

# Оглавление

<b>Об авторе</b> .....	15
<b>О научном редакторе</b> .....	16
<b>Предисловие</b> .....	17
<b>Благодарности</b> .....	19
<b>Введение</b> .....	20
На кого рассчитана эта книга .....	21
Как читать эту книгу.....	21
О чем эта книга .....	22
Замечания о хакинге .....	24
От издательства .....	25
<b>Глава 1. Основы охоты за уязвимостями</b> .....	26
Уязвимости и награды за их нахождение.....	26
Клиент и сервер .....	27
Что происходит, когда вы заходите на веб-сайт .....	28
Шаг 1. Извлечение доменного имени .....	28
Шаг 2. Получение IP-адреса.....	28
Шаг 3. Установление TCP-соединения .....	29
Шаг 4. Отправка HTTP-запроса.....	30

---

Шаг 5. Ответ сервера .....	31
Шаг 6. Отображение ответа .....	32
HTTP-запросы .....	33
Методы запроса .....	33
Протокол HTTP не хранит состояние .....	34
Итоги.....	35
<b>Глава 2. Open Redirect.....</b>	<b>36</b>
Как работает Open Redirect.....	37
Open Redirect на странице установки темы оформления Shopify .....	39
Open Redirect на странице входа в Shopify.....	39
Перенаправление на межсайтовой странице HackerOne .....	40
Итоги.....	42
<b>Глава 3. Засорение HTTP-параметров.....</b>	<b>43</b>
НРР на серверной стороне.....	43
НРР на клиентской стороне .....	45
Кнопки социальных сетей в HackerOne .....	46
Уведомления об отпуске в Twitter .....	47
Web Intents в Twitter .....	49
Итоги.....	51
<b>Глава 4. Межсайтовая подделка запросов .....</b>	<b>52</b>
Аутентификация.....	53
CSRF в GET-запросах .....	54
CSRF в POST-запросах .....	55
Защита от атак CSRF .....	57
Отключение Twitter от Shopify .....	58

Изменение пользовательских зон в Instacart .....	59
Полный захват учетной записи Badoo.....	61
Итоги.....	63
<b>Глава 5.</b> Внедрение HTML-элемента и подмена содержимого.....	64
Внедрение комментариев в Coinbase путем кодирования символов .....	65
Непредвиденное внедрение HTML в HackerOne .....	67
Обход исправления непредвиденного внедрения HTML в HackerOne .....	70
Подмена содержимого в Within Security .....	71
Итоги.....	73
<b>Глава 6.</b> Внедрение символов перевода строки .....	74
Передача скрытого HTTP-запроса .....	74
Разделение ответа в v.shopify.com .....	75
Разделение HTTP-ответа в Twitter .....	77
Итоги.....	79
<b>Глава 7.</b> Межсайтовый скриптинг .....	80
Виды XSS.....	84
Shopify Wholesale.....	87
Форматирование валюты в Shopify .....	88
Хранимая уязвимость XSS в Yahoo! Mail .....	90
Поиск по картинкам Google .....	92
Хранимая уязвимость XSS в Google Tag Manager .....	93
XSS в United Airlines .....	94
Итоги.....	98

---

<b>Глава 8. Внедрение шаблонов</b> .....	99
Внедрение шаблонов на стороне сервера .....	99
Внедрение шаблонов на стороне клиента .....	100
Внедрение шаблона AngularJS на сайте Uber .....	101
Внедрение шаблонов Flask Jinja2 на сайте Uber .....	102
Динамический генератор в Rails .....	105
Внедрение шаблонов Smarty на сайте Unikrn .....	106
Итоги .....	110
<b>Глава 9. Внедрение SQL</b> .....	111
Реляционные базы данных .....	111
Контрмеры в отношении SQLi .....	113
Слепая атака SQLi на сайт Yahoo! Sports .....	114
Слепая уязвимость SQLi на сайте Uber .....	118
Уязвимость SQLi в Drupal .....	121
Итоги .....	125
<b>Глава 10. Подделка серверных запросов</b> .....	126
Демонстрация последствий подделки серверных запросов .....	126
Сравнение GET- и POST-запросов .....	127
Выполнение слепых атак SSRF .....	128
Атака на пользователей с помощью ответов SSRF .....	129
Уязвимость SSRF на сайте ESEA и извлечение метаданных из AWS .....	129
Уязвимость SSRF на сайте Google с применением внутреннего DNS-запроса .....	132
Сканирование внутренних портов с помощью веб-хуков .....	136
Итоги .....	138

<b>Глава 11. Внешние XML-сущности</b> .....	139
Расширяемый язык разметки .....	139
Определение типа документа .....	140
XML-сущности.....	142
Как работает атака XXE .....	143
Чтение внутренних файлов Google .....	144
XXE в Facebook с применением Microsoft Word .....	145
XXE в Wikiloc.....	148
Итоги.....	150
<b>Глава 12. Удаленное выполнение кода</b> .....	151
Выполнение команд оболочки .....	151
Выполнение функций .....	153
Стратегии обострения удаленного выполнения кода .....	154
Уязвимость в ImageMagick на сайте Polyvore .....	155
Уязвимость RCE на сайте facebooksearch.algolia.com .....	158
Атака RCE через SSH .....	160
Итоги.....	161
<b>Глава 13. Уязвимости памяти</b> .....	162
Переполнение буфера .....	163
Чтение вне допустимого диапазона .....	166
Целочисленное переполнение в PHP-функции ftp_genlist() .....	167
Модуль Python hotshot .....	168
Чтение вне допустимого диапазона в libcurl.....	169
Итоги.....	170

---

<b>Глава 14. Захват поддомена.....</b>	<b>171</b>
Доменные имена .....	171
Как происходит захват поддомена .....	172
Захват поддомена Ubiquiti.....	173
Поддомен Scan.me, ссылающийся на Zendesk.....	174
Захват поддомена windsor на сайте Shopify .....	175
Захват поддомена fastly на сайте Snapchat .....	176
Захват поддомена на сайте Legal Robot .....	177
Захват поддомена с почтовым сервисом SendGrid на сайте Uber.....	178
Итоги.....	180
<b>Глава 15. Состояние гонки .....</b>	<b>181</b>
Множественное получение приглашения на HackerOne.....	182
Превышение лимита на приглашения на сайт Keybase .....	184
Состояние гонки в механизме выплат на сайте HackerOne.....	185
Состояние гонки на платформе Shopify Partners.....	187
Итоги.....	189
<b>Глава 16. Небезопасные прямые ссылки на объекты .....</b>	<b>190</b>
Поиск простых уязвимостей IDOR.....	190
Поиск более сложных уязвимостей IDOR .....	191
Повышение привилегий на сайте Binary.com.....	192
Создание приложений на сайте Moneybird.....	193
Похищение токена для API-интерфейса Twitter Morpub .....	195
Раскрытие клиентской информации.....	197
Итоги.....	199

<b>Глава 17. Уязвимости в OAuth</b> .....	200
Принцип работы OAuth.....	201
Похищение OAuth-токенов на сайте Slack.....	204
Прохождение аутентификации с паролем по умолчанию.....	205
Похищение токенов для входа на сайт Microsoft.....	206
Похищение официальных токенов доступа на сайте Facebook.....	209
Итоги.....	210
<b>Глава 18. Уязвимости в логике и конфигурации приложений</b> .....	211
Получение администраторских привилегий на сайте Shopify.....	213
Обход защиты учетных записей на сайте Twitter.....	214
Манипуляция репутацией пользователей на сайте HackerOne.....	215
Некорректные права доступа к бакету S3 на сайте HackerOne.....	216
Обход двухфакторной аутентификации на сайте GitLab.....	219
Раскрытие страницы PHP Info на сайте Yahoo!.....	220
Голосование на странице HackerOne Hacktivity.....	222
Доступ к Memcache на сайте PornHub.....	224
Итоги.....	227
<b>Глава 19. Самостоятельный поиск уязвимостей</b> .....	228
Предварительное исследование.....	229
Составление списка поддоменов.....	229
Сканирование портов.....	230
Создание снимков экрана.....	231
Обнаружение содержимого.....	232
Ранее обнаруженные уязвимости.....	234
Тестирование приложений.....	234

---

Стек технологий.....	235
Определение возможностей приложения .....	236
Обнаружение уязвимостей .....	237
Дальнейшие действия .....	239
Автоматизация работы .....	239
Анализ мобильных приложений.....	239
Определение новых возможностей.....	240
Отслеживание файлов JavaScript.....	240
Платный доступ к новым возможностям .....	240
Изучение технологий .....	241
Итоги.....	241
<b>Глава 20. Отчеты об уязвимостях.....</b>	<b>242</b>
Прочитайте условия программы .....	242
Чем больше подробностей, тем лучше.....	243
Перепроверьте уязвимость .....	243
Ваша репутация .....	244
Относитесь к компании с уважением .....	245
Подача апелляции в программах Bug Bounty .....	247
Итоги.....	248
<b>Дополнение А. Инструменты .....</b>	<b>249</b>
Веб-прокси .....	249
Поиск поддоменов .....	251
Исследование содержимого .....	252
Создание снимков экрана .....	252
Сканирование портов .....	253



Предварительное исследование .....	254
Инструменты для хакинга .....	255
Взлом мобильных устройств .....	257
Расширения для браузера .....	257
<b>Дополнение Б. Дополнительный материал.....</b>	<b>259</b>
Онлайн-курсы.....	259
Платформы Bug Bounty.....	261
Список рекомендованных источников.....	262
Видеоматериалы .....	264
Рекомендуемые блоги.....	265