به نام خدا

راهنمای آزمون نفوذ در سامانه‌های تحت‌وب براساس استاندارد OWASP

مترجمین :

جوادمرادی

میثم‌میرزائی

محمدحسین حسن نیا

عنوان کتاب: **راهنمای آزمون نفوذ در سامانه های تحت وب براساس استاندارد OWASP**

عنوان کتاب اصلی : OWASP Testing Guide 4.0

مترجمان : جواد مرادی- میثم میرزائی-محمدحسین حسن نیا

ناشر: موسسه فرهنگی هنری دیباگران تهران

ویراستار: الهام نقیبی

صفحه آرایی: نازنین نصیری

طراح جلد:داریوش فرسایی

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۹

چاپ و صحافی: صدف

تیراژ: ۱۰۰ جلد

قیمت: ۸۰۰۰۰۰ ریال

شابک: ۹۷۸-۶۲۲-۲۱۸-۳۵۰-۹

نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، روبروی پاساژ مهستان، پلاک ۱۲۵۱

تلفن: ۲۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagarantehran.com

www.dibbook.ir

نشانی تلگرام:mftbook@

نشانی اینستاگرام دیبا dibagaran_publishing

سرشناسه: میوچی،ماتئو Meucci,Matteo

عنوان و نام پدیدآور: راهنمای آزمون نفوذ در سامانه های تحت وب براساس استاندارد OWASP (ماتئو میوچی،اندرو مولر)؛مترجمان: جواد مرادی، میثم میرزائی، محمدحسین حسن زاده؛ ویراستار : الهام نقیبی.

مشخصات نشر: تهران : دیباگران تهران :۱۳۹۹

مشخصات ظاهری:۳۶۴ص:مصور،

شابک: ۹۷۸-۶۲۲-۲۱۸-۳۵۰-۹

وضعیت فهرست نویسی: فیپا

یادداشت: عنوان اصلی: OWASP Testing Guide v4,2019

یادداشت : کتابنامه.

موضوع: شبکه های کامپیوتری –تدابیر ایمنی-آزمون ها

موضوع: computer networks-security measures-examinations

موضوع: وبگاه ها- تدابیر ایمنی

موضوع: web sites-security measures

شناسه افزوده: مولر اندرو، Muller Andrew

شناسه افزوده: مرادی، جواد، ۱۳۷۱- مترجم.

شناسه افزوده: میرزائی، میثم، ۱۳۶۸- مترجم.

شناسه افزوده: حسن زاده، محمد حسین، ۱۳۵۶-مترجم.

رده بندی کنگره:۵۱۰۵/۵۹ TK

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۷۳۰۶۴۹۲

هرکتاب دیباگران ،یک فرصت جدید شغلی.

هرگوشی همراه،یک فروشگاه کتاب دیباگران تهران.

از طریق سایتها و اپ دیباگران،در هر جای ایران به کتابهای ما دسترسی دارید.

فهرست مطالب

مقدمه ناشر ۸

مقدمه مؤلفین ۹

فصل اول

مقدمه و اهداف ۱۰

مقدمه ۱۱

فصل دوم

جمع‌آوری اطلاعات ۱۳

۲-۱: مقدمه ۱۴

۲-۲: بررسی موتورهای جستجوگر به‌منظور نشت اطلاعات ۱۵

۲-۳: انگشت‌نگاری وب سرور ۱۸

۲-۴: بازبینی فراپرونده‌های وب سرور به‌منظور نشت اطلاعات ۲۷

۲-۵: برشماری برنامه‌های کاربردی بر روی وب سرور ۳۳

۲-۶: بازبینی توضیحات و فراداده‌های صفحات وب برای نشت اطلاعات ۳۷

۲-۷: شناسایی نقاط ورودی برنامه‌های کاربردی ۴۰

۲-۸: نقشه‌کشی مسیرهای اجرایی در برنامه کاربردی ۴۲

۲-۹: انگشت‌نگاری چارچوب برنامه کاربردی وب ۴۵

۲-۱۰: انگشت‌نگاری برنامه کاربردی وب ۵۲

۲-۱۱: نقشه معماری برنامه کاربردی ۵۷

فصل سوم

آزمون پیکربندی و مدیریت استقرار ۶۰

۳-۱: مقدمه ۶۱

۳-۲: آزمون پیکربندی شبکه/زیرساخت ۶۲

۳-۳: آزمون پیکربندی بستر برنامه کاربردی ۶۴

۴-۳: آزمون پردازش پسوند فایل‌ها برای داده‌های حساس ۷۰
۵-۳: بررسی فایل‌های قدیمی، پشتیبان و بدون مرجع برای داده‌های حساس ۷۳
۶-۳: آزمون برشماری واسط‌های مدیریتی زیرساخت و برنامه کاربردی ۷۹
۷-۳: آزمون متدهای HTTP ۸۳
۸-۳: آزمون HSTS ۸۹
۹-۳: آزمون قوانین بین دامنه‌ای RIA ۹۰
۱۰-۳: آزمون مجوز فایل ۹۳

فصل چهارم

آزمون مدیریت هویت ۹۶

۱-۴: مقدمه ۹۷
۲-۴: آزمون تعریف نقش‌های سامانه ۹۷
۳-۴: آزمون فرایند ثبت‌نام کاربر ۹۹
۴-۴: آزمون فرایند تأمین حساب کاربری ۱۰۲
۵-۴: آزمون برشماری حساب‌های کاربری و نام‌های کاربری قابل حدس ۱۰۴
۶-۴: آزمون صحت و انعطاف‌پذیری سیاست انتخاب نام کاربری ۱۱۰

فصل پنجم

اصالت‌سنجی ۱۱۱

۱-۵: مقدمه ۱۱۲
۲-۵: آزمون ارسال اطلاعات حساب کاربری از درون کانال رمز شده ۱۱۳
۳-۵: آزمون بررسی اعتبارنامه‌های پیش‌فرض ۱۱۷
۴-۵: آزمون برای سازوکار ضعیف مسدودسازی ۱۲۱
۵-۵: آزمون برای دور زدن شمای اصالت‌سنجی ۱۲۳
۶-۵: آزمون برای سازوکار حفظ نمودن گذرواژه ۱۲۹
۷-۵: آزمون برای ضعف‌های حافظهٔ نهان ۱۳۰
۸-۵: آزمون برای سیاست ضعیف گذرواژه ۱۳۳
۹-۵: آزمون برای پرسش/پاسخ امنیتی ضعیف ۱۳۳
۱۰-۵: آزمون برای سازوکار ضعیف بازنشانی یا تغییر گذرواژه ۱۳۶
۱۱-۵: آزمون آسیب‌پذیری در کانال‌های اصالت‌سنجی جایگزین ۱۳۸

فصل ششم

مجازشماری ۱۴۱

۶-۱: مقدمه ۱۴۲
۶-۲: آزمون پیمایش مسیر پوشه‌ها و فایل‌های آن ۱۴۲
۶-۳: آزمون دور زدن شمای مجوزهای اصالت‌سنجی ۱۴۹
۶-۴: آزمون ارتقاء سطح دسترسی ۱۵۱
۶-۵: آزمون برای مراجع مستقیم ناامن به شیء ۱۵۴

فصل هفتم

آزمون مدیریت نشست ۱۵۶

۷-۱: مقدمه ۱۵۷
۷-۲: آزمون شمای مدیریت نشست ۱۵۸
۷-۳: آزمون ویژگی کوکی‌ها ۱۶۵
۷-۴: آزمون بررسی وجود آسیب‌پذیری تثبیت نشست ۱۶۹
۷-۵: آزمون متغیرهای افشاء شده نشست ۱۷۲
۷-۶: آزمون جعل درخواست ۱۷۵
۷-۷: آزمون عملکرد خروج ۱۸۱
۷-۸: آزمون اتمام مهلت نشست ۱۸۴
۷-۹: آزمون آشفتگی نشست ۱۸۶

فصل هشتم

ورودی نامعتبر ۱۸۸

۸-۱: مقدمه ۱۸۹
۸-۲: آزمون XSS انعکاسی ۱۹۱
۸-۳: آزمون XSS ذخیره شده ۱۹۹
۸-۴: آزمون متدهای مخرب ۲۰۶
۸-۵: آزمون آلودگی پارامترهای HTTP ۲۱۱
۸-۶: آزمون تزریق SQL ۲۱۵

۸-۷: آزمون تزریق LDAP ۲۳۴
۸-۸: آزمون تزریق ORM ۲۳۷
۸-۹: آزمون تزریق XML ۲۳۹
۸-۱۰: آزمون تزریق SSI ۲۴۸
۸-۱۱: آزمون تزریق XPATH ۲۵۲
۸-۱۲: آزمون تزریق IMAP/SMTP ۲۵۶
۸-۱۳: آزمون تزریق کد ۲۶۳
۸-۱۳-۱: آزمون FILE INCLUSION محلی ۲۶۵
۸-۱۳-۲: آزمون FILE INCLUSION راه دور ۲۶۸
۸-۱۴: آزمون تزریق فرمان ۲۷۰
۸-۱۵: آزمون سرریز بافر ۲۷۶

فصل نهم

آزمون مدیریت خطا ۲۸۲

۹-۱: مقدمه ۲۸۳
۹-۲: تحلیل کدهای خطا ۲۸۳
۹-۳: آزمون برای ردیابی پشته ۲۹۰

فصل دهم

آزمون رمزنگاری ۲۹۳

۱۰-۱: مقدمه ۲۹۴
۱۰-۲: ارزیابی برای رمزنگاری ضعیف SSL / TLS ۲۹۴
۱۰-۳: ارسال داده‌های حساس در کانال‌های رمزگذاری نشده ۳۱۶
۱۰-۴: آزمون رمزنگاری ضعیف ۳۲۰

فصل یازدهم

آزمون منطق کسب‌وکار ۳۲۳

۱۱-۱: مقدمه ۳۲۴
۱۱-۲: آزمون اعتبارسنجی داده منطق کسب‌وکار ۳۲۵

۳-۱۱: آزمون بررسی امکان جعل درخواست ۳۲۷
۴-۱۱: آزمون یکپارچگی داده‌ها ۳۲۹
۵-۱۱: آزمون بررسی زمان پردازش ۳۳۱
۶-۱۱: آزمون محدودیت تعداد دفعات استفاده از یک عملکرد ۳۳۳
۷-۱۱: آزمون دور زدن جریان کاری ۳۳۴
۸-۱۱: آزمون دفاع در برابر عدم استفاده مناسب از برنامه کاربردی ۳۳۶

فصل دوازدهم

آزمون سمت کاربر ۳۳۹

۱-۱۲: مقدمه ۳۴۰
۲-۱۲: ارزیابی XSS مبتنی بر DOM ۳۴۱
۳-۱۲: تزریق HTML ۳۴۴
۴-۱۲: انتقال URL سمت کاربر ۳۴۶
۵-۱۲: آزمون تزریق CSS ۳۴۸
۶-۱۲: دستکاری منابع سمت کاربر ۳۵۰
۷-۱۲: آزمون وب سوکت ۳۵۴
۸-۱۲: ارزیابی پیام‌رسانی وب ۳۵۷
۹-۱۲: ارزیابی ذخیره‌ساز محلی ۳۶۰

مراجع ۳۶۴

مقدمه ناشر

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب هایی است که بتواند
خواسته های 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 دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گستردگی علوم و 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 روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُربار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت **"مهندسان جواد مرادی-میثم میرزائی-محمد حسین حسن زاده"** و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
bookmarket@mft.info

مقدمه مؤلفین

بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، فرهنگی، اجتماعی و ارتباطات، در کلیه سطوح اعم از افراد، مؤسسه‌های غیردولتی و نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد و با گسترش روزافزون استفاده از فضای سایبری، امنیت در این فضا به یکی از دغدغه‌های اصلی سازمان‌ها و افراد تبدیل شده است. یکی از مهم‌ترین عامل‌های حفظ امنیت در فضای سایبری، انجام ارزیابی‌های امنیتی است. ارزیابی امنیتی به فرآیند شبیه‌سازی حملات سایبری بر روی یک وب‌سایت یا شبکه کامپیوتری گفته می‌شود. هدف این کار شناسایی نقاط ضعف و تلاش برای برطرف کردن آسیب‌پذیری‌ها است که این کار از حمله‌های آتی هکرها و بهره‌مندی غیرمجاز آن‌ها از سیستم جلوگیری می‌کند.

کتاب ارزشمندی که پیش‌رو دارید ترجمه OWASP Testing Guide v4 است که به‌عنوان استاندارد ارزیابی امنیتی و آزمون نفوذ وب‌سایت تلقی می‌شود. در این کتاب سعی شده است که تمامی حملات رایج سایبری با بیانی ساده و به‌طور اختصار بیان شود و در ادامه نحوهٔ ارزیابی و تشخیص این آسیب‌پذیری‌ها ذکر گردند. محتوای کتاب به‌نحوی نگارش شده است که هم برای افرادی که به تازگی قصد ورود به حوزه ارزیابی امنیتی و آزمون نفوذ دارند و هم افرادی که سابقه کار در این حوزه را دارند، مناسب باشد. آنها با مطالعه این سند می‌توانند به یک رهیافت جامع در ارزیابی سامانه‌های تحت وب دست پیدا کنند. حملات تحت وب در ۱۱ بخش اصلی که شامل موارد زیر است، تقسیم‌بندی می‌شوند:

- جمع‌آوری اطلاعات
- آزمون پیکربندی و مدیریت استقرار
- آزمون مدیریت هویت
- آزمون اصالت‌سنجی
- آزمون مجاز شماری
- آزمون مدیریت نشست
- آزمون اعتبارسنجی ورودی
- پردازش خطا
- آزمون رمزنگاری ضعیف
- آزمون منطق کسب‌وکار
- آزمون سمت کاربر

هر کدام از دسته‌های فوق حملات مختلفی را شامل می‌شوند که در طی فصل‌های جداگانه به تشریح آنها می‌پردازیم.

لازم است از جناب مهندس حسن نیا که متن کتاب را بازخوانی و نکات مهمی را گوشزد نمود و موجبات چاپ کتاب را فراهم کرده، سپاس گذاری کنیم.

در پایان از خوانندگان محترم خواهشمندم که انتقادات سازنده و پیشنهادهای خود را به پست الکترونیکی moradi.pentest1214@gmail.com ارسال کنند.