SuperSliv.Biz - Курсы, Тренинги, Семинары, Каждый день!

ВЗЛОМ

От киберпанка до DevSecOps. 7 книг, ради которых DevSecOps-инженеру стоит выучить английский

Антон Карев, 13.02.2018 14 комментария 60,423 Добавить в закладки

Содержание статьи

Помнишь «весь спектр радуги» лучших книг из легендарного фильма «Хакеры»? Пересмотрев фильм еще раз, мы задались вопросом: а что бы сегодня читали киберпанки прошлого, ставшие в наше время DevSecOps'ами? И вот что у нас получилось...

«Радужная серия»

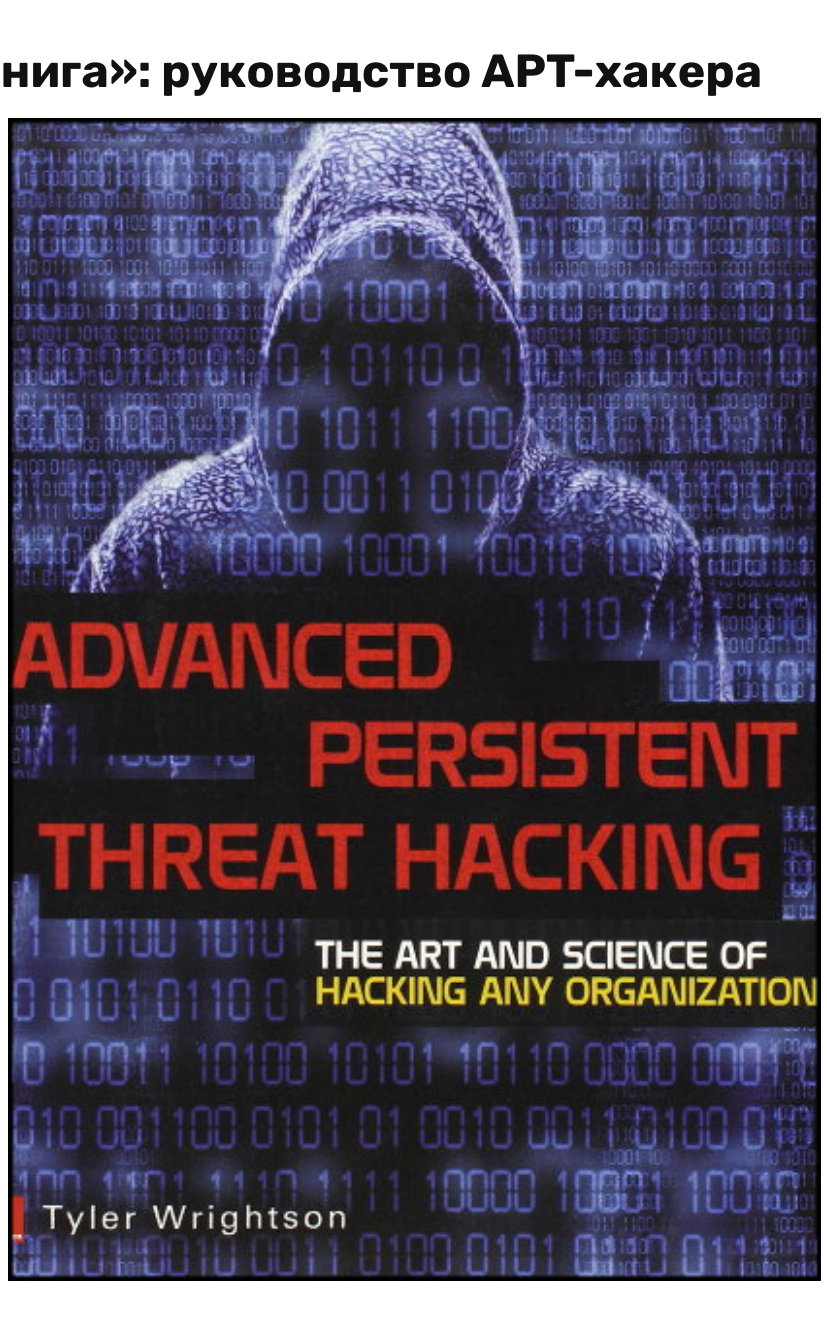
Другие статьи в выпуске:
Хакер #227. Meltdown и Spectre
Содержание выпуска
Подписка на «Хакер» -70%

- «Оранжевая книга»: критерии защиты данных компьютера по стандартам DOD.
- «Розовая рубашка»: справочник IBM (прозвали так из-за стремной розовой рубашки на мужике с обложки).
- «Книга дьявола»: библия UNIX.
- «Книга дракона»: разработка компилятора.
- «Красная книга»: сети национального управления безопасности (известна как «уродливая красная книга, которая не умещается на полке»).

Перевод фильма «Хакеры» не передает игру слов и порой искажает смысл. Ты смотрел его на английском?

- ○ Да, конечно!
- ○ Нет, но теперь посмотрю
- ○ Лучше потрачу время на книгу

«Фиолетовая книга»: руководство APT-хакера



***Tyler Wrightson.* Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organizations. 2015. 434 p.**

Эта книга написана ради одной-единственной цели: продемонстрировать, что в мире не существует безопасных систем. Причем написана она с позиции преступника, без компромиссов и лишней политкорректности. Автор беззастенчиво демонстрирует современные реалии кибер-не-безопасности и без утайки делится самыми интимными подробностями APT-хакерства. Такой брутальный подход к изложению материала можно понять: автор уверен, что только так мы сможем по-настоящему «узнать своего врага в лицо», как это советовал Сунь-цзы в своей книге «Искусство войны». Только мысля как хакер, безопасник сможет разработать сколь-нибудь эффективную защиту от киберугроз.

В книге описывается образ мыслей APT-хакера, инструменты и навыки — которые позволяют ему взламывать абсолютно любую организацию, вне зависимости от того, какая там развернута система безопасности. С демонстрацией реальных примеров взлома, для реализации которых вполне достаточно скромного бюджета и скромных технических навыков.

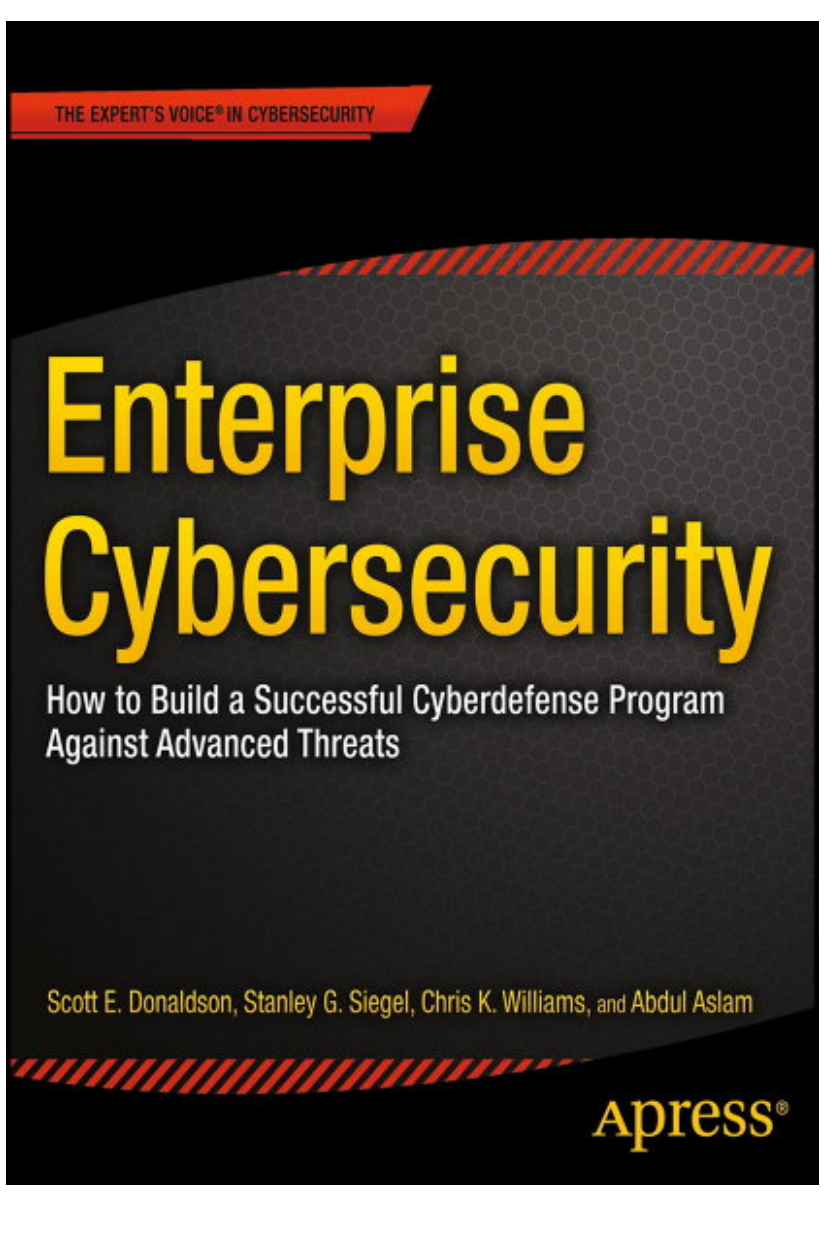
INFO

Всякий раз, когда мы читаем про «злые взломают всех, кто подключен хотя бы к сети 220 вольт», мы вспоминаем про нашу мифбрейкерскую статью Всемогущество взломщика: оцениваем реальную степень угрозы хакерских атак.

Тебе приходилось встречаться на практике с целенаправленными атаками (APT)?

- ○ Нет, кому я нужен
- ○ Да, я был жертвой атаки
- ○ Да, я их сам выполнял

«Черная книга»: корпоративная кибер(не)безопасность



***Scott Donaldson.* Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats. 2015. 536 p.**

В книге представлена гибкая и наглядная схема для управления всеми аспектами корпоративной программы кибербезопасности (КПК), в которой вся КПК разделена на 11 функциональных областей и на 113 предметных аспектов. Эта схема очень удобна для проектирования, разработки, внедрения, контроля и оценки КПК, управления рисками. Схема универсальна и легко масштабируется под нужды организации любых размеров. В книге подчеркивается, что абсолютная неуязвимость принципиально недостижима. Потому что, имея в запасе неограниченное время, предприимчивый злоумышленник может в конце концов преодолеть даже самую передовую киберзащиту. Поэтому эффективность КПК оценивается не в абсолютных категориях, а в относительных — двумя относительными показателями: **насколько быстро** она позволяет обнаруживать кибератаки и **насколько долго** она позволяет сдерживать натиск противника. Чем лучше эти показатели, тем больше у штатных специалистов времени на то, чтобы оценить ситуацию и принять контрмеры.

В книге подробно описаны все действующие лица на всех уровнях ответственности. Объясняется, как применять предложенную схему КПК для объединения разношерстных департаментов, скромных бюджетов, корпоративных бизнес-процессов и уязвимой киберинфраструктуры в рентабельную КПК, способную противостоять передовым кибератакам и способную значительно сокращать ущерб в случае пробоя. В рентабельную КПК, которая принимает во внимание ограниченность бюджета, выделенного на обеспечение кибербезопасности, и которая помогает находить нужные компромиссы, оптимальные именно для вашей организации. С учетом повседневной оперативной деятельности и долгосрочных стратегических задач.

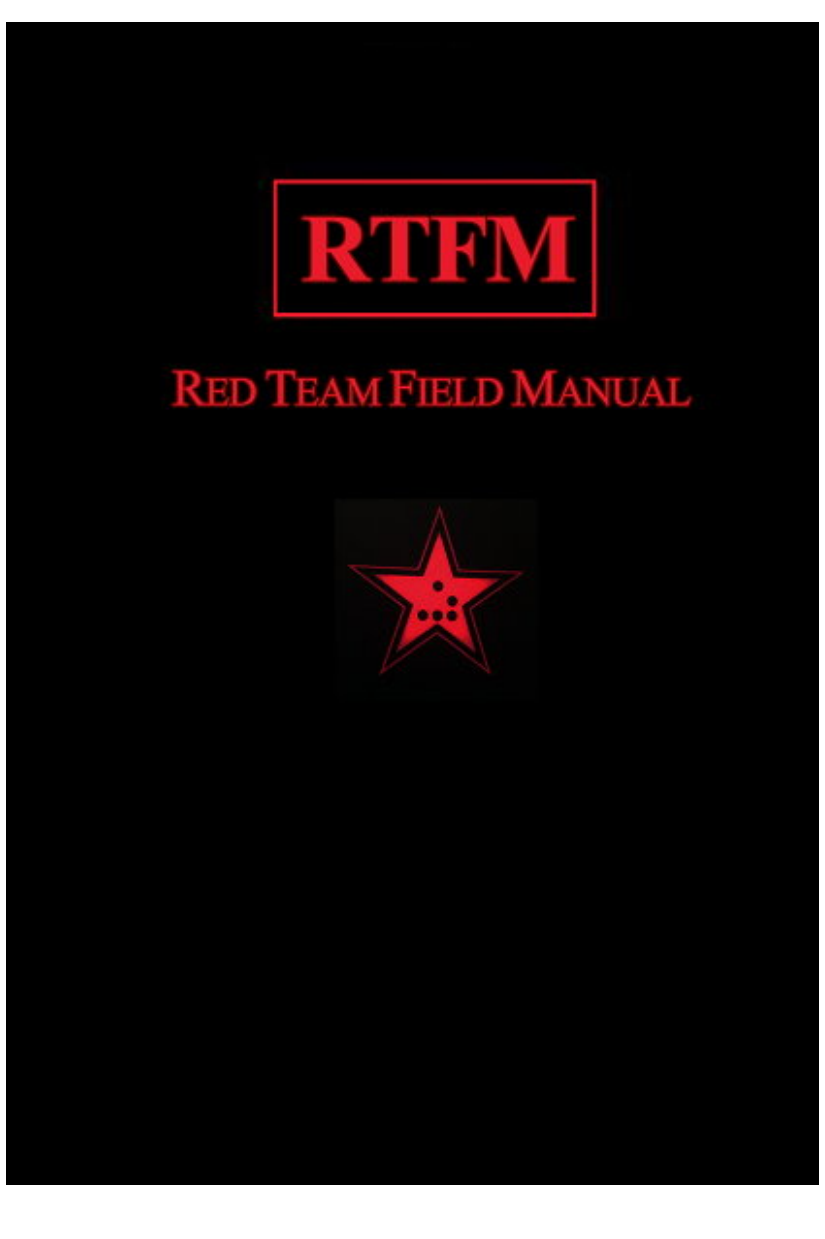
При первом знакомстве с книгой владельцы малого и среднего бизнеса, имеющие ограниченные бюджеты, могут посчитать, что для них представленная в книге схема КПК, с одной стороны, не по карману, а с другой — вообще излишне громоздка. И действительно: далеко не все предприятия могут позволить себе учитывать все элементы комплексной программы КПК. Когда генеральный директор работает по совместительству также финансовым директором, секретарем и службой технической поддержки — полномасштабная КПК явно не для него. Однако в той или иной степени проблему кибербезопасности приходится решать любому предприятию, и если почитать книгу внимательно, то можно увидеть, что представляемая схема КПК легко адаптируема под нужды даже самого маленького предприятия. Так что она подходит для предприятий любых размеров.

Следует заметить, что авторы книги — признанные эксперты по кибербезопасности, которым доводилось сражаться «на передовой» против APT-хакеров, отстаивая в разное время правительственные, военные и корпоративные интересы.

Как ты относишься к стандартам корпоративной безопасности?

- ○ Их надо выполнять неукоснительно
- ○ Они устаревают прежде, чем их сформулируют
- ○ Я один из тех, кто их пишет

«Красная книга»: справочник «красноармейца»



***Ben Clark.* RTFM: Red Team Field Manual. 2014. 96 p.**

В RTFM приведен базовый синтаксис основных инструментов командной строки (для Windows и Linux). Освещаются и оригинальные варианты их использования, в комплексе с такими мощными инструментами, как Python и Windows PowerShell. RTFM будет снова и снова экономить тебе целую кучу времени и сил, избавляя от необходимости вспоминать/искать трудно запоминающиеся нюансы операционной системы, связанные с такими инструментами, как Windows WMIC, инструменты командной строки DSQUERY, значения ключей реестра, синтаксис планировщика Task Scheduler, Windows-скрипты и так далее. Кроме того, что еще более важно, RTFM помогает своему читателю перенять наиболее передовые «красноармейские» техники.

Ты часто используешь командную строку?

- ○ Конечно! Скрипты и командлеты — наше все
- ○ Нет, кому она вообще нужна в эпоху GUI
- ○ иногда копирую команды из какой-нибудь статьи или справки

«Книга бизона»: культивирование DevOps-культуры в сообществе разработчиков

***Jennifer Davis, Ryn Daniels.* Effective DevOps: Building a Culture of Collaboration, Affinity, and Tooling at Scale. 2016. 410 p.**

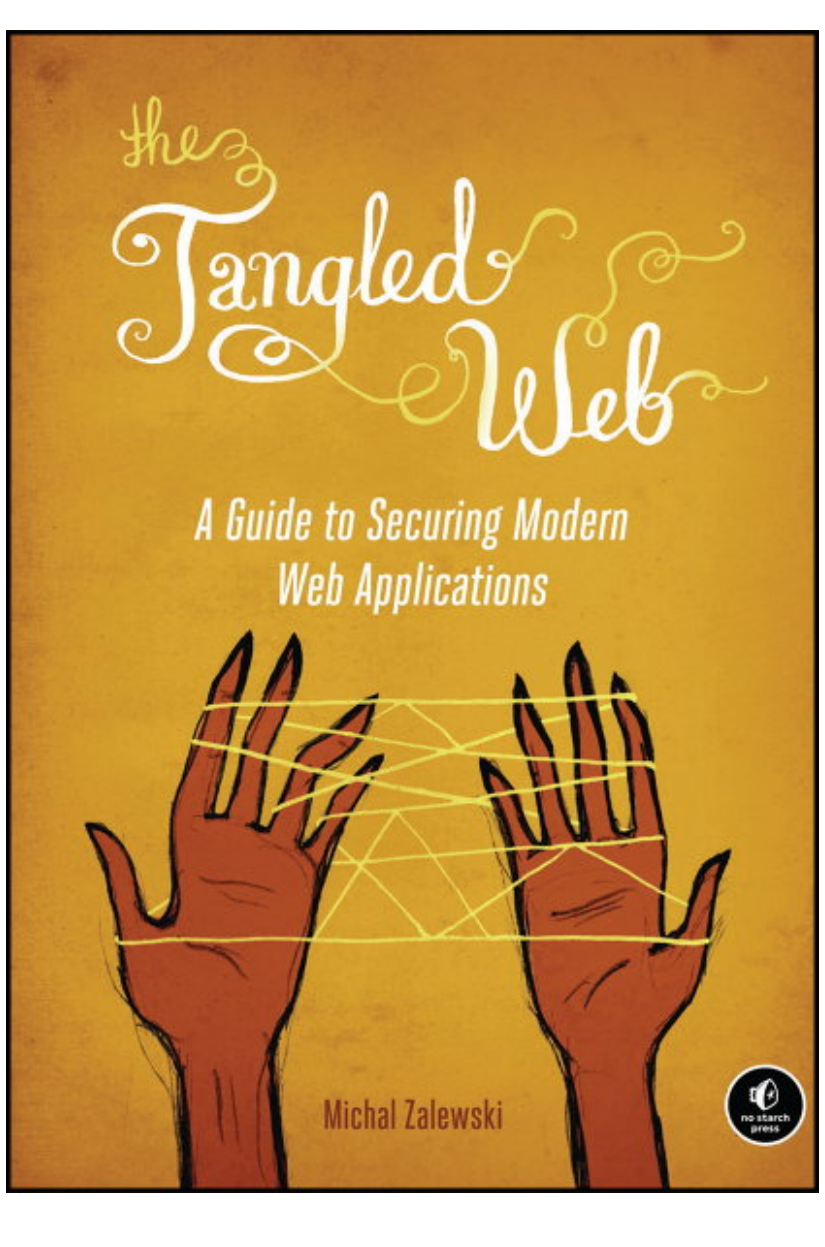
Книга бизона (названа так из-за зверя с обложки) — «самое удачное из ныне существующих пособий по формированию корпоративной DevOps-культуры». Чувствуешь, как от этих слов потянуло духом мутных психотренингов, коучинга, тимбилдингов и корпоративных гимнов? 🙂 Тем не менее почитать ее стоит (если не веришь во всю эту фигню — то хотя бы чтобы знать врага в лицо и быть готовым, когда тебя захотят сделать членом большой и дружной семьи счастливых работников). Впрочем, достаточно критики с позиции рядового члена команды — с точки зрения руководителя (а ведь они нас тоже читают), в этой книге DevOps рассматривается как новый способ мышления и работы, позволяющий формировать «умные команды».

«Умные команды» отличаются от прочих тем, что их члены понимают особенности своего образа мышления и применяют это понимание с пользой для себя и для дела. Такая способность «умных команд» развивается в результате систематической практики ToM (Theory of Mind, наука самоосознания). ToM-компонент DevOps-культуры позволяет распознавать сильные стороны — свои и своих коллег; позволяет улучшать понимание себя и других. В результате способность людей сотрудничать и сопереживать друг другу увеличивается. Организации с развитой DevOps-культурой реже допускают ошибки, быстрее восстанавливаются после сбоев. Сотрудники этих организаций чувствуют себя более счастливо. А счастливые люди, как известно, более продуктивны. Поэтому цель DevOps — выработка взаимопонимания и общих целей, позволяющих установить долговременные и прочные рабочие взаимоотношения между отдельными сотрудниками и целыми департаментами.

DevOps-культура — это своеобразный фреймворк, располагающий к тому, чтобы обмениваться ценным практическим опытом и развивать между сотрудниками сопереживание. DevOps — это культурная ткань, сплетенная из трех нитей: непрерывного выполнения должностных обязанностей, развития профессиональных компетенций и личного самосовершенствования. Эта культурная ткань «обволакивает» как отдельных сотрудников, так и целые департаменты, позволяя им эффективно и непрерывно развиваться в профессиональном и личном плане. DevOps помогает уйти от «старого подхода» (культуры упреков и поиска виноватых) и прийти к «новому подходу» (использование неизбежных ошибок не для порицания, а для извлечения практических уроков). В результате в команде увеличивается прозрачность и доверие — что очень благотворно сказывается на способности членов команды сотрудничать друг с другом.

Таково краткое содержание книги. Теперь можешь встать и спеть свой корпоративный гимн, даже если никто не слышит. 🙂

«Желтая паутина»: классическая подборка уязвимостей всемирной паутины



***Michal Zalewski.* The Tangled Web: A guide to Securing Modern Web Applications. 2012. 300 p.**

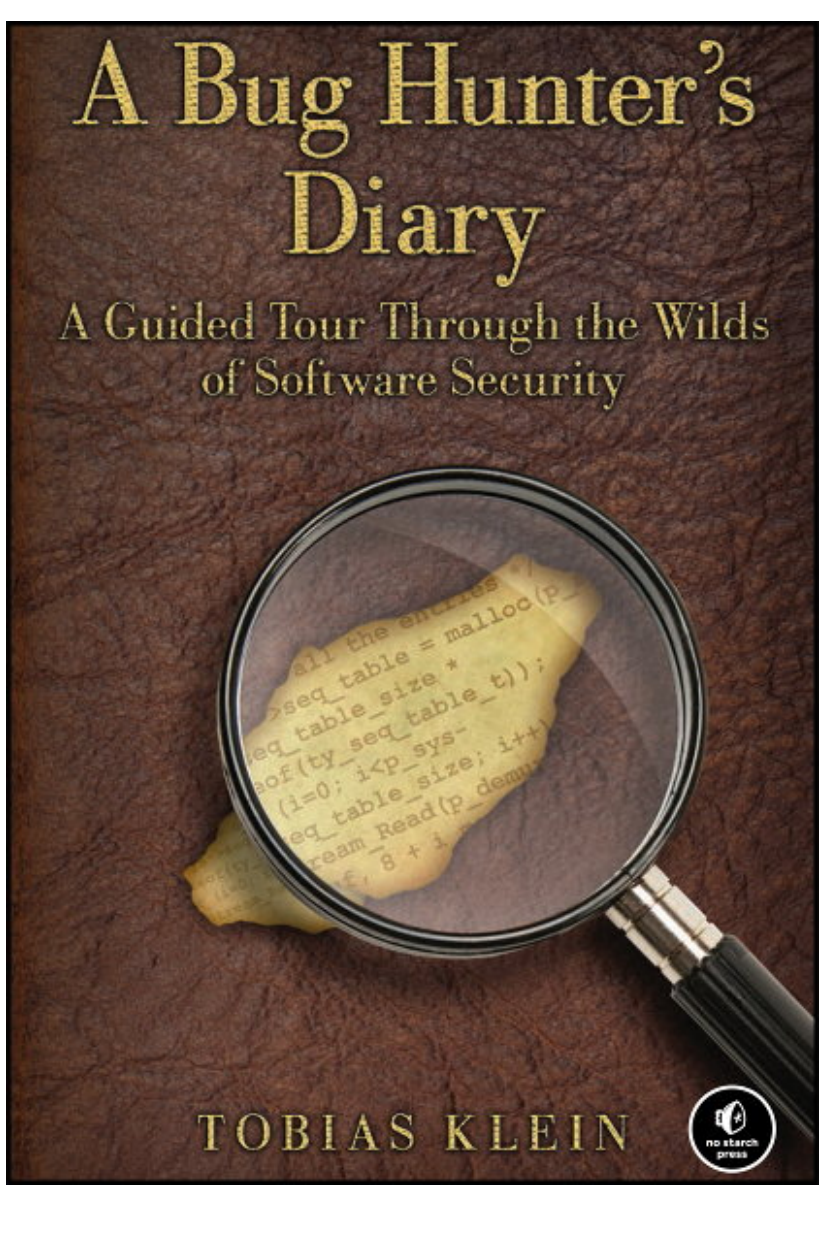
Всего каких-нибудь двадцать лет назад интернет был настолько же простым, насколько и бесполезным. Он представлял собой причудливый механизм, позволяющий небольшой кучке студентов и вундеркиндов посещать домашние странички друг друга. Подавляющее большинство таких страничек было посвящено науке, домашним питомцам и поэзии.

Архитектурные изъяны и недостатки реализации всемирной паутины, с которыми нам приходится мириться сегодня, — плата за историческую непредусмотрительность. Ведь это была технология, которая никогда не стремилась к тому глобальному статусу, который она получила сегодня. В итоге мы имеем очень уязвимую киберинфраструктуру: как выяснилось, стандарты, дизайн и протоколы всемирной паутины, которых было достаточно для домашних страничек с танцующими хомяками, совершенно недостаточно, скажем, для интернет-магазина, который ежегодно обрабатывает миллионы транзакций по кредитным картам.

Оглядываясь на прошлые два десятка лет, трудно не разочароваться: практически каждое сколь-нибудь полезное web-приложение, разработанное до сегодняшнего дня, было вынуждено заплатить кровавую цену за непредусмотрительность вчерашних архитекторов всемирной паутины. Мало того что интернет оказался куда более востребованным, чем это ожидалось, так мы еще и закрывали глаза на отдельные неудобные его характеристики, которые выходили за пределы зоны нашего комфорта. И ладно бы закрывали глаза в прошлом — мы продолжаем закрывать их и сейчас… Более того, даже очень хорошо спроектированные и тщательно проверенные веб-приложения все равно имеют гораздо больше проблем, чем их несетевые собратья.

Итак, мы порядком наломали дров. Пришло время покаяться. В целях такого покаяния эта книга и была написана. Это первая (и на данный момент лучшая в своем роде) книга, которая предоставляет систематический и тщательный анализ текущего (ну как «текущего», это скорее классика — 2012 год. — Прим. ред.) состояния безопасности веб-приложений. Для такого сравнительно небольшого объема текста количество рассмотренных нюансов просто ошеломительное. Более того, инженеры-безопасники, ищущие быстрых решений, порадуются наличию чит-листов, которые можно найти в конце каждого раздела. В этих чит-листах описываются эффективные подходы для решения наиболее злободневных проблем, с которыми сталкивается разработчик веб-приложений.

«Коричневая книга»: книга «багоборца»



***Tobias Klein.* A Bug Hunter 's Diary: A Guided Tour Through the Wilds of Software Security. 2011. 208 p.**

Одна из интереснейших книг, вышедших за последнее десятилетие. Ее посыл можно резюмировать следующими словами: «Дайте человеку эксплоит, и вы сделаете его хакером на один день, научите его эксплуатировать ошибки — и он останется хакером на всю жизнь». Читая «Дневник багоборца», ты проследуешь за практикующим экспертом кибербезопасности, который выявляет ошибки и эксплуатирует их в самых популярных на сегодняшний день приложениях, таких как Apple iOS, VLC-медиаплеер, веб-браузеры и даже ядро Mac OS X. Читая эту уникальную в своем роде книгу, ты получишь глубокие технические знания и понимание того, какой у хакеров подход к трудноразрешимым проблемам, а также в каком экстазе они находятся в процессе охоты на баги.

Из книги ты узнаешь:

- как пользоваться проверенными временем методами поиска багов, такими как трассировка вводимых пользователем данных и реверс-инжиниринг;
- как эксплуатировать уязвимости, такие как разыменование NULL-указателей, переполнение буфера, огрехи преобразования типов;
- как писать код, демонстрирующий наличие уязвимости;
- как грамотно уведомлять вендоров о выявленных в их софте багах.

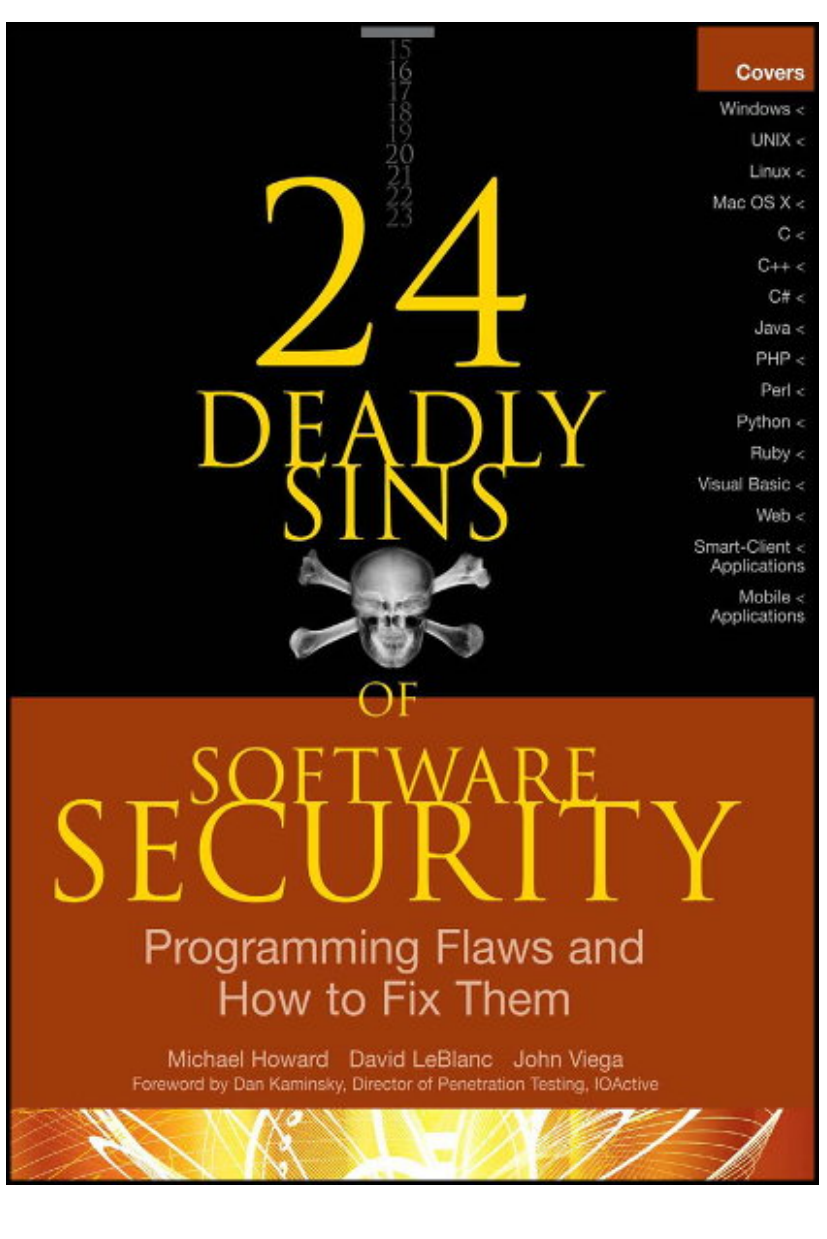
«Дневник багоборца» испещрен реальными примерами уязвимого кода и авторскими программами, разработанными для облегчения поиска багов.

Ради какой бы цели ты ни охотился за багами, будь то развлечение, заработок или же альтруистическое стремление сделать мир более безопасным, эта книга поможет развить ценные навыки, поскольку с ее помощью ты заглядываешь через плечо профессионала-багоборца, и не только на экран его монитора, но и в его голову. Максимальную отдачу от книги получат те, кто хорошо знаком с языком программирования C/C++ и x86-ассемблером.

Тебе приходилось применять эксплоиты?

- ○ Да, я даже на какое-то время почувствовал себя хакером
- ○ Да, я их регулярно пишу
- ○ Нет, мне проще хакнуть человека

«Книга возмездия»: библия безопасной разработки кода



***Michael Howard, David LeBlanc, John Viega.* 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them. 2010. 394 p.**

Сегодня любой разработчик софта просто обязан обладать навыками написания безопасного кода. Эта книга вскрывает 24 принципиальных момента, очень некомфортных для разработчиков софта. Некомфортных в том плане, что разработчики практически всегда допускают тут серьезные огрехи. В книге представлены практические советы, каким образом при разработке софта избежать этих огрехов и как протестировать на их наличие уже имеющийся софт, написанный другими людьми. Повествование книги простое, доступное и основательное.

Эта книга будет ценной находкой для любого разработчика, независимо от языка, который он использует. Она будет полезна всем тем, кто заинтересован в разработке качественного, надежного и безопасного кода. В книге наглядно продемонстрированы наиболее распространенные и опасные огрехи сразу для нескольких языков (C++, C#, Java, Ruby, Python, Perl, PHP и другие), а также приведены проверенные временем и хорошо зарекомендовавшие себя техники, позволяющие искупить грехи долгих лет косячного, небезопасного программирования. 🙂

Руководители некоторых софтверных компаний используют эту книгу для проведения блиц-тренингов непосредственно перед началом разработки нового софта. Обязывают разработчиков прочитать из этой книги разделы, затрагивающие технологии, с которыми им предстоит иметь дело. Книга разбита на четыре «греховных» раздела, посвященных веб-софту, разработке, криптографии и сетевым проблемам.

Скачано с сайта - SuperSliv.Biz - Присоединяйся!