Я посвящаю эту книгу моему самому любимому человеку.
Спасибо, что ты останавливал мир на время,
которого мне хватило, чтобы написать эту книгу.
Я чувствую, что с твоей поддержкой могу все.

Содержание

От издательства

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу dmkpress@gmail.com. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Wiley очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Об авторе

Таня Янца, она же SheHacksPurple, – автор бестселлеров «Alice and Bob Learn Secure Coding», «Alice and Bob Learn Application Security» и карточной игры AppSec Antics. За 28 лет карьеры в ИТ она стала лауреатом бесчисленных премий (включая звание пожизненного выдающегося члена OWASP и хакера года), выступала с докладами по всей планете и является плодовитым блогером. Таня обучила тысячи разработчиков программного обеспечения и специалистов по безопасности в своих онлайновых академиях (We Hack Purple и Semgrep Academy) и на практических семинарах. В рамках контртеррористической деятельности обеспечивала безопасность выборов 52-го генерал-губернатора Канады и обезопасила бесчисленное количество приложений. Таня Янца считается общепризнанным международным авторитетом по безопасности программного обеспечения.

О технических редакторах

Барре Дийкстра 25 лет занимается разработкой ПО на различных ролях – от практического программирования до руководства.

За это время он пришел к выводу о необходимости уделять больше внимания безопасности приложения, от кода до архитектуры и процесса. В настоящее время он часто оказывает поддержку клиентским командам по таким вопросам, как моделирование угроз, конфиденциальность и безопасность по определению, а также работает с группами обеспечения безопасности, занимающимися разработкой.

Помимо работы в сфере разработки ПО, Барре играет в CTF*, работает волонтером в Голландском институте обнаружения уязвимостей (Dutch Institute for Vulnerability Disclosure – DIVD), который принимает участие в организации одного из крупнейших соревнований по CTF, и несколько семестров преподавал на курсах подготовки бакалавров в области методов взлома и обратного проектирования.

Фабьен Ло Рикко – системный инженер с богатым 15-летним опытом в области конструирования ПО, системной инженерии и технической поддержки. Специализируется на обеспечении безопасности с упором на предотвращение потери данных (data loss prevention – DLP) и применяет свой практический опыт для защиты конфиденциальной информации.

Занимаясь на протяжении карьеры обслуживанием малых предприятий, он наработал разносторонний набор навыков, покрывающих весь спектр ИТ – от технической поддержки до проектирования архитектуры систем. Он активно выступает за ПО с открытым исходным кодом и применяет как проприетарные, так и открытые решения для проектирования надежных и экономичных систем, ориентированных на потребности бизнеса.

Франциска Пассинг – старший инженер-эксплуатационник в Дуолинго. Раньше работала в отделах инженерии внутренних платформ и обеспечения безопасности в таких компаниях, как Mapbox, Microsoft и др. Является опытным докладчиком, организатором технических сообществ и активным членом феминистского хакерского клуба Heart of Code. В настоящее время проживает в Берлине, где любит попивать кофе и участвовать в триатлонах. Связаться с ней можно через сайт https://franka.tech.

---

* Capture the Flag (захвати флаг) – командная игра по компьютерной безопасности. – *Прим. перев.*

Благодарности

Выражаю глубокую благодарность трем моим выдающимся техническим редакторам (Фабьену Ло Рикко, Франке Шмидт и Барре Дийкстра), чья непоколебимая поддержка, конструктивная критика и преданность были для меня стимулом на протяжении всего времени написания второй моей книги. Их воодушевление, настойчивость и стремление к совершенству не только повысили качество работы, но и вдохновили меня на достижение новых высот на моем писательском пути. Я в неоплатном долгу перед ними за их бесценный вклад и за то, что они находились со мной больше двух лет, сопровождая на всех подъемах и спусках процесса написания книги. Мне не хватает слов, чтобы в должной мере отблагодарить их за наставления, опыт и веру в проект.

Вступительное слово

С технической точки зрения сейчас отличное время быть инженером-программистом. Когда я была юным ботаном, зачитывалась научно-фантастическими романами и смотрела ранние эпизоды фильмов «Доктор Кто» и «Звездный путь: новое поколение», меня очаровывали технологии, демонстрируемые на экране. В том новом будущем у нас были приложения и приспособления для решения любой проблемы.

25 лет промелькнули быстро, и кажется, что мы сейчас живем в век необычайных изобретений. Программы проникли чуть ли не в каждую часть нашей жизни, от работы до свободного времени, а создаем их мы, инженеры.

Системы, которые мы пишем, объединяют нас и помогают сотрудничать и делиться информацией в невиданных ранее масштабах. Программы также помогают нам определять состояние здоровья, управлять роботами, которые помогают преодолевать неблагоприятные окружающие условия и даже ездят вместо нас по улицам наших городов. Однако при такой зависимости от программ и преимуществ, которые они предлагают, мы несем общую ответственность за то, что эти программы могут делать, и за их воздействие на людей, данные и системы.

В начале моей карьеры разработчика создаваемые мной системы (в области финансов и налогообложения) были не такими ответственными, как теперь. Эти системы обычно использовались только с 9 утра до 5 вечера с понедельника по пятницу, а если они вдруг переставали работать, то это, конечно, было неудобно, но компенсировалось многочисленными ручными системами.

Нынешние программы так глубоко вплетены в нашу жизнь, что последствия инцидентов и проблем значительно многообразнее и – в некоторых случаях – намного опаснее.

Именно поэтому настоящая книга и вся Танина работа по безопасному кодированию так важны. Мы, разработчики программного обеспечения, стоим на распутье. Мы обязаны следить за тем, чтобы наши программы и системы были высочайшего качества и отвечали самым строгим стандартам. Мы несем ответственность за баланс производительности, масштабируемости, удобства использования, наблюдаемости и доступности – всего того, благо-

даря чему наши приложения работают как задумано, когда это необходимо, обслуживая максимально возможное количество людей.

Самое время добавить сюда еще и безопасность.

В этой книге Таня постаралась сделать безопасное кодирование доступным разработчикам ПО на все случаи жизни и во всех программных экосистемах. Благодаря ее легким для понимания примерам и простому, прагматичному подходу даже самые занятые команды разработчиков смогут приступить к работе над безопасностью своего кода с учетом сложившегося у них цикла разработки, культуры и выбора языка. Изобилующая примерами и врезками, эта книга станет удобным справочником, который вы захотите вручить своей команде.

Если мы собираемся строить это чудесное пронизанное программами будущее вместе, то надеюсь, что сможем уделить время тому, чтобы сделать каждый следующий день немного безопаснее, чем предыдущий, а каждую строку кода будем рассматривать как возможность улучшить качество и безопасность своих систем.

Лаура Майн Белл,
генеральный директор и основатель компании SafeStack