

امنیت وب سرورها



تألیف: مهدی دربندی



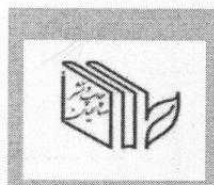
۱۳۹۷

سرشناسه	:	دربندی، مهدی، ۱۳۶۵ -
عنوان و پدیدآور	:	امنیت وب سرورها / مهدی دربندی.
مشخصات نشر	:	تهران: انتشارات صالحیان، ۱۳۹۷.
مشخصات ظاهری	:	۱۳۷ ص.
شابک	:	۹۷۸-۶۲۲-۲۱۴-۰۲۳-۶
وضعیت فهرست نویسی	:	فیپا
موضوع	:	وب -- سرورها -- تدابیر ایمنی
موضوع	:	Web servers -- Security measures
موضوع	:	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	:	Computer networks -- Security measures
رده بندی کنگره	:	TK۵۱۰۵/۸۸۸/د۴الف۸ ۱۳۹۷
رده بندی دیویی	:	۰۰۰۷۲
شماره کتابشناسی ملی	:	۸۳۴۰۱۱

تهران، میدان انقلاب، رگرج جنوبی، خیابان شهدای ژاندامری، پلاک ۱۲۷ واحد ۳

تلفن: ۰۹۱۰۹۱۰۷۴۰۳۰۶۶۹۷۰۴۰۲

سایت انتشارات: www.pubayanz.com



امنیت وب سرورها

کدامولف	مهدی دربندی
کدناشر	صالحیان
کدصفحه آرا	زهرا کرمی
کدشمارگان	۱۰۰۰ نسخه
کدسال و نوبت چاپ	۱۳۹۷-اول
کدشابک	۹۷۸-۶۲۲-۲۱۴-۰۲۳-۶
کدقیمت	۲۴۰۰۰ تومان

فهرست مطالب

۱۰	چکیده
----	-------

فصل ۱: سرورهای شبکه/۱۱

۱۱	مقدمه
۱۲	تعریف سرور
۱۴	انواع وب سرورها
۱۴	وب سرور اینترنت
۱۴	وب سرور اینترنت
۱۴	سرورهای اینترنتی
۱۵	آپاچی (Apache)
۱۷	IIS
۲۳	مقایسه IIS و Apache
۲۷	مقایسه امنیتی Apache در مقابل IIS

فصل ۲: حملات به سرورهای شبکه/۳۰

۳۰	شناسایی تهدیدها و حملات
۳۱	انواع تهدیدها
۳۱	عوامل بروز تهدیدها
۳۱	حملات
۳۲	کدهای مخرب
۳۴	هدف هک
۳۵	لایه‌ها و نقاط ضعف TCP/IP
۳۵	حملات روی لایه فیزیکی
۳۶	حملات روی لایه اینترنت
۳۷	حملات لایه انتقال
۳۸	حملات لایه کاربردی
۳۹	هدف امنیت
۴۰	شیوه‌های هکرها جهت حمله به وب سایت‌ها
۴۰	SQL Injection
۴۲	Cross-Site Scripting
۴۳	Directory Traversal Attacks

۴۳		Parameter Manipulation
۴۵		مهندسی اجتماعی
۴۸		خطرات امنیتی در سرورها
۴۸		سرریز بافر
۵۰		مقابله با سرریز
۵۱		ACTIVE CONTENT
۵۱		مفهوم Java Script
۵۳		Activex
۵۴		کوکي:
۵۵		مشکلات کوکي
۵۶		حملات به کوکي
۵۷		CGI
۵۸		INSTANT MESSAGING
۵۹		روند شکل گیری برنامه های IM
۶۰		MSN Messenger
۶۰		Yahoo Messenger
۶۱		مسائل موجود در IM
۶۱		راه حل مشکلات IM
۶۱		PACKET SNIFFING
۶۴		مراقبت از وب سرورها
۶۴		نظارت بر سرریز بافر
۶۴		تحقیق در مورد سرور و برنامه های موجود در آن
۶۴		توجه به هشدارهای امنیتی
۶۴		استفاده از Login روی سرور
۶۴		استفاده صحیح از رمز گذاری
۶۴		Backup
۶۵		استفاده از ابزارهای Scanning
۶۵		اسکنرهای آسیب پذیری وب
۶۵		AcunetixWeb Vulnerability Scanner
۷۰		Nikto
۷۰		Nessus
۷۲		Nmap
۷۹		tcpsequence

۷۹	 ipidsequence
۷۹	 traceroute

فصل ۳: روشهای کاهش حملات به سرورها/۸۱

۸۱	 مقدمه
۸۳	 ایمن سازی زیرساخت شبکه
۸۳	 استفاده از پروتکل های ارتباطی ایمن
۸۴	 ایمن سازی سیستم ها
۸۴	 ایمن سازی برنامه های کاربردی
۸۴	 تصدیق نام بر
۸۵	 تصدیق کار هوشمند
۸۵	 گواهی نام
۸۵	 تصدیق بیومتریک
۸۵	 فعال کردن بازرسی
۸۶	 فایروال
۸۶	 انواع فایروال
۹۰	 پیکربندی بهینه یک فایروال
۹۱	 لایه لایه کردن سیستم امنیتی
۹۲	 SSL/TLS
۹۳	 ملزومات یک ارتباط مبتنی بر پروتکل امنیتی SSL
۹۳	 اجزای پروتکل SSL
۹۵	 نحوه عملکرد داخلی پروتکل SSL
۹۶	 حملات تأثیر گذار بر SSL
۹۷	 پروتکل HTTPS
۹۷	 نحوه عملکرد HTTPS
۹۹	 تفاوت میان Http// با Https//
۱۰۰	 پیشنهاد برای ایجاد امنیت بر روی وب سرورها

فصل ۴: نتیجه گیری/۱۰۳

فصل ۵: منابع و مآخذ/۱۰۷

۱۱۱	 ضمائم
-----	-------------

چکیده:

از زمان پیدایش شبکه جهانی اینترنت، فاکتور بسیار مهم و حیاتی امنیت، از منظر بخشهای مختلف آن، مورد توجه قرار گرفت. اصلی ترین و شاید کلیدی ترین قسمت آن، بخش سرورها بود. این کتاب تلاش در جهت معرفی انواع مختلف سرورها دارد، و در ضمن به طور خاص به مسئله امنیت در وب سرور ها می پردازد و سعی بر این است تا با معرفی و توضیح مشکلات رایج امنیتی آن، کاربران و دانشجویان علاقمند را با بیشتر این گونه مسائل آشنا نماییم. همچنین در فصل های آتی این کتاب به بحث در مورد چگونگی آسیب پذیری، از جمله استخرهای اسید، پذیری و روش مقاله با این مشکلات و حملات، به طور مثال بکارگیری دیواره های آتش به روز خواهیم پرداخت.