



به نام خدا

امنیت سامانه های اینترنتی

جلد دوم

مولفان:

دافید استوتارت

مارکوس پیتو

مترجم:

علیرضا طالبی



هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

◀ عنوان کتاب: امنیت سامانه های اینترنتی - جلد دوم

◀ مترجم: علیرضا طالبی

◀ ناشر: موسسه فرهنگی هنری دیباگران تهران

◀ ویراستار: ناهید یعقوبی هرزندی

◀ صفحه آرایی: نازنین نصیری

◀ طراح جلد: داریوش فرسای

◀ نوبت چاپ: اول

◀ تاریخ نشر: 1402

◀ چاپ و صحافی: نامن

◀ تیراژ: 100 جلد

◀ قیمت: 3850000 ریال

◀ شابک: 978-622-218-771-2

◀ نشانی واحد فروش: تهران، خیابان انقلاب، خیابان دانشگاه

◀ تقاطع شهدای ژاندارمری - پلاک 158 ساختمان دانشگاه -

◀ طبقه دوم - واحد 4 تلفن ها: 22085111-66965749

◀ فروشگاههای اینترنتی دیباگران تهران:

WWW.MFTBOOK.IR

www.dibagarantehran.com

سرشناسه: استاترد، داوید، 1972-م 1972-1972، Dafydd, Stuttard

عنوان و نام پدیدآور: امنیت سامانه های اینترنتی جلد

دوم / مولفان: دافید استوتارت، مارکوس پینتو؛ مترجم: علیرضا طالبی؛

ویراستار: ناهید یعقوبی هرزندی.

مشخصات نشر: تهران: دیباگران تهران: 1402

مشخصات ظاهری: 406 ص: مصور.

شابک: 978-622-218-770-5 ج 1 - شابک ج 2: 978-622-218-771-2

وضعیت فهرست نویسی: فیا

یادداشت: عنوان اصلی: the web application hacker's handbook: finding and exploiting security flaws 2nd ed. c2011

یادداشت: کتاب حاضر با عنوان راهنمای هکرها در تست نفوذ برنامه های تحت وب: پیدا کردن و اکتشاف انواع مشکلات امنیتی. ترجمه محمدمبین نداد توسط انتشارات زانکودر سال 1398 فیا گرفته است.

عنوان دیگر: راهنمای هکرها در تست نفوذ برنامه های تحت وب: پیدا کردن و اکتشاف انواع مشکلات امنیتی.

موضوع: اینترنت - تدابیر ایمنی

موضوع: internet-security measures

موضوع: کامپیوترها - ایمنی اطلاعات

موضوع: computer security

شناسه افزوده: پینتو، مارکوس، 1978-م

شناسه افزوده: Pinto, Marcus, 1978

شناسه افزوده: طالبی، علیرضا، 1360- مترجم

رده بندی کنگره: TK 5105/875

رده بندی دیویی: 005/8

شماره کتابشناسی ملی: 9438530

نشانی اینستاگرام دیبا: **dibagaran_publishing** نشانی تلگرام: **@mftbook**

هر کتاب دیباگران، یک فرصت جدید علمی و شغلی.

هر گوشی همراه، یک فروشگاه کتاب دیباگران تهران.

از طریق سایتهای دیباگران، در هر جای ایران به کتابهای ما دسترسی دارید.

فهرست مطالب

فصل ۱۲

حمله به کاربران: اسکریپت بین سایتی ۱۱

۱۳	انواع XSS
۱۳	منعکس کننده آسیب پذیری های XSS
۱۸	آسیب پذیری های XSS ذخیره شده
۱۹	آسیب پذیری های XSS مبتنی بر DOM
۲۱	حملات XSS در عمل
۲۱	حملات XSS در دنیای واقعی
۲۶	مکانیسم های تحویل برای حملات XSS
۳۰	یافتن و بهره برداری از آسیب پذیری های XSS
۳۱	یافتن و بهره برداری از آسیب پذیری های بازتاب شده XSS
۶۰	یافتن و بهره برداری از آسیب پذیری های ذخیره شده XSS
۶۶	یافتن و بهره برداری از آسیب پذیری های XSS مبتنی بر DOM
۷۰	جلوگیری از حملات XSS
۷۰	جلوگیری از بازتاب و ذخیره XSS
۷۴	جلوگیری از XSS مبتنی بر DOM
۷۵	خلاصه
۷۶	سوالات

فصل ۱۳

حمله به کاربران: تکنیک های دیگر ۷۷

۷۷	القای اقدامات کاربر
۷۸	درخواست جعل
۸۷	رفع UI
۹۱	گرفتن داده های متقاطع دامنه
۹۱	گرفتن داده با تزریق HTML
۹۳	گرفتن داده با تزریق CSS
۹۵	ربودن جاوا اسکریپت
۹۹	سیاست منبع بازبینی
۱۰۴	عبور از دامنه ها با برنامه های کاربردی سرویس پروکسی

۱۰۵.....	سایر حملات تزریق سمت مشتری
۱۰۶.....	تزریق هدر HTTP
۱۰۷.....	تزریق کوکی‌ها
۱۱۵.....	آسیب‌پذیری‌های Redirection را باز کنید
۱۲۱.....	تزریق SQL سمت مشتری
۱۲۲.....	آلودگی پارامتر HTTP سمت مشتری
۱۲۳.....	حملات حریم خصوصی محلی
۱۲۳.....	کوکی‌های ماندگار
۱۲۵.....	تاریخچه مرور
۱۲۵.....	تکمیل خودکار
۱۲۶.....	فلش اشیای مشترک محلی
۱۲۷.....	ذخیره‌سازی ایزوله Silverlight
۱۲۷.....	داده‌های کاربر اینترنت اکسپلورر
۱۲۷.....	مکانیسم‌های ذخیره‌سازی محلی HTML5
۱۲۸.....	جلوگیری از حملات حریم خصوصی محلی
۱۲۸.....	حمله به کنترل‌های ActiveX
۱۲۹.....	یافتن آسیب‌پذیری‌های ActiveX
۱۳۱.....	جلوگیری از آسیب‌پذیری‌های ActiveX
۱۳۲.....	حمله به مرورگر
۱۳۳.....	ورود به سیستم ضربه زدن به کلید
۱۳۳.....	سرقت تاریخچه مرورگر و پرس‌وجوهای جست‌وجو
۱۳۳.....	شمارش برنامه‌های کاربردی فعلی
۱۳۴.....	اسکن پورت
۱۳۵.....	حمله به هاست‌های دیگر شبکه
۱۳۵.....	بهره‌برداری از خدمات غیر HTTP
۱۳۶.....	بهره‌برداری از اشکالات مرورگر
۱۳۶.....	DNS Rebinding
۱۳۷.....	چارچوب‌های بهره‌برداری مرورگر
۱۳۹.....	حملات مرد میانی (Man-in-the-Middle)
۱۴۱.....	خلاصه
۱۴۱.....	سؤالات

فصل ۱۴

۱۴۳..... خودکارسازی حملات سفارشی‌شده

۱۴۴..... اتوماسیون سفارشی

۱۴۵.....	شمارش شناسه‌های معتبر.....
۱۴۵.....	رویکرد اساسی.....
۱۴۶.....	تشخیص بازدهیها.....
۱۴۸.....	اسکرپت‌نویسی حمله.....
۱۴۹.....	جت اتک.....
۱۵۳.....	جمع‌آوری داده‌های مفید.....
۱۵۶.....	Fuzzing برای آسیب‌پذیری‌های رایج.....
۱۵۹.....	قرار دادن این همه با هم: Burp Intruder.....
۱۶۹.....	موانع اتوماسیون.....
۱۷۰.....	مکانیسم‌های رسیدگی به جلسه.....
۱۷۷.....	کنترل‌های CAPTCHA.....
۱۷۹.....	خلاصه.....
۱۸۰.....	سؤالات.....

فصل ۱۵

بهره‌برداری از افشای اطلاعات..... ۱۸۱

۱۸۱.....	بهره‌برداری از پیام‌های خطا.....
۱۸۲.....	پیام‌های خطای اسکرپت.....
۱۸۳.....	ردیابی پشته.....
۱۸۴.....	پیام‌های اشکال‌زدایی آموزنده.....
۱۸۵.....	پیام‌های سرور و پایگاه داده.....
۱۸۸.....	استفاده از اطلاعات عمومی.....
۱۸۹.....	پیام‌های خطای اطلاعاتی مهندسی.....
۱۹۰.....	جمع‌آوری اطلاعات منتشرشده.....
۱۹۱.....	استفاده از استنتاج.....
۱۹۳.....	جلوگیری از نشت اطلاعات.....
۱۹۳.....	از پیام‌های خطای عمومی استفاده کنید.....
۱۹۴.....	محافظت از اطلاعات حساس.....
۱۹۵.....	نشت اطلاعات سمت مشتری را به حداقل برسانید.....
۱۹۵.....	خلاصه.....
۱۹۵.....	سؤالات.....

فصل ۱۶

حمله به برنامه‌های کامپایل‌شده بومی..... ۱۹۸

۱۹۹.....	آسیب‌پذیری‌های سرریز بافر.....
----------	--------------------------------

۱۹۹.....	پشته‌های سرریز
۲۰۰.....	هیپ سرریز
۲۰۱.....	آسیب‌پذیری‌های "Off-by-One"
۲۰۳.....	شناسایی آسیب‌پذیری‌های بافر Overflow
۲۰۵.....	آسیب‌پذیری‌های عدد صحیح
۲۰۵.....	سرریز اعداد صحیح
۲۰۶.....	شناسایی آسیب‌پذیری‌های عدد صحیح
۲۰۷.....	آسیب‌پذیری‌های رشته را قالب‌بندی کنید
۲۰۸.....	شناسایی آسیب‌پذیری‌های رشته قالب
۲۰۹.....	خلاصه
۲۰۹.....	سوالات

فصل ۱۷

حمله به معماری اپلیکیشن ۲۱۱

۲۱۱.....	معماری‌های لایه‌ای
۲۱۲.....	حمله به معماری‌های طبقه‌ای
۲۱۳.....	بهره‌برداری از روابط اعتماد بین لایه‌ها
۲۱۸.....	میزبانی مشترک و ارائه‌دهندگان خدمات برنامه کاربردی
۲۱۹.....	میزبانی مجازی
۲۲۷.....	ایمن‌سازی محیط‌های مشترک
۲۲۹.....	خلاصه
۲۲۹.....	سوالات

فصل ۱۸

حمله به سرور برنامه ۲۳۰

۲۳۱.....	پیکربندی سرور آسیب‌پذیر
۲۳۱.....	اعتبار پیش‌فرض
۲۳۲.....	محتوای پیش‌فرض
۲۳۸.....	فهرست‌های دایرکتوری
۲۴۳.....	سرور برنامه به‌عنوان یک پروکسی
۲۴۴.....	میزبانی مجازی با پیکربندی نادرست
۲۴۵.....	ایمن‌سازی پیکربندی وب سرور
۲۴۶.....	نرم‌افزار سرور آسیب‌پذیر
۲۴۶.....	ایرادات چارچوب برنامه
۲۴۹.....	آسیب‌پذیری‌های مدیریت حافظه

۲۵۰.....	رمزگذاری و متعارف‌سازی
۲۵۴.....	پیدا کردن ایرادات وب سرور
۲۵۵.....	امنیت نرم‌افزار وب سرور
۲۵۷.....	فایروال‌های برنامه کاربردی وب
۲۵۹.....	خلاصه
۲۵۹.....	سؤالات

فصل ۱۹

یافتن آسیب‌پذیری‌ها در کد منبع ۲۶۰

۲۶۱.....	رویکردهای بررسی کد
۲۶۱.....	تست جعبه سیاه در مقابل جعبه سفید
۲۶۲.....	روش بررسی کد
۲۶۳.....	امضای آسیب‌پذیری‌های رایج
۲۶۳.....	اسکرپت بین‌سایتی
۲۶۴.....	تزریق SQL
۲۶۵.....	پیمایش مسیر
۲۶۶.....	تغییر مسیر دلخواه
۲۶۷.....	پسوردهای درب پستی
۲۶۷.....	اشکالات نرم‌افزار بومی
۲۶۹.....	پلتفرم جاوا
۲۶۹.....	شناسایی داده‌های ارائه‌شده توسط کاربر
۲۷۰.....	تعامل جلسه
۲۷۱.....	APIهای بالقوه خطرناک
۲۷۴.....	پیکربندی محیط جاوا
۲۷۵.....	ASP.NET
۲۷۵.....	شناسایی داده‌های ارائه‌شده توسط کاربر
۲۷۷.....	تعامل جلسه
۲۷۸.....	APIهای بالقوه خطرناک
۲۸۲.....	پیکربندی محیط ASP.NET
۲۸۳.....	PHP
۲۸۳.....	شناسایی داده‌های ارائه‌شده توسط کاربر
۲۸۵.....	تعامل جلسه
۲۸۶.....	APIهای بالقوه خطرناک
۲۹۱.....	پیکربندی محیط PHP
۲۹۳.....	پزل

۲۹۴.....	شناسایی داده‌های ارائه‌شده توسط کاربر
۲۹۵.....	تعامل جلسه
۲۹۵.....	API‌های بالقوه خطرناک
۲۹۷.....	پیکربندی محیط پرل
۲۹۸.....	جاوا اسکریپت
۲۹۸.....	اجزای کد پایگاه داده
۲۹۹.....	تزریق SQL
۳۰۰.....	فراخوانی به عملکردهای خطرناک
۳۰۰.....	ابزارهایی برای مرور کد
۳۰۱.....	خلاصه
۳۰۲.....	سوالات

فصل ۲۰

یک جعبه ابزار هک برنامه وب..... ۳۰۴

۳۰۵.....	مرورگرهای وب
۳۰۵.....	اینترنت اکسپلورر
۳۰۶.....	فایرفاکس
۳۰۷.....	کروم
۳۰۸.....	مجموعه‌های تست یکپارچه
۳۰۸.....	ابزارها چگونه کار می‌کنند
۳۲۵.....	تست جریان کار
۳۲۷.....	جایگزین‌های رهگیری پروکسی
۳۲۹.....	اسکنرهای آسیب‌پذیری مستقل
۳۳۰.....	آسیب‌پذیری‌های شناسایی‌شده توسط اسکنرها
۳۳۲.....	محدودیت‌های ذاتی اسکنرها
۳۳۳.....	چالش‌های فنی پیش‌روی اسکنرها
۳۳۶.....	محصولات فعلی
۳۳۸.....	استفاده از اسکنر آسیب‌پذیری
۳۴۰.....	ابزارهای دیگر
۳۴۰.....	Wikto/Nikto
۳۴۱.....	Firebug
۳۴۱.....	Hydra
۳۴۲.....	اسکرپت‌های سفارشی
۳۴۴.....	خلاصه

متدولوژی هکر برنامه وب ۳۴۶

۳۴۸.....	دستورالعمل‌های عمومی
۳۵۳.....	برنامه را تجزیه و تحلیل کنید.....
۳۵۵.....	کنترل‌های سمت مشتری را آزمایش کنید.....
۳۶۰.....	مکانیسم احراز هویت را آزمایش کنید.....
۳۶۸.....	مکانیسم مدیریت جلسه را آزمایش کنید.....
۳۷۵.....	کنترل‌های دسترسی را آزمایش کنید.....
۳۷۸.....	تست برای آسیب‌پذیری‌های مبتنی بر ورودی.....
۳۹۰.....	برای آسیب‌پذیری‌های ورودی عملکردهای خاص را آزمایش کنید.....
۳۹۶.....	تست برای ایرادات منطقی.....
۳۹۸.....	تست برای آسیب‌پذیری‌های هاست اشتراکی.....
۳۹۹.....	برای آسیب‌پذیری‌های سرور برنامه آزمایش کنید.....
۴۰۳.....	چک متفرقه.....
۴۰۶.....	پیگیری هرگونه نشانه‌های اطلاعات.....

خط‌مشی انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی با کیفیت عالی است که تواند
خواسته‌های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.
هر کتاب دیباگران تهران، یک فرصت جدید شغلی و علمی

حمد و سپاس ایزد منان را که با الطاف بی‌کران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی و آموزشی گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و سرعت توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه، نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش برجسته نموده است.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران و محققان در زمینه‌های گوناگون و مورد نیاز جامعه تلاش نموده برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهد.

کتابی که در دست دارید ترجمه "جناب آقای علیرضا طالبی" است که با تلاش همکاران ما در نشر دیباگران تهران منتشر گشته و شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

با نظرات خود مشوق و راهنمای ما باشید

با ارائه نظرات و پیشنهادات و خواسته‌های خود، به ما کمک کنید تا بهتر و دقیق‌تر در جهت رفع نیازهای علمی و آموزشی کشورمان قدم برداریم. برای رساندن پیام‌هایتان به ما از رسانه‌های دیباگران تهران شامل سایتهای فروشگاهی و صفحه اینستاگرام و شماره‌های تماس که در صفحه شناسنامه کتاب آمده استفاده نمایید.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
dibagaran@mftplus.com