸
رده بنا:	۶۵۸/۸۷۲
شمار کتابخانه ملی:	۴۰۵۴۷۶۸
مؤلفین:	سازنگ قربانیان، سید مهدی عمادی استرآبادی، مجیدرضا اخوان، یوسف عطاری
طراح جلد:	حیدر سی ایق
صفحه آرا:	فاطمه حسن زاده
شمارگان:	۶۰۰۰
قیمت:	۲۹۰۰۰ تومان
شابک:	۹۷۸-۶۰۰-۹۵۲۸۱-۴-۱
تاریخ انتشار:	زمستان ۱۳۹۴
نوبت چاپ:	اول
چاپ و صحافی:	طوس

کلیه حقوق این اثر متعلق به انتشارات ادیبان روز می باشد و هرگونه استفاده از این کتاب (کپی، تکثیر، استفاده در کارگاه های آموزشی) بدون اجازه ناشر پیگرد قانونی دارد.

تلفن: ۰۲۱-۶۶۹۵۶۸۱۲-۱۵

خرید الکترونیکی از طریق:

[Http://adibanbook.com](http://adibanbook.com)

[Http://adibanbook.ir](http://adibanbook.ir)



انتشارات ادیبان روز

فهرست مطالب

۱۳	فصل اول: مفاهیم پایه و اساس امنیت در تجارت الکترونیک
۱۴	۱-۱ سیستم مدیریت امنیت اطلاعات
۱۵	۲-۱ مفاهیم امنیت شبکه
۲۰	۳-۱ اهمیت امنیت برای سازمان های کوچک و متوسط در کشورهای در حال توسعه
۲۲	۴-۱ خصوصیات یا سرویس هایی برای پروتکل های امنیتی
۲۲	۵-۱ رمزنگاری
۲۳	۶-۱ احراز هویت مبتنی بر رمز
۲۴	۷-۱ احراز اصالت و حریم خصوصی
۲۵	۸-۱ جامعیت
۲۵	۹-۱ تبادل کلید احراز هویت مبتنی بر رمز
۲۶	۱۰-۱ عدم انکار
۲۷	۱۱-۱ اختفاء
۲۸	۱۲-۱ در دسترس بودن
۲۹	۱۳-۱ آشنایی با حملات pharming
۲۹	۱۴-۱ گونه ای جدید از حمله
۳۳	۱۵-۱ بررسی دنیای واقعی
۳۳	۱۶-۱ امضا
۳۵	۱۷-۱ انصاف (fairness)
۳۵	۱۸-۱ اثر انگشت منحصر به فرد
۳۷	فصل دوم: رمزنگاری و الگوریتمهای آن
۳۸	۱-۲ معرفی و اصطلاحات



۳۹	۲-۲ الگوریتم‌ها
۴۲	۳-۲ کلیدها در رمزنگاری
۴۵	۴-۲ شکستن کلیدهای رمزنگاری
۴۵	۵-۲ الگوریتمهای متقارن
۴۶	۶-۲ الگوریتم های نامتقارن
۴۷	۷-۲ رمزنگاری در پروتکل های انتقال
۴۷	۸-۲ پروتکل ها
۴۸	۹-۲ پروتکل های رمزنگاری انتقال
۶۴	۱۰-۲ رمز گذاری با TLS
۷۵	فصل سوم: رویکردی عملی به امنیت شبکه لایه بندی شده
۷۷	۱-۳ افزودن به ضریب عملکرد، کرها
۷۷	۲-۳ مدل امنیت لایه بندی شده
۹۳	فصل چهارم: بیومتریک و تجهیزات مربوطه
۹۴	۱-۴ Behavioral and Physiometric (خصوصیات رفتاری و فیزیکی)
۱۰۰	۲-۴ امنیت فیزیکی در مراکز حساس IT
۱۰۴	۳-۴ امنیت فیزیکی
۱۰۷	فصل پنجم: آشنایی با ویروسها و ...
۱۱۲	۱-۵ اولین نکته چگونگی امکان ویروسی شدن کامپیوترها
۱۱۳	۲-۵ راه مقابله با ویروسی شدن کامپیوتر با ایمیل
۱۱۸	۳-۵ نمونه هایی از حملات اینترنتی توسط نامه های الکترونیکی
۱۱۹	۴-۵ ترفندهای هکری
۱۲۲	۵-۵ Subseven چیست؟
۱۲۸	۶-۵ آموزش کامل تروجان subseven , pars seven

۱۳۵	۷-۵ آموزش هک با نرم افزار Magic - PS
۱۳۶	۸-۵ آشنایی با یک ویروس ساده
۱۳۷	۹-۵ سوزاندن سخت افزارهای دارای هد
۱۳۷	۱۰-۵ نحوه بدست آوردن IP افراد در Yahoo Messenger بدون ابزار
۱۳۹	۱۱-۵ ویروس و علائم آن در یک نگاه
۱۴۰	۱۲-۵ ساخت یک ویروس
۱۴۱	۱۳-۵ Rookit چیست؟
۱۴۵	۱۴-۵ Banker - AML تروجان
۱۴۶	۱۵-۵ Haxdoor - TC تروجان
۱۴۷	۱۶-۵ Peepview - W تروجان
۱۴۹	۱۷-۵ PWS - AI تروجان
۱۵۰	۱۸-۵ Sickbt - D تروجان
۱۵۱	۱۹-۵ Banload-TI تروجان
۱۵۲	۲۰-۵ Bagle - DM کرم
۱۵۵	۲۱-۵ USKAF - A کرم
۱۵۷	۲۲-۵ Spam چیست؟
۱۶۰	۲۳-۵ Spyware چیست؟
۱۶۶	۲۴-۵ W32/NetSky.B ویروس
۱۶۹	۲۵-۵ معرفی سه گروه اینترنتی Zar.A , Brovia.A و Mydoom.AE
۱۷۰	۲۶-۵ ویروس استاکس نت
۱۷۱	۲۷-۵ ویروس شناسی
۱۷۵	۲۸-۵ تحلیل کد ویروس
۱۸۳	۲۹-۵ Flame ویروس



۱۹۳	فصل ششم: چگونگی فعالیت دیوارهای آتش در لایه‌های مختلف و انواع آنها
۱۹۴	۱-۶ چگونگی فعالیت دیوارهای آتش در لایه‌های مختلف و انواع آنها
۱۹۶	۲-۶ انواع دیوارهای آتش
۱۹۸	۳-۶ صندوق پستی خود را ضد اسپم بسازید
۲۰۳	۴-۶ مدیریت پورتهای و جلوگیری از بروز مشکل به وسیله Firewall
۲۰۴	۵-۶ آبرزش نرم‌افزار Zone Alarm 5.5
۲۰۶	۶-۶ تنظیم برنامه فایروال Zone Alarm
۲۱۰	۷-۶ شمای کلی از نرم افزار
۲۱۵	۸-۶ نگاهی تخصصی
۲۱۶	۹-۶ نوشتن یک سناریوی امنیتی
۲۲۳	۱۰-۶ راهنمای نصب Norton Antivirus
۲۲۶	۱۱-۶ آنتی ویروس و دیوار آتش Microsoft Security Essential
۲۳۱	فصل هفتم: امنیت تجارت و بانکداری الکترونیک
۲۳۳	۱-۷ دیدگاه توسعه بانکداری الکترونیک
۲۳۴	۲-۷ حمله به شبکه های بانکی
۲۳۶	۳-۷ حمله به برنامه های بانکی موجود در گوشی های هوشمند
۲۳۷	۴-۷ اینترنت بانک؛ هدف جدید تروجان
۲۴۰	۵-۷ بدافزاری برای تخلیهی حساب بانکی
۲۴۱	۶-۷ بدافزاری بنام Ghost Push
۲۴۲	۷-۷ راه حل‌های رمزگذاری اطلاعات در سیستمهای بانکی
۲۴۳	۸-۷ زیرساختارهای امنیتی مدرن برای مبادلات در شبکه اینترنت
۲۵۴	۹-۷ امنیت در اینترنت و شبکه های ارتباطی
۲۵۹	۱۰-۷ بررسی نقاط ضعف امنیتی شبکه‌های وب

۲۶۳	۱۱-۷ حمله به برنامه‌های وبی
۲۷۴	۱۲-۷ ایجاد یک ارتباط ایمن در برنامه های وب
۲۹۱	۱۳-۷ امنیت اطلاعات در Web 2.0
۲۹۲	۱۴-۷ خرد جمعی در دهکده ای به نام Web 2.0
۲۹۲	۱۵-۷ خرد جمعی در دهکده ای به نام Web 2.0
۲۹۴	۱۶-۷ امنیت معاملات اینترنتی تا چه اندازه است.
۲۹۶	۱۷-۷ امنیت تعاملات الکترونیکی
۲۹۹	۱۸-۷ امنیت در معاملات اینترنتی
۳۰۱	۱۹-۷ امنیت و داده‌های امنیتی در داد و ستدهای الکترونیک
۳۱۰	۲۰-۷ ارزش ایجاد امنیت
۳۱۳	۲۱-۷ ایمنی و داده‌های امنیتی در اینترنت با کارت SIGN TRUST
۳۱۷	۲۲-۷ حفاظت از حریم شخصی در اینترنت
۳۲۱	۲۳-۷ یک اساس نامه امنیتی (Security Policy) چیست؟
۳۲۵	۲۴-۷ کوکی‌ها و مسائل امنیتی آنها در سایت‌های تجاری و همراه کامپیوترها
۳۳۱	۲۵-۷ کوکی، راز پنهان در مرورگرهای اینترنتی
۳۳۵	۲۶-۷ کلیدهای امنیتی جدید و رمزهای یک دقیقه‌ای!
۳۳۷	۲۷-۷ سایت‌های دولتی نیاز به امنیت دارند
۳۴۷	فصل هشتم: نفوذ و تشخیص نفوذ
۳۴۸	۱-۸ مقایسه تشخیص نفوذ و پیشگیری از نفوذ
۳۵۲	۲-۸ مقایسه امنیت در ویندوز و لینوکس بعنوان سیستم‌های عامل سرور
۳۶۱	فصل نهم: تعریف، تحلیل، پیاده سازی و مقابله با تزریق کدهای SQL
۳۶۲	۱-۹ مقدمه
۳۶۳	۲-۹ تزریق SQL چیست؟



۳۶۵	۳-۹ دسته بندی حملات تزریق
۳۶۶	۴-۹ شاخصهای حملات تزریق SQL
۳۷۰	۵-۹ استنتاج
۳۷۱	۶-۹ پرس و جوهای نادرست غیر مجاز/غیر منطقی
۳۷۲	۷-۹ پرس و جوی Union
۳۸۶	۸-۹ دسته بندی نهایی حمله ها با کمک چند مثال متداول
۳۹۰	۹-۹ تکنیک های تشخیص و جلوگیری
۳۹۲	۱۰-۹ تکنیکهای خودکار تشخیص و جلوگیری از تزریق کد متداول
۳۹۲	۱۱-۹ بررسی کننده های امنیتی
۳۹۳	۱۲-۹ تحلیل ترکیبی استاتیک پویا
۳۹۴	۱۳-۹ یک نمونه دیگر از حمله تزریق کد
۳۹۴	۱۴-۹ تکنیکها و مکانیزهای حفاظتی در برابر تزریق کد
۳۹۵	۱۵-۹ نحوه تشخیص سایتهای آسیب پذیر
۳۹۶	۱۶-۹ مقایسه الگوریتم ها و ابزارهای ارائه شده
۴۰۰	۱۷-۹ ارائه ایده تحقیق و بررسی آن
۴۰۴	۱۸-۹ آزمایش حملات رویه های ذخیره شده با تکنولوژی لینک
۴۰۴	۱۹-۹ برتری هایی لینک در برابر تکنولوژی های ارتباطی سنتی
۴۰۵	فصل دهم: ترفندها و نکات عملیاتی مهم
۴۰۶	۱-۱۰ ابزارهای ناشناخته اما کارآمد برای مسلح سازی سیستم در برابر هکرها
۴۰۶	۲-۱۰ کشف حفره های امنیتی
۴۰۷	۳-۱۰ برنامه های رفع مشکلات امنیتی
۴۰۸	۴-۱۰ امنیت سیستم شخصی
۴۰۹	۵-۱۰ رد ایمیل های دریافتی خود را بگیرید!

۴۱۰	۶-۱۰ ده ترفند برای افزایش امنیت سیستم عامل لینوکس
۴۱۴	۷-۱۰ فعال‌سازی قابلیت مقابله با هکرها در ویندوز XP
۴۱۵	۸-۱۰ اسکن کردن کامپیوتر توسط خودتان، بدون استفاده از آنتی‌ویروس!
۴۱۷	۹-۱۰ جلوگیری از تشخیص اشتباه هرزنامه‌ها در Gmail
۴۱۸	۱۰-۱۰ افزایش سرعت باز شدن صفحات اینترنتی در تمام مرورگرها
۴۲۱	۱۱-۱۰ جلوگیری از دسترسی بدون اجازه‌ی اپلیکیشن‌ها به اینترنت در اندروید
۴۲۲	۱۲-۱۰ ذخیره‌ی نقشه‌های Google Maps برای استفاده‌ی آفلاین در اندروید
۴۲۳	۱۳-۱۰ پی بردن به روت بودن گوشی‌های دارای سیستم عامل اندروید
۴۲۴	۱۴-۱۰ دست‌یابی به لینک مستقیم حساب کاربری در لاین
۴۲۵	۱۵-۱۰ بازگشت به تنظیمات واهی که از آن خارج شده‌اید در تلگرام
۴۲۶	۱۶-۱۰ دو راه برای پی‌ریز کردن به در عبور ذخیره‌شده‌ی شبکه‌ی بی‌سیم در محیط ویندوز
۴۲۸	۱۷-۱۰ نمایان کردن فایل‌ها، مخفی شده توسط ویروس‌ها با یک کلیک!
۴۳۱	منابع و مراجع

پیشگفتار

گروه فناوری اطلاعات انتشارات ادیان روز با سال‌ها تدریس در دانشگاه‌های سراسری، آزاد، علمی-کاربردی و پیام‌نور و با برگیری تجارب از برگزاری دوره‌های آموزش عالی و در نظر گرفتن نه‌واسه‌های دانشجویان رشته‌های متفاوت فناوری اطلاعات، مهندسی و علوم کامپیوتر سعی بر آن‌رد تا آردآوری و تالیف کتب مختلف فناوری اطلاعات به دانشجویان و دانش‌پژوهان در این رشته بزرگ علمی در کشور گام جدیدی را بردارد.

نگرش ما در این سلسله از کتاب‌ها، گرش علمی و در جهت عملی و پیاده‌سازی درست مفاهیم فناوری اطلاعات است.

این گروه با ترکیبی از متخصصین فناوری و مدیریت فناوری و مهندسی کامپیوتر و تجربه عملی در این زمینه دانش فنی خود را طبق سرفصل‌های مورد تایید وزارت علوم و تحقیقات و فناوری در این سلسله از کتاب‌ها به طور روشن و با مراحااحت کلام به مخاطب خود منتقل می‌سازد.

لازم به توضیح است که مخاطب ما فقط دانشجویان دوره‌های فناوری اطلاعات نیست بلکه عموم علم‌آموزان رشته فناوری اطلاعات می‌توانند برای یادگیری و سودآموزی از این مجموعه استفاده نمایند.