

# C#

Г Л А З А М И

# ХАКЕРА

Михаил Фленов

**Теория безопасности кода**

**Безопасность веб-приложений  
на реальных примерах**

**Оптимизация кода**

**Защита Web API**

**Сетевые функции**

**Реальные примеры атак хакеров  
и защиты от них**



Материалы  
на [www.bhv.ru](http://www.bhv.ru)

**bhv**<sup>®</sup>

Михаил Фленов

**С#**

**Г Л А З А М И**

**ХАКЕРА**

Санкт-Петербург

«БХВ-Петербург»

2023

УДК 004.438 С#  
ББК 32.973.26-018.1  
Ф71

**Фленов М. Е.**

Ф71 С# глазами хакера. — СПб.: БХВ-Петербург, 2023. — 224 с.: ил. —  
(Глазами хакера)

ISBN 978-5-9775-1781-2

Подробно рассмотрены все аспекты безопасности от теории до реальных реализаций .NET-приложений на языке С#. Рассказано, как обеспечивать безопасную регистрацию, авторизацию и поддержку сессий пользователей. Перечислены уязвимости, которые могут быть присущи веб-сайтам и Web API, описано, как хакеры могут эксплуатировать уязвимости и как можно обеспечить безопасность приложений. Даны основы оптимизации кода для обработки максимального количества пользователей с целью экономии ресурсов серверов и денег на хостинг. Рассмотрены сетевые функции: проверка соединения, отслеживание запроса, доступ к микросервисам, работа с сокетами и др. Приведены реальные примеры атак хакеров и способы защиты от них.

*Для веб-программистов, администраторов  
и специалистов по безопасности*

УДК 004.438 С#  
ББК 32.973.26-018.1

### Группа подготовки издания:

Руководитель проекта	<i>Евгений Рыбаков</i>
Зав. редакцией	<i>Людмила Гауль</i>
Редактор	<i>Григорий Добин</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Дизайн серии	<i>Марины Дамбиевой</i>
Оформление обложки	<i>Зои Канторович</i>

Подписано в печать 02.03.23.

Формат 70×100<sup>1/16</sup>. Печать офсетная. Усл. печ. л. 18,06.

Тираж 1200 экз. Заказ № 6250.

"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Отпечатано с готового оригинал-макета

ООО "Принт-М", 142300, М.О., г. Чехов, ул. Полиграфистов, д. 1

ISBN 978-5-9775-1781-2

© ООО "БХВ", 2023  
© Оформление. ООО "БХВ-Петербург", 2023

# Оглавление

<b>Предисловие</b> .....	<b>7</b>
Об авторе .....	7
О книге.....	8
Благодарности.....	8
<b>Глава 1. Теория безопасности</b> .....	<b>11</b>
1.1. Комплексная защита.....	12
1.2. Отказ в обслуживании.....	15
1.3. Управление кодом .....	17
1.4. Стабильность кода: нулевые исключения .....	19
1.5. Исключительные ситуации .....	21
1.6. Журналы ошибок и аудит .....	22
1.7. Ошибки нужно исправлять .....	24
1.8. Отгружаем легко и часто .....	28
1.8.1. Обновление базы данных.....	30
1.8.2. Копирование файлов .....	31
1.8.3. Распределенное окружение.....	32
1.9. Шифрование трафика.....	33
1.10. POST или GET? .....	35
<b>Глава 2. Безопасность .NET-приложений</b> .....	<b>39</b>
2.1. Шаблон приложения .....	39
2.2. Регистрация пользователей.....	41
2.3. Форма регистрации .....	43
2.3.1. Корректные данные регистрации.....	44
2.3.2. Email с плюсом и точкой.....	48
2.4. Хранение паролей.....	49
2.4.1. Хеширование.....	51
2.4.2. MD5-хеширование .....	51
2.4.3. Безопасное хеширование .....	54
2.5. Создание посетителей .....	55
2.6. Captcha.....	56
2.6.1. Настраиваем Google reCAPTCHA.....	57

2.6.2. Пример использования reCAPTCHA .....	59
2.6.3. Отменяем капчу .....	62
2.7. Авторизация .....	63
2.7.1. Базовая авторизация .....	63
2.7.2. Журналирование и защита от перебора .....	65
2.7.3. Защищаемся от перебора .....	66
2.8. Инъекция SQL: основы .....	69
2.8.1. SQL-уязвимость в ADO.NET .....	69
2.8.2. Защита от SQL-инъекции .....	73
2.9. Dapper ORM .....	75
2.10. Entity Framework .....	80
2.11. Отправка электронной почты .....	84
2.11.1. Очереди сообщений .....	85
2.11.2. Работа с очередью .....	87
2.11.3. Отправляем письма .....	88
2.12. Многоуровневая авторизация .....	90
2.13. Запомни меня .....	91
2.13.1. Зашифрованный якорь .....	92
2.13.2. Опасность <i>HttpOnly</i> .....	95
2.13.3. Что дальше? .....	97
2.14. Подделка параметров .....	97
2.15. Флуд .....	100
2.16. XSS: межсайтовый скриптинг .....	102
2.16.1. Защита от XSS в .NET .....	103
2.16.2. Примеры эксплуатации XSS .....	106
2.16.3. Типы XSS .....	108
2.16.4. Хранимая XSS .....	109
2.16.5. XSS: текст внутри тега .....	115
2.16.6. Скрипты .....	116
2.17. SQL Injection: доступ к недоступному .....	117
2.18. CSRF: межсайтовая подделка запроса .....	119
2.19. Загрузка файлов .....	123
2.20. Контроль доступа .....	125
2.21. Переадресация .....	128
2.22. Защита от DoS .....	130
<b>Глава 3. Основы производительности .....</b>	<b>135</b>
3.1. Основы .....	135
3.2. Когда нужно оптимизировать? .....	137
3.3. Оптимизация и рефакторинг .....	138
3.4. Отображение данных .....	139
3.5. Асинхронное выполнение запросов .....	142
3.6. Параллельное выполнение .....	143
3.7. LINQ .....	144
3.8. Обновление .NET .....	146
<b>Глава 4. Производительность в .NET .....</b>	<b>147</b>
4.1. Типы данных .....	147
4.1.1. Производительность .....	147

4.1.2. Отличие структур от классов.....	149
4.1.3. Ссылки на структуры .....	154
4.2. Виртуальные методы.....	156
4.3. Управление памятью .....	158
4.4. Закрытие соединений с базой данных .....	161
4.5. Циклы .....	164
4.6. Строки.....	165
4.7. Исключительные ситуации .....	167
4.8. Странный <i>HttpClient</i> .....	168
<b>Глава 5. Сеть .....</b>	<b>171</b>
5.1. Проверка соединения .....	171
5.2. Отслеживание запроса.....	172
5.3. Класс <i>HTTP-клиент</i> .....	175
5.4. Класс <i>Uri</i> .....	176
5.5. Уровень розетки.....	178
5.5.1. Сервер.....	178
5.5.2. Клиент.....	182
5.6. Доменная система имен .....	184
<b>Глава 6. Web API.....</b>	<b>187</b>
6.1. Пример Web API.....	187
6.2. JWT-токены.....	188
6.3. Устройство токенов.....	195
<b>Глава 7. Трюки .....</b>	<b>199</b>
7.1. Кеширование.....	199
7.1.1. Защита от XSS в .NET .....	199
7.1.2. Кеширование статичными переменными .....	203
7.1.3. Кеширование уровня запроса .....	204
7.1.4. Кеширование в памяти.....	205
7.1.5. Сервер кеширования .....	207
7.1.6. Cookie в качестве кеша.....	208
7.2. Сессии.....	210
7.2.1. Пишем свою сессию .....	210
7.2.2. Безопасность сессии .....	212
7.3. Защита от множественной обработки.....	213
<b>Заключение.....</b>	<b>217</b>
<b>Литература .....</b>	<b>219</b>
<b>Приложение. Описание файлового архива, сопровождающего книгу .....</b>	<b>221</b>
<b>Предметный указатель .....</b>	<b>222</b>