



الفبای امنیت وب در سمت کاربر

تألیف:

لیون دزمت

فیلیپ دیریک

مارتین جان

فرانک پیسنز

ترجمه:

مهندس راضیه اسکندری

دکتر مریم موزرانی

عنوان و نام پدیدآور:	الفبای امنیت وب در سمت کاربر / تألیف فیلیپ دیریک ... (و دیگران)؛ ترجمه راضیه اسکندری، مریم موزرانی.
مشخصات نشر:	شهرکرد: دانشگاه شهرکرد، ۱۳۹۸.
مشخصات ظاهری:	۲۱۹ ص:، مصور، جدول، نمودار.
شابک:	۹۷۸-۹۶۴-۹۰۹۳۲-۷-۷
یادداشت:	عنوان اصلی: Primer on client-side web security, 2014.
یادداشت:	تألیف فیلیپ دیریک، لیون دزمت، فرانک پیسنز، مارتین جان.
یادداشت:	واژه‌نامه.
موضوع:	کامپیوترها -- ایمنی اطلاعات
موضوع:	Computer security
موضوع:	کامپیوترهای سرویس دهنده و سرویس گیرنده
موضوع:	Client/server computing
موضوع:	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع:	Computer networks -- Security measures
موضوع:	وب
موضوع:	World Wide Web
موضوع:	فیلیپ دیریک
موضوع:	De Ryck, Philippe
موضوع:	دیریک، فیلیپ، راف. ۱۳۶۴ - مترجم
موضوع:	موزرانی، مریم، ۱۳۶۴ - مترجم
موضوع:	دانشگاه شهرکرد
موضوع:	۸ ۷۶/۹
موضوع:	۰۰۵/۸
موضوع:	۵۷۲۴۴۷۲
موضوع:	شماره کتابشناسی ملی:



انتشارات دانشگاه شهرکرد

نام کتاب:	الفبای امنیت وب در سمت کاربر
تألیف:	فیلیپ دیریک، لیون دزمت، فرانک پیسنز، مارتین جان
ترجمه:	راضیه اسکندری، مریم موزرانی
ویراستار ادبی:	ابراهیم ظاهری عبدهوند
ناشر:	دانشگاه شهرکرد
امور فنی و اجرایی:	فاطمه قانی
چاپ اول:	بهار ۱۳۹۸
تیراژ:	۵۰۰ نسخه
قطع:	وزیری
چاپ:	گاندی
قیمت:	۵۵۰۰۰۰ ریال
شابک:	۹۷۸-۹۶۴-۹۰۹۳۲-۷-۷

کلیه حقوق این اثر برای نویسندگان و دانشگاه شهرکرد محفوظ است.
نشانی: چهارمحال و بختیاری، شهرکرد، بلوار رهبر، انتشارات دانشگاه شهرکرد، صندوق پستی ۱۱۵.

پیش‌گفتار مؤلفان

آیا تاکنون اندیشیده‌اید که چرا کاربران عادی به‌صورت ناگهانی شروع به فرستادن پیام‌های عجیب و غریب در شبکه‌های اجتماعی می‌کنند؟ چگونه مسیر یاب‌های بی‌سیم از راه دور می‌توانند کنترل شوند؟ چرا حساب eBay می‌تواند با یک درخواست HTTP ربوده شود؟ یا چرا یک وب‌سایت خبری به‌طور ناگهانی صفحه‌ای از ارتش الکترونیک سوریه را نشان می‌دهد؟ همه این حوادث، به دلیل کنترل برخی از کدهای درون مرورگر قربانی توسط یک مهاجم، شذنی هستند. این امر نتیجه وضعیت فعلی امنیت وب است. به دنبال پژوهشگران امنیت، ما با شکاف بزرگی بین وضعیت فعلی فن‌آوری‌های امنیت و آنچه در حال حاضر در دسترس است، مواجه هستیم؛ بنابراین این کتاب را برای بهبود این وضعیت، نوشته‌ایم تا دید دقیقی درباره چشم‌انداز امنیت وب سمت کاربر فراهم شود. به راحتی روی آسیب‌پذیری‌های امنیتی سمت کاربر متمرکز می‌شویم؛ آسیب‌پذیری‌هایی که از درون یک مرورگر نشأت می‌گیرند یا به‌صورت صریح مرورگر را برای سوءاستفاده هدف قرار داده‌اند، چرا که به این آسیب‌پذیری‌های سمت کاربر، در حالت کلی در مقایسه با هم‌تایان سمت کارگزار، توجه کمتری شده است. در مجموع سیزده حمله را بررسی کرده‌ایم. برای هر یک شرحی به‌صورت مفصل داده‌ایم. سپس مروری کلی بر تکنیک‌های قدیمی و جدیدی از حملات و وضعیت فعلی پژوهش‌ها خواهیم داشت. در هر حمله، وضعیت فعلی آن را در برنامه‌های وب توصیف و بهترین شیوه دفاع را در برابر این حملات در عصر مدرن بیان کرده‌ایم.

این کتاب با در نظر گرفتن چندین مخاطب هدف نوشته شده است: در مرحله اول، برای دانش‌آموزان، معلمان و مربیان؛ این کتاب شامل مقدمه‌ای در زمینه امنیت وب سمت کاربر، به همراه فهرستی از منابع گسترده برای یادگیری بیشتر در مورد هر موضوع است. از قسمت بهترین تجربه‌های عملی، می‌توان به عنوان مواد آموزشی برای دوره‌های توسعه نرم‌افزار امن استفاده کرد. این کتاب، به پژوهشگران کمک می‌کند تا آن‌ها در این زمینه، به سرعت پیشرفت کنند. همچنین این کتاب، یک نمای کلی از وضعیت فعلی را برای پژوهشگران باتجربه‌ای که به دنبال فرصت‌های جدید برای کشف هستند، فراهم

می‌کند. در نهایت توسعه‌دهندگان و دست‌اندرکاران امنیتی یک نمای کلی از وضعیت فعلی و فن‌آوری‌های آینده به دست می‌آورند.

این کتاب بخشی از تجربه نویسندگان کتاب به عنوان پژوهشگران امنیتی^۱ است که روی امنیت وب، با تمرکز قوی در سمت امنیت کاربر کار می‌کنند؛ یعنی روی موضوعات امنیتی وب مانند حمله CSRF، حمله نبشته سایت قلابی^۲، مشکلات مدیریت نشست و کلیک‌رایبی. علاوه بر این نویسندگان این کتاب به طور جدی در پروژه‌های امنیت وب اروپایی مانند STREWS^۳، WebSand^۴ و NESSoS^۵ شرکت دارند و با کمیته‌های استاندارد IETF و W3C همکاری می‌کنند که باعث گسترش دید آن‌ها درباره وضعیت فعلی و بهترین تجربه‌های عملی شده است.

بدین وسیله از حمایت اژانس نوآوری‌های علم و فناوری^۶ (IWT) و پروژه STREWS که نسخه اولیه این کتاب در آن نوشته شد و پروژه IWT-SBO مربوط به SPION^۷ که باعث افزایش بینش نویسندگان در رابطه با حریم خصوصی و موضوعات امنیتی برنامه‌های کاربردی وب معاصر شد، تشکر و قدردانی می‌شود.

^۱ فیلیپ دیریک، لیون دزمت و فرانک پیسنز با گروه پژوهشی iMinds-DistriNet در دانشگاه KULeuven (بلژیک) همکاری می‌کنند و مارتین جونز در گروه پژوهشی SAP Research (آلمان) مشغول به فعالیت است.

^۲ XSS (Cross Site Scripting)

^۳ <https://www.strewn.eu/>.

^۴ <https://www.websand.eu/>.

^۵ <http://www.nessos-project.eu/>.

^۶ Agency For Innovation By Science And Technology

^۷ <http://www.spion.me/>.