مؤسسه فرهنگی هنری
دیباگران تهران

به نام خدا

امنیت سامانه های اینترنتی

جلد اول

مولفان:
دافید استوتارت
مارکوس پینتو

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 می‌گیرند.

مؤسسه فرهنگی هنری
دیباگران تهران

◂ عنوان کتاب: **امنیت سامانه های اینترنتی –جلد اول**

◂ مترجم : **علیرضا طالبی**

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

◂ **ویراستار:** ناهید یعقوبی هرزندی

◂ **صفحه آرایی:** نازنین نصیری

◂ **طراح جلد:** داریوش فرسایی

◂ **نوبت چاپ:** اول

◂ **تاریخ نشر:** ۱۴۰۲

◂ **چاپ و صحافی:** صدف

◂ **تیراژ:** ۱۰۰ جلد

◂ **قیمت:** ۳۸۵۰۰۰۰ ریال

◂ **شابک:** ۹۷۸-۶۲۲-۲۱۸-۷۷۰-۵

نشانی واحد فروش: تهران، خیابان انقلاب، خیابان دانشگاه
–تقاطع شهدای ژاندارمری–پلاک ۱۵۸ساختمان دانشگاه–
طبقه دوم–واحد۴ تلفن ها: ۶۶۹۶۵۷۴۹–۲۲۰۸۵۱۱۱

فروشگاههای اینترنتی دیباگران تهران :
WWW.MFTBOOK.IR
www.dibagarantehran.com

سرشناسه:استاترد،داوید،۱۹۷۲–م Stuttard,Dafydd,1972
عنوان و نام پدیدآور:امنیت سامانه های اینترنتی جلد اول/مولفان:دافید استوتارت،مارکوس پینتو؛مترجم:علیرضا طالبی؛ ویراستار:ناهید یعقوبی هرزندی.
مشخصات نشر: تهران : دیباگران تهران :۱۴۰۲
مشخصات ظاهری:۴۰۶ ص:مصور.
شابک: ۹۷۸-۶۲۲-۲۱۸-۷۷۰-۵
وضعیت فهرست نویسی: فیپا
یادداشت:عنوان اصلی: the web application hacker's handbook:finding and exploiting security flaws 2nd ed.c2011
یادداشت:کتاب حاضربا عنوان راهنمای هکرهادرتست نفوذ برنامه های تحت وب :پیداکردن و اکسپلویت انواع مشکلات امنیتی.ترجمه محمدامین ندا،توسط انتشارات زانکودر سال ۱۳۹۸ فیپاگرفته است.
عنوان دیگرراهنمای هکرهادرتست نفوذبرنامه های تحت وب:پیدا کردن و اکسپلویت انواع مشکلات امنیتی.
موضوع:اینترنت–تدابیر ایمنی
موضوع:internet-security measures
موضوع:کامپیوترها–ایمنی اطلاعات
موضوع:computer security
شناسه افزوده:پینتو،مارکوس،۱۹۷۸–م
شناسه افزوده:Pinto,Marcus,1978
شناسه افزوده:طالبی،علیرضا،۱۳۶۰–مترجم
رده بندی کنگره:TK ۵۱۰۵/۸۷۵
رده بندی دیویی:۰۰۵/۸
شماره کتابشناسی ملی:۹۴۳۸۵۳۰

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

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 ۳

فناوری‌های کاربردی وب ۵۴

فصل ۴

فصل ۵

فصل ۶

فصل ۷

فصل ۸

فصل ۱۰

فصل ۱۱

مقدمه ناشر

خط مشی انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب هایی با کیفیت عالی 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 و آموزشی گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گستردگی علوم وسرعت 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 زمینه های گوناگون و مورد نیاز جامعه تلاش نموده برای رفع کمبودها و نیازهای موجود، منابعی پُربار، 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 منتشرگشته و شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

با نظرات خود مشوق و راهنمای ما باشید

با ارائه نظرات و پیشنهادات وخواسته های خود،به ما کمک کنید تا بهتر و دقیق تر در جهت رفع نیازهای علمی و آموزشی کشورمان قدم برداریم.برای رساندن پیام هایتان به ما از رسانه های دیباگران تهران شامل سایتهای فروشگاهی و صفحه اینستاگرام و شماره های تماس که در صفحه شناسنامه کتاب آمده استفاده نمایید.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
dibagaran@mftplus.com

مقدمه

این کتاب راهنمای عملی برای کشف و بهره‌برداری از نواقص امنیتی در برنامه‌های کاربردی وب است. منظور ما از «برنامه‌های وب» برنامه‌هایی است که با استفاده از یک مرورگر وب برای ارتباط با یک وب سرور به آن‌ها دسترسی پیدا می‌کنند. ما طیف گسترده‌ای از فناوری‌های مختلف، مانند پایگاه‌های داده، سیستم‌های فایل و سرویس‌های وب را بررسی می‌کنیم، اما فقط در زمینه‌ای که این فناوری‌ها توسط برنامه‌های کاربردی وب استفاده می‌شوند.

اگر می‌خواهید بدانید که چگونه از نفوذ مهاجمان به برنامه وب، از سرقت داده‌های حساس و اقدامات غیرمجاز جلوگیری کنید، این کتاب برای شما مناسب است.

مروری بر این کتاب

تمرکز این کتاب بسیار کاربردی است. اگرچه ما پیشینه و تئوری کافی برای درک آسیب‌پذیری‌های برنامه‌های کاربردی وب را برای شما گنجانده‌ایم، اما نگرانی اصلی ما وظایف و تکنیک‌هایی است که برای شکستن آن‌ها باید تسلط داشته باشید. در سرتاسر کتاب، مراحل خاصی که باید برای شناسایی هرنوع آسیب‌پذیری دنبال کنید و نحوه استفاده از آن برای انجام اقدامات غیرمجاز را توضیح می‌دهیم. ما همچنین تعداد زیادی نمونه از دنیای واقعی که از تجربه چندین‌ساله به‌دست آمده است و اینکه چگونه انواع مختلف نقص‌های امنیتی در برنامه‌های کاربردی وب امروزی خود را نشان می‌دهند، خواهیم آورد.

آگاهی امنیتی معمولاً یک شمشیر دولبه است. همان‌طور که توسعه‌دهندگان برنامه‌ها می‌توانند از درک روش‌هایی که مهاجمان استفاده می‌کنند سود ببرند، هکرها نیز می‌توانند از دانستن اینکه چگونه برنامه‌ها می‌توانند به طور مؤثر از خود دفاع کنند، سود ببرند. علاوه‌بر تشریح آسیب‌پذیری‌های امنیتی و تکنیک‌های حمله، اقدامات متقابلی را که برنامه‌ها می‌توانند برای خنثی کردن یک مهاجم انجام دهند، به تفصیل شرح می‌دهیم. اگر آزمایش‌های نفوذ برنامه‌های تحت وب را انجام دهید، به شما این امکان را می‌دهد تا توصیه‌های اصلاحی با کیفیت بالا را به صاحبان برنامه‌هایی که در مخاطرات امنیتی هستند، ارائه دهید.

چه کسی باید این کتاب را بخواند

مخاطب اصلی این کتاب هرکسی است که به حمله به برنامه‌های کاربردی وب، علاقه شخصی یا حرفه‌ای دارد. همچنین برای هر کسی که مسئول توسعه و مدیریت برنامه‌های کاربردی وب است. دانستن نحوه عملکرد دشمنان به شما کمک می‌کند در برابر آن‌ها دفاع کنید.

ما فرض می‌کنیم که شما با مفاهیم اصلی امنیتی مانند ورود به سیستم و کنترل‌های دسترسی آشنا هستید و از فناوری‌های اصلی وب مانند مرورگرها، سرورهای وب و HTTP آگاهی دارید. با این حال، هرگونه شکاف در دانش فعلی شما در این زمینه‌ها، ازطریق توضیحات موجود در این کتاب و یا ارجاعات در جاهای دیگر، به‌راحتی قابل رفع خواهد بود.

در طول نمایش بسیاری از دسته‌بندی‌های نقص‌های امنیتی، کدهایی را ارائه می‌کنیم که نشان می‌دهد چگونه برنامه‌ها می‌توانند آسیب‌پذیر باشند. این مثال‌ها به اندازه کافی ساده هستند که می‌توانید بدون دانش قبلی از زبان موردنظر آن‌ها را درک کنید. اما اگر تجربه اولیه در خواندن یا نوشتن کد داشته باشید، بسیار مفید هستند.

این کتاب چگونه سازماندهی شده است

این کتاب تقریباً مطابق با وابستگی‌های بین موضوعات مختلف تحت پوشش سازماندهی شده است. اگر در زمینه هک برنامه‌های وب تازه‌کار هستید، باید کتاب را از ابتدا تا انتها بخوانید و دانش و درک لازم برای مقابله با فصل‌های بعدی را به‌دست آورید. اگر قبلاً در این زمینه تجربه دارید، می‌توانید مستقیماً به هر فصل یا زیربخشی که مخصوصاً برای شما جالب است بروید. درصورت لزوم، ما ارجاعات متقابلی را به فصول دیگر اضافه کرده‌ایم که می‌توانید از آن‌ها برای پر کردن هر شکافی در درک خود استفاده کنید.

ما با سه فصل تنظیم زمینه شروع می‌کنیم که وضعیت فعلی امنیت برنامه‌های کاربردی وب و روندهایی که نشان می‌دهد چگونه در آینده نزدیک ممکن است تکامل یابد را توصیف خواهیم کرد. همچنین مشکل اصلی امنیتی مؤثر بر برنامه‌های کاربردی وب و مکانیسم‌های دفاعی که برنامه‌ها برای رفع این مشکل پیاده‌سازی می‌کنند را بررسی می‌کنیم. درمورد فناوری‌های کلیدی مورداستفاده در برنامه‌های کاربردی وب امروزی نیز راهکارهایی ارائه می‌دهیم.

بخش عمده‌ای از کتاب به موضوع اصلی ما مربوط می‌شود؛ تکنیک‌هایی که می‌توانید برای نفوذ به برنامه‌های وب استفاده کنید. این مطالب حول وظایف کلیدی که برای انجام یک حمله جامع باید انجام دهید، سازماندهی شده است. این‌ها شامل نقشه‌برداری از عملکرد برنامه، بررسی دقیق و حمله به مکانیسم‌های دفاعی اصلی آن و بررسی دسته‌های خاصی از نقص‌های امنیتی است.

◄ مقدمه

در این کتاب ما فرآیند یافتن آسیب‌پذیری‌ها در سورس کدبرنامه را توضیح می‌دهیم، ابزارهایی که می‌توانند در هنگام هک برنامه‌های وب به شما کمک کنند را مرور می‌کنیم و یک روش دقیق برای انجام یک حمله جامع و عمیق علیه یک هدف خاص ارائه می‌کنیم.

فصل ۱، «امنیت برنامه‌های وب»، وضعیت فعلی امنیت در برنامه‌های کاربردی وب در اینترنت را توصیف می‌کند. باوجود تضمین‌های رایج، اکثر برنامه‌ها ناامن هستند و می‌توانند به سینتسکی با درجه متوسطی از مهارت در معرض خطر قرار گیرند. آسیب‌پذیری‌ها در برنامه‌های کاربردی وب به‌دلیل یک مشکل اصلی ایجاد می‌شوند: کاربران می‌توانند ورودی دلخواه را ارسال کنند. این فصل به بررسی عوامل کلیدی می‌پردازد که در وضعیت امنیتی ضعیف برنامه‌های امروزی نقش دارند. همچنین توضیح می‌دهد که چگونه نقص در برنامه‌های کاربردی وب می‌تواند زیرساخت فنی گسترده‌تر یک سازمان را در برابر حمله بسیار آسیب‌پذیر کند.

فصل ۲، «مکانیسم‌های دفاعی اصلی»، مکانیسم‌های امنیتی کلیدی که برنامه‌های کاربردی وب برای رسیدگی به مشکل اساسی، که همه ورودی‌های کاربر غیرقابل اعتماد هستند، به کار می‌گیرند را توضیح می‌دهد. این مکانیسم‌ها ابزاری هستند که ازطریق آن‌ها یک برنامه کاربردی دسترسی کاربر را مدیریت می‌کند، ورودی

کاربر را مدیریت می‌کند و به مهاجمان پاسخ می‌دهد. این مکانیسم‌ها همچنین شامل توابع ارائه‌شده برای مدیران به‌منظور مدیریت و نظارت بر خود برنامه است. مکانیسم‌های امنیتی اصلی برنامه همچنین سطح حمله اولیه آن را نشان می‌دهند، بنابراین قبل از اینکه بتوانید به‌طور مؤثر به آن‌ها حمله کنید، باید بدانید که این مکانیسم‌ها چگونه کار می‌کنند.

فصل ۳، «تکنولوژی‌های برنامه‌های وب»، آغازگر کوتاهی درمورد فناوری‌های کلیدی است که احتمالاً هنگام حمله به برنامه‌های وب با آن‌ها روبه‌رو خواهید شد. تمام جنبه‌های مرتبط پروتکل HTTP، فناوری‌هایی که معمولاً در سمت مشتری و سرور استفاده می‌شوند و طرح‌های مختلفی که برای رمزگذاری داده‌ها استفاده می‌شوند را پوشش می‌دهد. اگر از قبل با فناوری‌های اصلی وب آشنا هستید، می‌توانید این فصل را مرور کنید.

فصل ۴، «نقشه‌برداری از برنامه»، اولین تمرینی که باید هنگام هدف قرار دادن یک برنامه جدید انجام دهید را توصیف می‌کند. جمع‌آوری اطلاعات تاحد امکان برای نقشه‌برداری از سطح حمله آن و تدوین برنامه حمله خود. این فرآیند شامل کاوش و بررسی برنامه برای فهرست کردن تمام محتوا و عملکرد آن، شناسایی تمام نقاط ورودی برای ورودی کاربر و کشف فناوری‌های درحال استفاده است.

فصل ۵، «دور زدن کنترل‌های سمت کلاینت»، اولین ناحیه آسیب‌پذیری واقعی را پوشش می‌دهد و زمانی ایجاد می‌شود که یک برنامه برای امنیت خود به کنترل‌های پیاده‌سازی‌شده در سمت کلاینت متکی باشد. این رویکرد معمولاً شگفت‌انگیز است؛ زیرا هر کنترل سمت مشتری را می‌توان دور زد. دو روش اصلی که در آن برنامه‌ها خود را آسیب‌پذیر می‌کنند، انتقال داده‌ها ازطریق کلاینت با این فرض که اصلاح نمی‌شوند و با تکیه بر بررسی‌های سمت مشتری در ورودی کاربر است. این فصل طیف وسیعی از فناوری‌های جالب را توصیف می‌کند؛ ازجمله کنترل‌های سبک‌وزنی که در HTML، HTTP، و جاوا اسکریپت پیاده‌سازی شده‌اند، و کنترل‌های سنگین‌تر با استفاده از اپلت‌های جاوا، کنترل‌های ActiveX، Silverlight و اشیایFlash.

فصل‌های ۶، ۷ و ۸ برخی از مهم‌ترین مکانیسم‌های دفاعی پیاده‌سازی‌شده در برنامه‌های کاربردی وب را پوشش می‌دهند: کسانی که مسئول کنترل دسترسی کاربر هستند. فصل ۶، «حمله تأیید هویت»، عملکردهای مختلفی را بررسی می‌کند که توسط آن‌ها برنامه‌ها از هویت کاربران خود اطمینان حاصل می‌کنند که شامل عملکرد ورود به سیستم اصلی و همچنین عملکردهای مرتبط با احراز هویت جانبی مانند ثبت نام کاربر، تغییر رمز عبور و بازیابی حساب می‌شود. مکانیسم‌های احراز هویت شامل انبوهی از آسیب‌پذیری‌های مختلف، هم در طراحی و هم در پیاده‌سازی هستند که مهاجم می‌تواند از آن‌ها برای دسترسی غیرمجاز استفاده کند. این موارد از عیوب آشکار، مانند رمزهای عبور بد و حساسیت به حملات brute-force، تا مشکلات مبهم‌تر در منطق احراز هویت را شامل می‌شود. ما همچنین انواع مکانیسم‌های ورود چندمرحله‌ای که در بسیاری از برنامه‌های کاربردی حیاتی امنیتی مورد استفاده قرار می‌گیرند را به تفصیل بررسی می‌کنیم و انواع جدیدی از آسیب‌پذیری‌ها که اغلب شامل آن‌ها هستند را توصیف می‌کنیم.

فصل ۷، «حمله مدیریت جلسه»، مکانیسمی را بررسی می‌کند که توسط آن اکثر برنامه‌ها پروتکل HTTP بدون حالت را با مفهوم یک جلسه حالت تکمیل می‌کنند و آن‌ها را قادر می‌سازد تا هر کاربر را در چندین درخواست مختلف به‌طور منحصربه‌فرد شناسایی کنند. این مکانیسم زمانی که به یک برنامه وب حمله می‌کنید،

یک هدف کلیدی است؛ زیرا اگر بتوانید آن را شکست دهید، می‌توانید به‌طور مؤثری از ورود به سیستم عبور کنید و مانند سایر کاربران بدون اطلاع از اعتبار آن‌ها، ظاهر شوید. ما به نقایص مختلف رایج در تولید و انتقال نشانه‌های جلسه نگاه می‌کنیم و مراحلی که می‌توانید برای کشف و بهره‌برداری از آن‌ها بردارید را شرح می‌دهیم.

فصل ۸، «حمله به کنترل‌های دسترسی»، به روش‌هایی می‌پردازد که برنامه‌ها درواقع کنترل‌های دسترسی را با تکیه بر مکانیسم‌های احراز هویت و مدیریت جلسه برای انجام این کار، اعمال می‌کنند. ما روش‌های مختلفی را توضیح می‌دهیم که کنترل‌های دسترسی می‌توانند ازطریق آن‌ها شکسته شده و اینکه چگونه می‌توانید این نقاط ضعف را شناسایی و از آن‌ها استفاده کنید.

فصل‌های ۹ و ۱۰ دسته بزرگی از آسیب‌پذیری‌های مرتبط را پوشش می‌دهند، زمانی به‌وجود می‌آیند که برنامه‌ها ورودی کاربر را به روشی ناامن در کد تفسیرشده قرار می‌دهند. فصل ۹، «حمله به فروشگاه‌های داده»، با بررسی دقیق آسیب‌پذیری‌های تزریق SQL آغاز می‌شود. این طیف وسیعی از حملات را پوشش می‌دهد، از واضح‌ترین و بی‌اهمیت‌ترین تا تکنیک‌های بهره‌برداری پیشرفته که شامل کانال‌های خارج از باند، استنتاج و تأخیرهای زمانی است. برای هرنوع آسیب‌پذیری و تکنیک حمله، تفاوت‌های مربوطه بین سه نوع رایج پایگاه داده را شرح می‌دهیم: MS-SQL، Oracle و MySQL. سپس به طیف وسیعی از حملات مشابه که علیه سایر ذخیره‌گاه‌های داده ازجمله NoSQL، XPath و LDAP رخ می‌دهند، نگاه می‌کنیم.

فصل ۱۰، «حمله به اجزای Back-End»، چندین دسته دیگر از آسیب‌پذیری‌های تزریق را توصیف می‌کند؛ ازجمله تزریق دستورهای سیستم عامل، تزریق به زبان‌های برنامه‌نویسی وب، حملات پیمایش مسیر فایل، آسیب‌پذیری‌های گنجاندن فایل، تزریق به XML، SOAP، درخواست‌های HTTP پشتیبان و خدمات ایمیل.

فصل ۱۱، «حمله به منطق برنامه»، یک منطقه مهم و اغلب نادیده گرفته‌شده از سطح حمله هر برنامه را بررسی می‌کند: منطق داخلی که برای اجرای عملکرد خود استفاده می‌کند. نقص در منطق برنامه بسیار متنوع است و تشخیص آن سخت‌تر از آسیب‌پذیری‌های رایج است.

مانند SQL injection و cross-site scripting به‌همین دلیل، ما مجموعه‌ای از نمونه‌های واقعی را ارائه می‌کنیم که در آن‌ها منطق معیوب، یک برنامه را آسیب‌پذیر کرده است. این‌ها تنوع مفروضات معیوبی که طراحان و توسعه‌دهندگان برنامه‌ها مطرح می‌کنند را نشان می‌دهد. از این آسیب‌های فردی مختلف، ما یک‌سری آزمایش‌های مشخص را استخراج می‌کنیم که می‌توانید برای پیدا کردن انواع بسیاری از معایب منطقی که اغلب شناسایی نمی‌شوند، انجام دهید.

فصل‌های ۱۲ و ۱۳ یک منطقه بزرگ و بسیار موضوعی از آسیب‌پذیری‌های مرتبط را پوشش می‌دهند، این آسیب‌پذیری‌ها زمانی به‌وجود می‌آیند که نقص در یک برنامه وب می‌تواند کاربر مخرب برنامه را قادر سازد تا به سایر کاربران حمله کند و آن‌ها را به روش‌های مختلف در معرض خطر قرار دهد. فصل ۱۲، «حمله به کاربران: اسکریپت بین سایتی»، برجسته‌ترین آسیب‌پذیری از این نوع را بررسی می‌کند؛ آسیب‌پذیری بسیار شایعی که بر اکثریت قریب به اتفاق برنامه‌های کاربردی وب در اینترنت تأثیر می‌گذارد. ما به‌طور مفصل تمام اشکال مختلف آسیب‌پذیری‌های XSS را بررسی می‌کنیم و یک روش مؤثر برای شناسایی و بهره‌برداری حتی مبهم‌ترین ترافیک‌های این آسیب‌پذیری‌ها را توصیف می‌کنیم.

فصل ۱۳، «حمله به کاربران: تکنیک‌های دیگر»، به چندین نوع دیگر از حملات علیه سایر کاربران، ازجمله القای اقدامات کاربر ازطریق جعل درخواست و اصلاح رابط کاربری، گرفتن داده‌ها از دامنه‌های متقابل با استفاده از فناوری‌های مختلف سمت مشتری، حملات مختلف علیه همان‌ها می‌پردازد. سیاست مبدأ، تزریق هدر HTTP، تزریق کوکی و رفع جلسه، تغییر مسیر باز، تزریق SQL سمت مشتری، حملات حریم خصوصی محلی، و سوءاستفاده از اشکالات در کنترل‌های ActiveX. این فصل با بحث درمورد طیف وسیعی از حملات علیه کاربران به پایان می‌رسد که به آسیب‌پذیری‌های هیچ برنامه وب خاصی وابسته نیستند، اما می‌توانند ازطریق هر وب‌سایت مخرب یا مهاجمی که موقعیت مناسبی دارند، ارائه شوند.

فصل ۱۴، «حملات سفارشی‌شده اتوماتیک»، هیچ دسته جدیدی از آسیب‌پذیری‌ها را معرفی نمی‌کند. درعوض، تکنیک مهمی را توصیف می‌کند که برای حمله مؤثر به برنامه‌های کاربردی وب باید در آن مهارت داشته باشید. از آنجایی که هر برنامه وب متفاوت است، اکثر حملات به روشی سفارشی می‌شوند و براساس رفتار خاص برنامه و روش‌هایی که برای دستکاری آن به نفع خود کشف کرده‌اید، تنظیم می‌شوند. آن‌ها همچنین اغلب نیاز به صدور تعداد زیادی درخواست مشابه و نظارت بر پاسخ‌های برنامه دارند. انجام این درخواست‌ها به‌صورت دستی بسیار پرزحمت و مستعد اشتباه است. برای جلوگیری از هک برنامه وب، باید تا آنجا که ممکن است این کار را خودکار کنید تا با حملات سفارشی سریع‌تر و مؤثرتر مقابله کنید. این فصل به تفصیل یک روش اثبات‌شده برای دستیابی به این را شرح می‌دهد. ما همچنین موانع مختلف رایج برای استفاده از اتوماسیون را بررسی می‌کنیم؛ ازجمله مکانیسم‌های مدیریت جلسه دفاعی و کنترل‌های CAPTCHA. علاوه‌بر این، ما ابزارها و تکنیک‌هایی را توضیح می‌دهیم که می‌توانید برای غلبه بر این موانع از آن‌ها استفاده کنید.

فصل ۱۵، «بهره‌برداری از افشای اطلاعات»، راه‌های مختلفی را بررسی می‌کند که در آن برنامه‌ها هنگام حمله فعال، اطلاعات را درز می‌کنند. هنگامی که انواع دیگر حملاتی که در این کتاب توضیح داده شده است را انجام می‌دهید، همیشه باید برنامه را زیرنظر داشته باشید تا منابع بیشتری از افشای اطلاعات را شناسایی کنید که می‌توان از آن‌ها سوءاستفاده کرد. توضیح می‌دهیم که چگونه می‌توانید رفتارهای غیرعادی و پیام‌های خطا را بررسی کنید تا درک عمیق‌تری از برنامه کاربردی به‌دست آورید.

ما همچنین راه‌هایی برای دستکاری مدیریت خطای معیوب برای بازیابی سیستماتیک اطلاعات حساس از برنامه را پوشش می‌دهیم.

فصل ۱۶، «حمله به برنامه‌های کامپایل‌شده بومی»، به مجموعه‌ای از آسیب‌پذیری‌های مهم می‌پردازد.

مواردی که در برنامه‌های کاربردی نوشته شده به زبان‌های کد بومی مانند C و C++ ایجاد می‌شوند. این آسیب‌پذیری‌ها عبارت‌اند از: سرریزهای بافر، آسیب‌پذیری‌های عدد صحیح، و اشکال رشته‌ای قالب‌بندی. از آنجایی که این یک موضوع بالقوه بزرگ است، ما برروی راه‌هایی برای شناسایی این آسیب‌پذیری‌ها در برنامه‌های کاربردی وب تمرکز می‌کنیم و به نمونه‌های واقعی از نحوه ظهور و بهره‌برداری از این آسیب‌پذیری‌ها نگاه می‌کنیم.

فصل ۱۷، «حمله به معماری برنامه»، حوزه مهمی از امنیت برنامه‌های کاربردی وب را بررسی می‌کند که اغلب نادیده گرفته می‌شود. بسیاری از برنامه‌ها از معماری لایه‌ای استفاده می‌کنند. ناتوانی در تفکیک صحیح

لایه‌های مختلف، اغلب یک برنامه را آسیب‌پذیر می‌کند و مهاجمی که نقصی در یک مؤلفه پیدا کرده است را قادر می‌سازد تا به سرعت کل برنامه را در معرض خطر قرار دهد. طیف متفاوتی از تهدیدات در محیط‌های میزبانی مشترک ایجاد می‌شود، جایی که نقص یا کد مخرب در یک برنامه گاهی اوقات می‌تواند برای به خطر انداختن خود محیط و سایر برنامه‌های درحال اجرا در آن مورد سوءاستفاده قرار گیرد. این فصل همچنین به طیف وسیعی از تهدیداتی می‌پردازد که در انواع محیط‌های میزبانی مشترک که به‌عنوان «رایانش ابری» شناخته می‌شوند، ایجاد شود.

فصل ۱۸، «حمله به سرور برنامه»، روش‌های مختلفی را توضیح می‌دهد که ازطریق آن‌ها می‌توانید یک برنامه وب را با هدف قرار دادن وب سروری که روی آن اجرا می‌شود، هدف قرار دهید. آسیب‌پذیری‌ها در وب سرورها به‌طور گسترده از نقص در پیکربندی و نقص‌های امنیتی در نرم‌افزار وب سرور تشکیل شده است. این موضوع در مرز موضوعاتی است که در این کتاب پوشش داده شده است؛ زیرا وب سرور کاملاً یک جزء متفاوت در پشته فناوری است. با این حال، اکثر برنامه‌های کاربردی وب به‌طور نزدیک به وب سروری که روی آن اجرا می‌شوند، متصل هستند. بنابراین، حملات علیه وب سرور در کتاب گنجانده شده است؛ زیرا اغلب می‌توان از آن‌ها برای به خطر انداختن یک برنامه به‌طور مستقیم استفاده کرد، نه اینکه به‌طور غیرمستقیم ابتدا میزبان اصلی را در معرض خطر قرار دهد.

فصل ۱۹، «یافتن آسیب‌پذیری‌ها در کد منبع»، رویکرد کاملاً متفاوتی را برای یافتن نقص‌های امنیتی با آنچه در جاهای دیگر این کتاب توضیح داده شده است، توصیف می‌کند. در بسیاری از شرایط ممکن است بتوان سورس کدبرنامه را بررسی کرد که همه آن‌ها نیاز به همکاری مالک برنامه ندارند. بررسی سورس کدیک برنامه اغلب می‌تواند در کشف آسیب‌پذیری‌هایی که شناسایی آن‌ها با بررسی برنامه درحال اجرا دشوار یا زمان‌بر است، بسیار مؤثر باشد. ما یک متدولوژی را توصیف می‌کنیم و یک برگه زبان ارائه می‌دهیم تا شما را قادر سازد حتی اگر تجربه برنامه‌نویسی محدودی دارید، بازبینی کد مؤثری انجام دهید.

فصل ۲۰، «مجموعه ابزار هکر برنامه وب»، ابزارهای مختلفی که در این کتاب توضیح داده شده است را گرد هم می‌آورد. این‌ها همان ابزارهایی هستند که نویسندگان هنگام حمله به برنامه‌های کاربردی وب در دنیای واقعی استفاده می‌کنند. ما ویژگی‌های کلیدی این ابزارها را بررسی می‌کنیم و نوع جریان کاری که عموماً برای استفاده از آن‌ها به بهترین شکل نیاز دارید را به تفصیل شرح می‌دهیم. همچنین بررسی می‌کنیم که هر ابزار کاملاً خودکار تا چه حد می‌تواند در یافتن آسیب‌پذیری‌های برنامه وب مؤثر باشد. درنهایت، نکات و توصیه‌هایی را برای استفاده حداکثری از جعبه ابزار خود ارائه می‌دهیم.

فصل ۲۱، «روش‌شناسی هکر برنامه‌های وب»، مجموعه‌ای جامع و ساختاریافته از تمام رویه‌ها و تکنیک‌های توصیف‌شده در این کتاب است. این‌ها براساس وابستگی‌های منطقی بین وظایف زمانی که شما درحال انجام یک حمله واقعی هستید، سازماندهی و مرتب می‌شوند. اگر تمام آسیب‌پذیری‌ها و تکنیک‌های شرح داده‌شده در این کتاب را خوانده‌اید و متوجه شده‌اید، می‌توانید از این روش به‌عنوان یک چک لیست کامل و برنامه کاری در هنگام توقف انجام حمله علیه یک برنامه وب استفاده کنید.

آنچه در این نسخه جدید است

زمانی که این کتاب را می‌خوانید، خیلی چیزها تغییر کرده و خیلی‌ها ثابت مانده‌اند. البته حرکت فناوری جدید به‌سرعت ادامه داشته است و این باعث ایجاد آسیب‌پذیری‌ها و حملات جدید شده است. نبوغ هکرها همچنین منجربه توسعه تکنیک‌های حمله جدید و روش‌های جدیدی برای بهره‌برداری از باگ‌های قدیمی شده است. اما هیچ‌یک از این عوامل، چه تکنولوژی و چه انسانی، انقلابی ایجاد نکرده است. فناوری‌های مورداستفاده در برنامه‌های امروزی ریشه در فناوری‌هایی دارد که سال‌ها قدمت دارند و مفاهیم اساسی درگیر در تکنیک‌های بهره‌برداری پیشرفته امروزی قدیمی‌تر از بسیاری از محققانی است که آن‌ها را به‌طور مؤثر به‌کار می‌برند. امنیت برنامه‌های کاربردی وب یک حوزه پویا و هیجان‌انگیز برای کار است، اما بخش عمده‌ای از دانش انباشته‌شده ما طی سال‌ها به کندی تکامل یافته است. برای تمرین‌کنندگانی که یک دهه یا بیشتر کار می‌کردند، به‌طور مشخصی قابل تشخیص بود.

بیشتر این مطالب برای امروز معتبر و جاری هستند. می‌توانید روی چیزهای جدید در این نسخه تمرکز کنید و به‌سرعت درمورد حوزه‌های امنیت برنامه‌های وب که در سال‌های اخیر تغییر کرده‌اند یاد بگیرید.

یکی از ویژگی‌های مهم جدید گنجاندن نمونه‌های واقعی تقریباً تمام آسیب‌پذیری‌های پوشش‌دهی‌شده در سراسر کتاب است. هرجا که «امتحانش کن!» را دیدی! می‌توانید آنلاین شوید و با مثال مورد بحث به‌صورت تعاملی کار کنید تا تأیید کنید که می‌توانید آسیب‌پذیری موجود در آن را پیدا و از آن بهره‌برداری کنید. چندصد مورد از این آزمایشگاه‌ها وجود دارد که می‌توانید در حین خواندن کتاب، با سرعت دلخواه از آن‌ها کار کنید. آزمایشگاه‌های آنلاین به‌صورت اشتراک با هزینه‌ای اندک در دسترس هستند تا هزینه‌های میزبانی و نگهداری زیرساخت‌های مربوطه را پوشش دهند.

ابزارهایی که به آن‌ها نیاز خواهید داشت

این کتاب به‌شدت به‌سمت تکنیک‌های عملی درحال حرکت است و می‌توانید برای حمله به برنامه‌های کاربردی وب از آن‌ها استفاده کنید. پس از خواندن کتاب، خواهید فهمید که ویژگی‌های هر کار جداگانه، چه چیزی را شامل می‌شود و چرا به شما کمک می‌کند آسیب‌پذیری‌ها را شناسایی و از آن‌ها بهره‌برداری کنید. این کتاب به‌طور قاطع درباره دانلود یک ابزار، نشان دادن آن به‌سمت یک برنامه هدف و باور آنچه که خروجی ابزار درمورد وضعیت امنیت برنامه به شما می‌گوید، نیست.

با این حال، هنگام انجام وظایف و تکنیک‌هایی که توضیح می‌دهیم، چندین ابزار مفید و گاهی ضروری پیدا خواهید کرد. همه این‌ها در اینترنت موجود است. توصیه می‌کنیم در حین مطالعه هر ابزاری را دانلود کرده و با آن آزمایش کنید.

◄ آنچه در وب‌سایت است

وب‌سایت همراه این کتاب حاوی منابع متعددی است که در دوره تسلط بر تکنیک‌ها مفید خواهند بود. ما آن‌ها را برای حمله به برنامه‌های واقعی توصیف و از آن‌ها استفاده می‌کنیم. به‌طور خاص، وب‌سایت شامل دسترسی به موارد زیر است:

- سورس کد برای برخی از اسکریپت‌هایی که در کتاب ارائه می‌کنیم؛
- فهرستی از پیوندهای فعلی به تمام ابزارها و سایر منابع مورد بحث در کتاب؛
- چک‌لیست مفیدی از وظایف مربوط به جلوگیری از حمله، به یک برنامه معمولی؛
- پاسخ به سؤالات مطرح‌شده در پایان هر فصل؛
- صدها آزمایشگاه آسیب‌پذیری تعاملی که در نمونه‌هایی در سراسر این کتاب استفاده می‌شوند و به‌صورت اشتراک در دسترس هستند تا به شما در توسعه و اصلاح مهارت‌های‌تان کمک کنند.

امنیت برنامه‌های کاربردی وب همچنان یک موضوع سرگرم‌کننده و پررونق است. امیدواریم که شما نیز از یادگیری تکنیک‌های مختلفی که توضیح می‌دهیم و نحوه دفاع در برابر آن‌ها لذت ببرید.

قبل از اینکه به ادامه مطلب برویم، باید به یک نکته مهم اشاره کنیم. در بیشتر کشورها، حمله به سیستم‌های کامپیوتری بدون اجازه مالک خلاف قانون است. اکثر تکنیک‌هایی که توضیح می‌دهیم اگر بدون رضایت انجام شوند، غیرقانونی هستند.

نویسندگان، تسترهای نفوذ حرفه‌ای هستند که به‌طور معمول ازطرف مشتریان به برنامه‌های کاربردی وب حمله می‌کنند تا به آن‌ها کمک کنند امنیت خود را بهبود بخشند. در سال‌های اخیر، بسیاری از متخصصان امنیتی و سایرین با آزمایش یا حمله فعال برروی سیستم‌های رایانه‌ای بدون اجازه، سوابق جنایی را به‌دست آورده‌اند و به کار خود پایان داده‌اند. ما از شما می‌خواهیم که از اطلاعات موجود در این کتاب فقط برای مقاصد قانونی استفاده کنید.