

грокаем

безопасность веб-приложений

Малькольм Макдональд

Предисловие Стюарта Макклюра

Выпущено
при поддержке

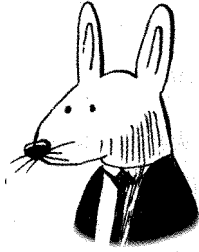
КРОК

 **ПИТЕР®**

Санкт-Петербург • Москва • Минск

2025

Оглавление



Предисловие	10
Введение	12
Благодарности	15
Об этой книге	17
Для кого эта книга	17
Структура книги	17
О коде в книге	18
Форум liveBook	18
Об авторе	19
От издательства	20
О научном редакторе русского издания	20
ЧАСТЬ 1	21
Глава 1. Врага нужно знать в лицо	22
Как (и почему) нападают хакеры	23
Преодоление последствий взлома	28
Насколько нужно включать паранойю	30
В какой момент начинать себя защищать	32
Подведем итоги	35

Глава 2. Безопасный браузер	36
Из чего состоит веб-браузер	37
Песочница JavaScript	38
Доступ к диску	50
Cookies	53
Межсайтовое отслеживание (cross-site tracking)	59
Подведем итоги	61
Глава 3. Шифрование	62
Принципы шифрования	63
Ключи шифрования	64
Шифрование при передаче	66
Шифрование в состоянии покоя	71
Проверка целостности	75
Подведем итоги	77
Глава 4. Безопасность веб-сервера	78
Валидация вводимых данных	79
Экранирование выходных данных	86
Работа с ресурсами	96
REST	98
Глубокая защита	99
Принцип минимальных привилегий	101
Подведем итоги	102
Глава 5. Безопасность как процесс	103
Принцип четырех глаз	104
Применение принципа минимальных привилегий к процессам ...	106
Автоматизируйте все подряд	107
Не изобретайте велосипед	108
Храните журналы аудита	110
Безопасное написание кода	111
Средства самообороны	120
Признавайте ошибки	124
Подведем итоги	126

ЧАСТЬ 2.	127
Глава 6. Уязвимости браузера	128
Межсайтовый скриптинг	129
Межсайтовая подделка запроса	140
Кликджекинг	148
Внедрение межсайтовых скриптов	152
Подведем итоги	156
Глава 7. Сетевые уязвимости	157
Уязвимости «монстр посередине»	158
Уязвимости ложного направления (misdirection)	165
Компрометация сертификатов	176
Краденые ключи	179
Подведем итоги	181
Глава 8. Уязвимости аутентификации	183
Атаки методом перебора	184
Технология единого входа	185
Повышение надежности аутентификации	191
Многофакторная аутентификация	196
Биометрия	198
Хранение учетных данных	200
Перечисление пользователей	205
Подведем итоги	211
Глава 9. Уязвимости сессий	213
Как работают сессии	214
Перехват сессий	219
Подмена сессии	225
Подведем итоги	226
Глава 10. Уязвимости авторизации	227
Моделирование авторизации	229
Проектирование авторизации	232
Реализация контроля доступа	233

Тестирование авторизации	242
Выявление распространенных недочетов авторизации	245
Подведем итоги	247
Глава 11. Уязвимости полезных данных	248
Атаки десериализации	249
Уязвимости XML	256
Уязвимости загрузки файлов	263
Обход пути	268
Массовое присваивание	270
Подведем итоги	272
Глава 12. Уязвимости внедрения	273
Удаленное выполнение кода	274
SQL-инъекция	280
NoSQL-инъекции	287
LDAP-инъекция	289
Внедрение команд	291
Внедрение CRLF	293
Внедрение регулярных выражений	296
Подведем итоги	298
Глава 13. Уязвимости в стороннем коде	299
Зависимости	302
Далее вниз по стеку	307
Утечка информации	309
Небезопасная конфигурация	313
Подведем итоги	315
Глава 14. Быть невольным соучастником	316
Подделка запросов на стороне сервера	317
Спуфинг электронной почты	321
Открытые редиректы	323
Подведем итоги	326

Глава 15. Что делать, если вас взломали	327
Как узнать, что вас взломали	328
Пресечение атаки	329
А что, собственно, произошло?	330
Как не допустить повторной атаки	331
Сообщение пользователям подробностей об инциденте	332
Снижение риска в будущем	333
Подведем итоги	334