

УДК 004.382
ББК 32.973-018
П85

П85 Эдриан Прутяну

Как стать хакером: Сборник практических сценариев, позволяющих понять, как рассуждает злоумышленник / пер. с англ. Д. А. Беликова – М.: ДМК Пресс, 2020. – 380 с.: ил.

ISBN 978-5-97060-802-9

Данная книга представляет собой руководство по защите веб-приложений от вредоносных воздействий. Рассматривая всевозможные уязвимости с позиции злоумышленника, автор дает читателям ключ к надежной защите своих ресурсов.

В книге рассматриваются наиболее часто встречающиеся уязвимости и показано, как хакер может использовать их в своих целях. Наряду с этим приводятся практические советы по предупреждению атак. Рассмотрены сценарии, в которых целью атаки может быть популярная система управления контентом или контейнерное приложение и его сеть.

Издание предназначено опытным разработчикам веб-приложений, специалистам по DevOps, а также будет полезно всем читателям, интересующимся хакерскими атаками и их противодействию.

УДК 004.382
ББК 32.973-018

Copyright ©Packt Publishing 2019. First published in the English language under the title «Becoming the Hacker» – (9781788627962).

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 978-1-78862-796-2 (англ.)
ISBN 978-5-97060-802-9 (рус.)

Copyright © 2019 Packt Publishing.
© Оформление, перевод на русский язык, издание,
ДМК Пресс, 2020

Оглавление

Об авторе	9
О рецензентах	10
Предисловие от издательства	11
Отзывы и пожелания	11
Список опечаток.....	11
Нарушение авторских прав	11
Предисловие.....	12
Кому адресована эта книга	12
О чем идет речь в книге	12
Как извлечь максимум из книги?.....	13
Загрузка примеров	14
Загрузка цветных изображений	14
Условные обозначения.....	15
Глава 1. Атаки на веб-приложения. Введение.....	16
Правила применения оружия	17
Обмен данными	18
Вопросы конфиденциальности данных	20
Очистка	21
Инструментарий тестировщика	22
Kali Linux	23
Альтернативы Kali Linux.....	23
Прокси-сервер	25
Burp Suite.....	25
Zed Attack Proxy	26
Облачная инфраструктура	27
Дополнительные источники.....	28
Упражнения	29
Резюме.....	29
Глава 2. Эффективное обнаружение	31
Типы тестирования	31
Построение карты сети	33
Masscan.....	35
hatWeb	37
Nikto	37
CMS-сканеры	38
Эффективная атака методом полного перебора.....	39

Средства сканирования	42
Постоянное картирование контента.....	46
Обработка полезной нагрузки.....	49
«Полиглот»	59
Тот же вирус, но другой контекст	64
Запутывание (обфускация) кода	66
Дополнительные источники.....	68
Упражнения	69
Резюме.....	69
Глава 3. Легкая добыча	70
Анализ сети	70
Ищем вход.....	73
Определение учетных данных	75
Есть способ получше	82
Очистка	86
Дополнительные ресурсы	87
Резюме.....	87
Глава 4. Продвинутые способы атаки с использованием метода полного перебора	89
Распыление подбора пароля.....	89
Спросим LinkedIn	92
Метаданные	96
Кассетная бомба	97
За семью прокси-серверами	101
Tor	102
ProxyCannon.....	109
Резюме.....	114
Глава 5. Внедрение файлов.....	115
Удаленное внедрение файлов.....	116
Локальное внедрение файлов.....	118
Внедрение файла для удаленного выполнения кода	127
Другие проблемы, связанные с загрузкой файлов.....	129
Резюме.....	134
Глава 6. Обнаружение и эксплуатация уязвимостей в приложениях с помощью внешних сервисов.....	135
Распространенный сценарий	136
Командно-контрольный сервер	137
Центр сертификации Let's Encrypt	139
INetSim	143
Подтверждение	148
Асинхронное извлечение данных	149

Построение выводов на основе анализа данных	152
Резюме.....	154
Глава 7. Автоматизированное тестирование	155
Расширение функциональных возможностей Burp Suite.....	155
Нелегальная аутентификация и злоупотребление учетными записями	158
Швейцарский нож	162
Запутывание кода.....	169
Collaborator	172
Открытый сервер	173
Выделенный сервер Collaborator.....	179
Резюме.....	184
Глава 8. Вредоносная сериализация.....	186
Использование десериализации	186
Атака на пользовательские протоколы.....	194
Анализ протокола.....	195
Эксплойт для осуществления атаки	199
Резюме.....	206
Глава 9. Практические атаки на стороне клиента	208
Правила ограничения домена	208
Совместное использование ресурсов разными источниками	212
Межсайтовый скриптинг	214
XSS-атака, основанная на отраженной уязвимости	214
Постоянный XSS	215
DOM-модели	217
Межсайтовая подделка запроса	219
BeEF	222
Перехват.....	227
Атаки с применением методов социальной инженерии	231
Кейлоггер	234
Закрепление в системе	240
Автоматическая эксплуатация.....	242
Туннелирование трафика	247
Резюме.....	249
Глава 10. Практические атаки на стороне сервера	250
Внутренние и внешние ссылки	251
Атаки XXE.....	253
Атака billion laughs.....	253
Подделка запроса	255
Сканер портов.....	259
Утечка информации.....	262
«Слепой» XXE.....	268
Удаленное выполнение кода	273

Резюме.....	279
Глава 11. Атака на API.....	280
Протоколы передачи данных	281
SOAP	282
REST.....	284
Аутентификация с помощью API	286
Базовая аутентификация	286
Ключи API	287
Токены на предъявителя.....	288
JWT	288
JWT4B	293
Postman	295
Установка	297
Вышестоящий прокси-сервер	299
Среда выполнения.....	300
Коллекции.....	302
Запуск коллекции.....	308
Факторы атаки	310
Резюме.....	312
Глава 12. Атака на CMS.....	313
Оценка приложения	314
WPScan	314
sqlmap.....	321
Droopescan	322
Arachni.....	324
Взлом кода с помощью бэкдора	327
Закрепление в системе	328
Утечка учетных данных	339
Резюме.....	349
Глава 13. Взлом контейнеров	350
Сценарий уязвимости в Docker	353
Плაცдарм	354
Осведомленность о ситуации	362
Взлом контейнера	371
Резюме.....	377
Предметный указатель	378