



به نام خدا

مروری بر مهمترین تست های امنیتی

سرویس های تحت وب

Owasp Web security Testing Guide

مؤلف:

احسان امجدی



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: **مروری بر مهمترین تست های امنیتی سرویس های تحت وب**

Owasp Web Security Testing Guide

◀ مولف: **احسان امجدی**

◀ ناشر: **موسسه فرهنگی هنری دیباگران تهران**

◀ ویراستار: **مهديه مخبري**

◀ صفحه آرايي: **فروش عبدلهي**

◀ طراح جلد: **داریوش فرسايي**

◀ نوبت چاپ: **اول**

◀ تاريخ نشر: **۱۴۰۲**

◀ چاپ و صحافي: **صدف**

◀ تیراژ: **۱۰۰ جلد**

◀ قيمت: **۳۰۵۰۰۰۰ ريال**

◀ شابک: **۹۷۸-۶۲۲-۲۱۸-۷۲۴-۸**

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

◀ تقاطع شهدای ژاندارمری - پلاک ۱۵۸ ساختمان دانشگاه -

◀ طبقه دوم - واحد ۴ تلفن ها: **۶۶۹۶۵۷۴۹-۲۲۰۸۵۱۱۱**

◀ فروشگاههای اینترنتی **دیباگران تهران** :

WWW.MFTBOOK.IR

www.dibagartehran.com

سرشناسه: **امجدی بیگوند، احسان، ۱۳۶۴-**

عنوان و نام پدیدآور: **مروری بر مهمترین تست های امنیتی**

سرویس های تحت وب **Owasp web security testing**

guide / مولف: احسان امجدی؛

ویراستار: مهديه مخبري.

مشخصات نشر: **تهران: دیباگران تهران: ۱۴۰۲**

مشخصات ظاهري: **۳۳۰ ص: مصور،**

شابک: **۹۷۸-۶۲۲-۲۱۸-۷۲۴-۸**

وضعیت فهرست نویسی: **فیبا**

موضوع: **وب- سرورها- تدابیر ایمنی**

موضوع: **web servers-security measures**

رده بندی کنگره: **TK ۵۱۰۵/۸۸۸**

رده بندی دیویی: **۰۰۵/۷۲**

شماره کتابشناسی ملی: **۹۳۴۷۳۳۲۳**

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 ۱ / معرفی پروژه تست OWASP..... ۷

۸ پروژه تست OWASP

۹ سنجش امنیت: آثار اقتصادی ناشی از وجود نرم افزار ناامن

۲۲ مدل سازی تهدید (Threat Modeling)

فصل ۲ / فریم ورک تست OWASP..... ۳۲

۳۳ فریم ورک تست امنیت وب سرویس

فصل ۳ / تست امنیت وب اپلیکیشن..... ۴۴

۴۵ ۳.۱ آشنایی با تست

۴۸ ۳.۲ جمع آوری اطلاعات (Information Gathering)

۱۲۰ ۳.۳ تست مدیریت پیکربندی و استقرار

۱۵۴ ۳.۴ تست مدیریت هویت

۱۶۳ ۳.۵ تست احراز هویت

۱۸۰ ۳.۶ تست مجوز دسترسی

۱۹۶ ۳.۷ تست مدیریت نشست

۲۱۹ ۳.۸ تست اعتبارسنجی ورودی ها

۲۹۳ ۳.۹ تست مدیریت خطا

۲۹۶ ۳.۱۰ تست رمزنگاری ضعیف

۳۰۲ تست منطق کسب و کار ۳.۱۱

۳۰۵ Client-Side تست ۳.۱۲

۳۲۵ فصل ۴ / گزارش نویسی

۳۲۶ بخش اول: معرفی

۳۲۷ بخش دوم: خلاصه‌ای از اقدامات انجام شده

۳۲۸ بخش سوم: یافته‌ها

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 تألیف "جناب آقای احسان امجدی" 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

مقدمه مولف

خداوند منان را شاکرم که به من این فرصت را داد تا بتوانم کتاب پیش‌رو را برای متخصصین و علاقه‌مندان به دنیای امنیت، بخصوص گرایش هک و تست نفوذ، گردآوری کنم. در این کتاب که بر پایه OWASP نوشته شده است، به مهمترین تست‌های امنیتی که روی سرویس‌های تحت وب قابل تعریف و انجام است، پرداخته شده است. یکی از مهمترین دغدغه‌هایی که در این زمینه وجود دارد، برداشت‌های مختلفی است که بعضاً برخی از متخصصین در این حوزه از اجرای تست نفوذ روی سرویس‌های تحت وب دارند. همین باعث شد تا نیاز به وجود مرجعی (به زبان فارسی) حس شود و تالیف این کتاب شاید فقط کمک کوچکی در رفع این نیاز و ارتقاء سطح فنی همکاران بویژه جوان‌تر، در این حوزه باشد.

لازم میدانم از همه عزیزانی که در طول این مدت به نوعی زمینه‌ساز تالیف این کتاب بودند، تشکر و قدردانی کنم.

این کتاب ماحصل اوقاتی است که خاص خانواده بوده است؛ به همین جهت آن را به همسر و فرزند عزیزم، نیکی تقدیم می‌کنم.