

# Безопасность веб-приложений

Разведка, защита, нападение



Эндрю Хоффман



Санкт-Петербург • Москва • Минск

2023

---

# Краткое содержание

Предисловие .....	16
<b>Глава 1.</b> История защиты программного обеспечения .....	<b>34</b>

## ЧАСТЬ I. РАЗВЕДКА

<b>Глава 2.</b> Введение в разведку веб-приложений.....	<b>55</b>
<b>Глава 3.</b> Структура современных веб-приложений.....	<b>61</b>
<b>Глава 4.</b> Поиск субдоменов.....	<b>90</b>
<b>Глава 5.</b> Анализ API .....	<b>114</b>
<b>Глава 6.</b> Обнаружение сторонних зависимостей .....	<b>124</b>
<b>Глава 7.</b> Поиск слабых мест в архитектуре приложения .....	<b>136</b>
<b>Глава 8.</b> Итоги части I .....	<b>145</b>

## ЧАСТЬ II. НАПАДЕНИЕ

<b>Глава 9.</b> Введение во взлом веб-приложений.....	<b>148</b>
<b>Глава 10.</b> Межсайтовый скриптинг (XSS).....	<b>151</b>
<b>Глава 11.</b> Подделка межсайтовых запросов (CSRF) .....	<b>166</b>
<b>Глава 12.</b> Атака на внешние сущности XML (XXE).....	<b>176</b>
<b>Глава 13.</b> Внедрение кода.....	<b>183</b>

<b>Глава 14.</b> Отказ в обслуживании (DoS) .....	196
<b>Глава 15.</b> Эксплуатация сторонних зависимостей .....	206
<b>Глава 16.</b> Итоги части II .....	218

### **ЧАСТЬ III. ЗАЩИТА**

<b>Глава 17.</b> Защита современных веб-приложений .....	221
<b>Глава 18.</b> Безопасная архитектура приложений .....	228
<b>Глава 19.</b> Проверка безопасности кода .....	240
<b>Глава 20.</b> Обнаружение уязвимостей.....	251
<b>Глава 21.</b> Управление уязвимостями .....	262
<b>Глава 22.</b> Противодействие XSS-атакам.....	272
<b>Глава 23.</b> Защита от CSRF .....	285
<b>Глава 24.</b> Защита от XXE-атак.....	293
<b>Глава 25.</b> Противодействие внедрению .....	297
<b>Глава 26.</b> Противодействие DoS-атакам .....	307
<b>Глава 27.</b> Защита сторонних зависимостей.....	312
<b>Глава 28.</b> Итоги части III .....	318
<b>Глава 29.</b> Заключение .....	327
Об авторе .....	329
Об обложке .....	330

---

# Оглавление

<b>Предисловие .....</b>	<b>16</b>
Исходные требования и цели обучения.....	16
Требования к уровню подготовки .....	17
Минимальный набор навыков .....	17
Кому больше всего пригодится эта книга? .....	18
Инженеры-программисты и разработчики веб-приложений.....	18
Общие цели обучения.....	20
Инженеры по безопасности, пентестеры и охотники за багами .....	20
Структура книги .....	21
Разведка.....	22
Нападение.....	23
Защита.....	24
Язык и терминология.....	27
Итоги .....	32
Условные обозначения.....	32
От издательства.....	33
<b>Глава 1. История защиты программного обеспечения.....</b>	<b>34</b>
Истоки хакерства.....	34
«Энигма», 1930-е.....	35
Автоматизированный взлом шифра «Энигмы», 1940-е .....	39
Появление «бомбы».....	40
Фрикинг, 1950-е.....	42
Метод борьбы с фрикингом, 1960-е.....	43
Начало компьютерного взлома, 1980-е .....	45

Расцвет Всемирной паутины, 2000-е .....	46
Современные хакеры, после 2015-го .....	49
Итоги .....	52

## ЧАСТЬ I РАЗВЕДКА

<b>Глава 2. Введение в разведку веб-приложений .....</b>	<b>55</b>
Сбор информации.....	55
Карта веб-приложения .....	58
Итоги .....	59
<b>Глава 3. Структура современных веб-приложений .....</b>	<b>61</b>
Сравнение современных и более ранних версий приложений.....	61
REST API .....	63
Формат JSON.....	66
JavaScript .....	68
Переменные и их область видимости.....	69
Функции .....	72
Контекст .....	73
Прототипное наследование .....	74
Асинхронное выполнение кода .....	77
Программный интерфейс DOM браузера .....	80
Фреймворки для SPA .....	82
Системы аутентификации и авторизации .....	83
Аутентификация.....	83
Авторизация .....	84
Веб-серверы .....	85
Базы данных на стороне сервера .....	86
Хранение данных на стороне клиента .....	87
Итоги .....	88
<b>Глава 4. Поиск субдоменов.....</b>	<b>90</b>
Множество приложений в рамках одного домена.....	90
Встроенные в браузер инструменты анализа.....	91

Общедоступная информация .....	94
Кэши поисковых систем .....	95
Поиск в архиве.....	97
Социальные профили.....	99
Атаки на передачу зоны .....	102
Брутфорс субдоменов .....	104
Перебор по словарю .....	110
Итоги .....	112
<b>Глава 5. Анализ API .....</b>	<b>114</b>
Обнаружение конечной точки .....	114
Механизмы аутентификации.....	118
Разновидности конечных точек .....	120
Основные разновидности .....	120
Специализированные разновидности .....	121
Итоги .....	123
<b>Глава 6. Обнаружение сторонних зависимостей .....</b>	<b>124</b>
Клиентские фреймворки .....	124
Фреймворки для одностраничных приложений.....	125
Библиотеки JavaScript.....	127
Библиотеки CSS .....	129
Фреймворки на стороне сервера .....	129
Заголовки .....	130
Стандартные сообщения об ошибке и страницы 404.....	130
Базы данных.....	133
Итоги .....	135
<b>Глава 7. Поиск слабых мест в архитектуре приложения.....</b>	<b>136</b>
Признаки безопасной и небезопасной архитектуры.....	137
Уровни безопасности .....	141
Заимствование и перекрой .....	142
Итоги .....	144
<b>Глава 8. Итоги части I .....</b>	<b>145</b>

## ЧАСТЬ II НАПАДЕНИЕ

<b>Глава 9. Введение во взлом веб-приложений.....</b>	<b>148</b>
Мышление хакера .....	148
Применение данных, полученных в процессе разведки.....	149
<b>Глава 10. Межсайтовый скриптинг (XSS) .....</b>	<b>151</b>
Обнаружение XSS-уязвимости .....	151
Хранимый XSS.....	155
Отраженный XSS.....	157
XSS-атака на базе DOM.....	160
XSS с мутациями.....	162
Итоги .....	164
<b>Глава 11. Подделка межсайтовых запросов (CSRF) .....</b>	<b>166</b>
Подделка параметров запроса.....	166
Изменение содержимого запроса GET.....	171
CSRF-атака на конечные точки POST .....	173
Итоги .....	175
<b>Глава 12. Атака на внешние сущности XML (XXE) .....</b>	<b>176</b>
Атака напрямую .....	176
Непрямая XXE-атака.....	180
Итоги .....	182
<b>Глава 13. Внедрение кода .....</b>	<b>183</b>
Внедрение SQL-кода .....	183
Внедрение кода.....	187
Внедрение команд.....	192
Итоги .....	195
<b>Глава 14. Отказ в обслуживании (DoS) .....</b>	<b>196</b>
ReDoS-атака.....	197
Логические DoS-уязвимости.....	200
Распределенная DoS-атака .....	203
Итоги .....	205

<b>Глава 15. Эксплуатация сторонних зависимостей .....</b>	<b>206</b>
Методы интеграции.....	208
Ветви и вилки .....	209
Приложения с собственным сервером.....	209
Интеграция на уровне кода .....	210
Диспетчеры пакетов .....	211
JavaScript .....	212
Java .....	214
Другие языки .....	214
База данных общеизвестных уязвимостей.....	215
Итоги .....	217
<b>Глава 16. Итоги части II.....</b>	<b>218</b>

## ЧАСТЬ III ЗАЩИТА

<b>Глава 17. Защита современных веб-приложений .....</b>	<b>221</b>
Архитектура защищенного ПО.....	222
Глубокий анализ кода .....	223
Поиск уязвимости .....	223
Анализ уязвимости .....	224
Управление уязвимостями.....	225
Регрессивное тестирование.....	225
Меры по снижению риска .....	226
Прикладные техники разведки и нападения .....	226
<b>Глава 18. Безопасная архитектура приложений .....</b>	<b>228</b>
Анализ требований к ПО.....	229
Аутентификация и авторизация .....	230
Протоколы SSL и TLS.....	230
Защита учетных данных.....	232
Хеширование учетных данных.....	233
Двухфакторная аутентификация .....	235



Личные данные и финансовая информация.....	237
Поиск.....	237
Итоги .....	238
<b>Глава 19. Проверка безопасности кода .....</b>	<b>240</b>
Начало проверки.....	241
Основные типы уязвимостей и пользовательские логические ошибки .....	242
С чего начать проверку безопасности .....	244
Антипаттерны безопасного программирования .....	246
Черные списки .....	247
Шаблонный код.....	248
Доверие по умолчанию .....	248
Разделение клиента и сервера.....	249
Итоги .....	250
<b>Глава 20. Обнаружение уязвимостей .....</b>	<b>251</b>
Автоматизированная проверка.....	251
Статический анализ .....	252
Динамический анализ .....	254
Регрессионное тестирование .....	255
Программы ответственного раскрытия информации .....	258
Программы Bug Bounty .....	259
Сторонние пентестеры .....	259
Итоги .....	260
<b>Глава 21. Управление уязвимостями .....</b>	<b>262</b>
Воспроизведение уязвимостей.....	262
Классификация уязвимостей .....	263
Общая система оценки уязвимостей .....	263
CVSS: Базовая метрика .....	265
CVSS: Временная метрика.....	268
CVSS: Контекстная метрика.....	269
Усовершенствованная классификация уязвимостей .....	270
Что делать потом .....	270
Итоги .....	271

<b>Глава 22. Противодействие XSS-атакам .....</b>	<b>272</b>
Приемы написания кода для противодействия XSS .....	272
Очистка пользовательского ввода.....	274
Приемник DOMParser .....	276
Приемник SVG .....	276
Приемник Blob .....	277
Санация гиперссылок .....	277
Символьные сущности в HTML.....	278
CSS.....	279
Политика защиты контента для предотвращения XSS.....	281
Директива script-src.....	281
Ключевые слова unsafe-eval и unsafe-inline .....	282
Внедрение CSP .....	283
Итоги .....	283
<b>Глава 23. Защита от CSRF .....</b>	<b>285</b>
Проверка заголовков .....	285
CSRF-токен .....	287
CSRF-токены без сохранения состояния .....	288
Противодействие CSRF на уровне кода .....	289
Запросы GET без сохранения состояния .....	289
Снижение риска CSRF на уровне приложения .....	290
Итоги .....	292
<b>Глава 24. Защита от XXE-атак .....</b>	<b>293</b>
Оценка других форматов данных .....	294
Дополнительные риски, связанные с XXE.....	295
Итоги .....	296
<b>Глава 25. Противодействие внедрению.....</b>	<b>297</b>
Противодействие внедрению SQL-кода .....	297
Распознавание внедрения SQL-кода .....	298
Подготовленные операторы .....	299
Более специфические методы защиты.....	301

Защита от других видов внедрения.....	302
Потенциальные цели внедрения .....	302
Принцип минимальных привилегий.....	303
Белый список команд.....	304
Итоги .....	305
<b>Глава 26. Противодействие DoS-атакам .....</b>	<b>307</b>
Противодействие атакам ReDoS.....	308
Защита от логических DoS-атак .....	308
Защита от DDoS .....	309
Смягчение DDoS-атак .....	310
Итоги .....	311
<b>Глава 27. Защита сторонних зависимостей.....</b>	<b>312</b>
Оценка дерева зависимостей.....	312
Моделирование дерева зависимости .....	313
Деревья зависимостей на практике .....	314
Автоматизированная оценка .....	314
Техники безопасной интеграции .....	315
Разделение интересов .....	315
Безопасное управление пакетами.....	316
Итоги .....	316
<b>Глава 28. Итоги части III .....</b>	<b>318</b>
История безопасности программного обеспечения.....	318
Разведка.....	320
Нападение.....	322
Защита .....	323
<b>Глава 29. Заключение .....</b>	<b>327</b>
Об авторе .....	329
Об обложке .....	330