



# Содержание

Об авторе .....	17
О технических редакторах .....	18
Благодарности .....	20
Предисловие .....	21
Введение .....	23
Сдвиг влево .....	25
О книге .....	27
Темы, выходящие за рамки книги .....	28
Ответы .....	28

## ЧАСТЬ I

### ВСЕ, ЧТО НУЖНО ЗНАТЬ О КОДЕ, БЕЗОПАСНОМ ДЛЯ ПУБЛИКАЦИИ В ИНТЕРНЕТЕ

Глава 1. Основы безопасности .....	33
Обязательство по обеспечению безопасности: «CIA» .....	33
Конфиденциальность .....	34
Целостность .....	36
Доступность .....	37
«Предполагать взлом» .....	39
Внутренние угрозы .....	42
Глубокая защита .....	44
Принцип наименьших привилегий .....	46
Безопасность цепи поставок .....	48
Безопасность через неясность .....	51
Уменьшение поверхности атаки .....	53
Жесткое кодирование .....	54

«Никогда не доверяй, всегда проверяй» .....	55
Удобство и безопасность .....	58
Факторы аутентификации .....	60
Упражнения .....	62
<b>Глава 2. Требования безопасности</b> .....	<b>65</b>
Требования .....	67
Шифрование .....	68
Никогда нельзя доверять входному потоку системы .....	70
Кодирование и экранирование .....	78
Сторонние компоненты .....	80
Заголовки безопасности: ремни безопасности для веб-приложений .....	84
Заголовки безопасности на практике .....	85
X-XSS-Protection .....	86
Content-Security-Policy (CSP) .....	86
X-Frame-Options .....	92
X-Content-Type-Options .....	93
Referrer-Policy .....	94
Strict-Transport-Security (HSTS) .....	95
Feature-Policy .....	98
X-Permitted-Cross-Domain-Policies .....	99
Expect-CT .....	99
Public Key Pinning Extension for HTTP (HPKP) .....	102
Обеспечение безопасности файлов cookies .....	103
Флаг Secure .....	104
Флаг HTTPOnly .....	105
Для постоянных cookies .....	105
Domain .....	106
Path .....	107
Same-site .....	107
Cookie с префиксом .....	109
Политика конфиденциальности .....	109
Классификация данных .....	110

Пароли, хранилище и другие важные решения, касающиеся обеспечения безопасности .....	112
HTTPS повсюду .....	122
Настройки TLS .....	124
Комментарии .....	125
Резервное копирование и восстановление .....	125
Элементы безопасности платформы .....	126
Технический долг = Долг безопасности .....	127
Загрузка файлов .....	129
Ошибки и их регистрация .....	130
Проверка и санитизация вводимых значений .....	133
Авторизация и аутентификация .....	134
Параметризованные запросы .....	135
Параметры URL .....	136
Принцип наименьших привилегий .....	137
Чек-лист требований .....	138
Упражнения .....	142
<b>Глава 3. Безопасность при проектировании ПО .....</b>	<b>144</b>
Ошибка проектирования и дефект безопасности .....	146
Позднее обнаружение ошибки проектирования .....	146
Сдвиг влево .....	148
Концепции проектирования безопасного ПО .....	149
Защита конфиденциальных данных .....	149
«Никогда не доверяй, всегда проверяй» и «Предполагать взлом» .....	153
Резервное копирование и откат .....	155
Валидация на стороне сервера .....	157
Функции безопасности платформы .....	159
Изоляция функций безопасности .....	160
Разделение приложения .....	161
Управление секретами приложения .....	162
Повторная аутентификация при транзакционных операциях (предотвращение CSRF-атаки) .....	163

Разделение производственных данных .....	164
Защита исходного кода .....	165
Моделирование угроз .....	167
Упражнения .....	174
<b>Глава 4. Безопасность кода ПО .....</b>	<b>176</b>
Выбор используемой платформы и языка программирования .....	176
Пример 1 .....	179
Пример 2 .....	180
Пример 3 .....	182
Языки программирования и платформы: правило .....	182
Сомнительные данные .....	183
HTTP-глаголы .....	187
Идентификация .....	189
Управление сессиями .....	190
Проверка границ .....	193
Аутентификация (AuthN) .....	195
Авторизация (AuthZ) .....	198
Обработка, регистрация и мониторинг ошибок .....	204
Правила работы с ошибками .....	206
Регистрация .....	207
Мониторинг .....	208
Упражнения .....	212
<b>Глава 5 .....</b>	<b>214</b>
<b>Часто встречающиеся подводные камни .....</b>	<b>214</b>
OWASP .....	214
Ранее не упомянутые средства защиты и уязвимости .....	220
Межсайтовая подделка запроса (CSRF) .....	220
Подделка запросов со стороны сервера (SSRF) .....	225
Десериализация .....	228
Состояние гонки .....	230
Заключительные комментарии .....	232
Упражнения .....	232

## ЧАСТЬ II

### КАК НАПИСАТЬ БЕЗУПРЕЧНЫЙ КОД

<b>Глава 6. Тестирование и развертывание</b> .....	237
Тестирование кода .....	238
Обзор кода .....	238
Статическое тестирование безопасности приложений (SAST) .....	241
Анализ состава программного обеспечения (SCA) .....	244
Модульное тестирование .....	247
Инфраструктура как код (IaC) и безопасность как код (SaC) .....	250
Тестирование приложения .....	253
Ручное тестирование .....	256
Браузеры .....	256
Инструменты разработчика .....	257
Веб-прокси .....	258
Фаззинг .....	260
Динамическое тестирование безопасности приложений (DAST) .....	261
Инфраструктура .....	261
Пользовательские приложения .....	262
Оценка уязвимости, оценка безопасности, пентестирование .....	264
Гигиена безопасности .....	268
Стресс-тестирование и тестирование производительности .....	271
Интеграционное тестирование .....	272
Интерактивное тестирование безопасности приложений .....	274
Регрессионное тестирование .....	275
Тестирование инфраструктуры .....	276
Тестирование базы данных .....	277
Тестирование API и веб-серверов .....	279

Тестирование интеграций .....	281
Тестирование сети .....	283
Развертывание .....	284
Редактирование кода на сервере в реальном времени .....	285
Публикация из среды IDE .....	287
«Самодельные» системы развертывания .....	288
Ранбуки .....	289
Непрерывная интеграция, непрерывная поставка, непрерывное развертывание .....	290
Упражнения .....	293
<b>Глава 7. Программы безопасности приложений .....</b>	<b>294</b>
Задачи программы по защите приложения .....	295
Создание и поддержка реестра приложения .....	297
Техническая возможность обнаружения уязвимостей в написанном, выполняемом и стороннем коде .....	299
Знания и ресурсы, необходимые для исправления уязвимостей .....	300
Образование и справочные материалы .....	301
Предоставление разработчикам инструментов по обеспечению безопасности приложений .....	303
Проведение одного или нескольких мероприятий по обеспечению безопасности на каждом этапе жизненного цикла разработки системы .....	304
Внедрение полезных и эффективных инструментов .....	306
Команда реагирования на инциденты, которая знает, когда вам звонить .....	307
Постоянное совершенствование программы на основе показателей, экспериментов и обратной связи .....	309
Метрики .....	310
Экспериментирование .....	313
Обратная связь от всех и каждой из заинтересованных сторон .....	314

Особое замечание о DevOps и Agile .....	315
Деятельность по обеспечению безопасности приложений .....	316
Инструменты по обеспечению безопасности приложений .....	319
Ваша программа безопасности приложения .....	322
Упражнения .....	322
<b>Глава 8. Обеспечение безопасности современных систем и приложений .....</b>	<b>324</b>
API и микросервисы .....	325
Онлайн-хранилище .....	330
Контейнеры и оркестровка .....	332
Бессерверные приложения .....	335
Инфраструктура как код (IaC) .....	338
Безопасность как код (SaC) .....	342
Платформа как услуга (PaaS) .....	343
Инфраструктура как услуга (IaaS) .....	345
Непрерывные интеграция, поставка и развертывание .....	346
Dev(Sec)Ops .....	348
DevSecOps .....	350
Облако .....	352
Облачные вычисления .....	352
Ориентированность на облако .....	354
Безопасность облачно-ориентированной среды .....	356
Облачные потоки .....	357
Современные инструменты .....	358
Интерактивное тестирование безопасности приложений IAST .....	359
Запуск защиты приложений .....	359
Контроль целостности файлов .....	360
Инструменты контроля приложений (список одобренного программного обеспечения) .....	360



Инструменты безопасности, созданные для конвейеров DevOps .....	362
Инструменты инвентаризации приложений .....	362
Автоматизация политики наименьших привилегий и других .....	363
Современные тактические приемы .....	364
В итоге .....	366
Упражнения .....	367

### **ЧАСТЬ III**

#### **ПОЛЕЗНАЯ ИНФОРМАЦИЯ О ТОМ, КАК ПОСТОЯННО ПИСАТЬ КОД ОЧЕНЬ ВЫСОКОГО КАЧЕСТВА**

<b>Глава 9. Полезные привычки .....</b>	<b>371</b>
Управление паролями .....	372
Отмена правил сложности пароля .....	372
Использование менеджера паролей .....	374
Парольные фразы .....	376
Отказ от повторного использования паролей .....	376
Отказ от ротации паролей .....	377
Многофакторная аутентификация .....	378
Реагирование на инциденты .....	380
Пожарные учения .....	381
Непрерывное сканирование .....	383
Технический долг .....	384
Инвентаризация .....	385
Другие полезные привычки .....	387
Политики .....	387
Загрузки и устройства .....	387
Блокировка рабочей техники .....	388
Приватность .....	388
Итоги .....	390
Упражнения .....	391

<b>Глава 10. Непрерывное обучение</b> .....	393
Что изучать .....	394
Нападение = защита .....	394
Не забывайте о «гибких навыках» .....	395
Лидерство != менеджмент .....	396
Варианты обучения .....	397
Действия, которые можно выполнять самостоятельно .....	398
Действия, которые можно выполнять на работе (или о чем можно попросить начальника) .....	400
Действия, которые можно выполнять в отношении своих сотрудников .....	402
Подотчетность .....	403
Составление плана .....	404
Действуйте .....	406
Упражнения .....	406
Учебный план .....	408
<b>Глава 11. Заключение</b> .....	409
Вопросы, оставшиеся без ответа .....	411
Когда можно говорить о достаточности предпринятых мер по обеспечению безопасности? .....	411
Как привлечь руководство к обеспечению безопасности? .....	415
Как привлечь разработчиков к обеспечению безопасности? .....	417
С чего начать? .....	419
Откуда брать помощь? .....	420
Заключение .....	421
<b>Приложение А. Источники</b> .....	422
<b>Приложение Б. Ответы</b> .....	431
<b>Предметный указатель</b> .....	456

## **Отзывы о книге Тани Янка «Безопасность веб-приложений. Визуальный гид для начинающих разработчиков»**

*Таня знает свое дело. Она обладает огромным объемом знаний и опыта в сфере безопасности приложений, DevSecOps и облачной безопасности. Мы все можем многое узнать от Тани, так что стоит прочитать ее книгу!*

**Дэвид Штутгард**, соавтор бестселлера  
The Web Application Hacker's Handbook, создатель  
приложения Burp Suite

*Я так много узнала из этой книги! Информационная безопасность действительно является работой каждого специалиста. Книга представляет собой потрясающее изложение обширных знаний, необходимых каждому: разработчику, специалисту по инфраструктуре, безопасности и многим другим. Благодарю госпожу Янку за написание такого познавательного и полезного учебника. Мне понравились правдоподобные истории с описанием реальных проблем, охватывающие всё, начиная с проектирования, миграции приложений из проблемных фреймворков, минимизации административных рисков и заканчивая вещами, которые должен знать каждый современный разработчик.*

**Джен Ким**, автор бестселлера The Unicorn Project,  
соавтор The Phoenix Project, DevOps Handbook  
и Accelerate

*Практическое руководство для современной эпохи. Таня отлично рассказывает о современном представлении о безопасности приложений понятным для всех языком.*

**Трой Хант**, создатель веб-сайта Have I Been Pwned?

Я посвящаю эту книгу моей неутомимой группе поддержки: Лекси, Матеусу, Эшу и Вейну. Постоянно поддерживая, ободряя и отмечая завершение каждого этапа создания книги, вы не позволили мне бросить начатое. Также спасибо, что не осуждаете меня за то, сколько мороженого я съела во время редактирования.



## Об авторе

**Таня Янка**, также известная под ником SheHacksPurple, является основательницей We Hack Purple, онлайн-академии, сообщества и канала подкастов, цель которых — обучение всех желающих созданию безопасного программного обеспечения. Она также является соучредителем компании WoSEC: Women of Security, руководит проектом OWASP DevSlop и отделением OWASP Victoria. Таня занимается программированием и работает в области IT более двадцати лет. За это время она завоевала множество наград, успела потрудиться везде, от стартапов до государственных организаций и технологических гигантов (Microsoft, Adobe и Nokia). Она занимала различные должности: была основателем стартапа, пентестером (тестировщиком, проверяющим уязвимость киберзащиты информационной системы), директором по информационной безопасности, инженером по безопасности приложений и разработчиком программного обеспечения. Будучи превосходным оратором, активным блогером и стримером, она провела сотни выступлений и тренингов на шести континентах. Она ценит разнообразие, вовлеченность и человеколюбие, что проявляется в ее бесчисленных инициативах.

## О технических редакторах

**Доминик Ригетто** начал свою карьеру в сфере разработки программного обеспечения, а восемь лет спустя перешел в область обеспечения безопасности, продолжая жить на границе двух миров. Доминику очень интересны наступательные и оборонительные аспекты безопасности приложений. В сфере безопасности (как и на всем протяжении профессиональной жизни) его главной целью было помогать командам разработчиков прагматически подходить к обеспечению безопасности своих проектов. С 2011 года Доминик является активным членом фонда OWASP, в рамках которого участвует в различных проектах, в основном касающихся его специализации в области доменов. Являясь приверженцем философии открытого исходного кода, в свободное время он участвует в различных проектах, соответствующих этой идее. Его домашняя страница — [righettod.eu](http://righettod.eu).

**Эли Саад** — опытный специалист в области информационной безопасности, работающий в банковской сфере. Он участвует в различных инициативах OWASP по стандартизации и регулярно публикует статьи по этой теме. Его основная цель — дать разработчикам программного обеспечения рекомендации по обеспечению безопасности и защите. Он провел несколько лекций,