SUMMER READING & LISTENING

Summer's longer days and slower pace invite us to pick up a book, follow our questions, and try our hand at something new. For developers who would like to learn more about security, here are some favorite books, podcasts, blogs, and hands-on exercises of Veracoders across our development, security, and product teams. From a just-published page-turner to classic *Phrack* articles, there's something here for everyone who is interested in information security. So dip your toe in or take a deep dive — happy summer and happy learning!

BOOKS

Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World

Joseph Menn

Joe Menn, an investigative technology reporter with *Reuters,* tells the fascinating story of the seminal hacking group Cult of the Dead Cow. Menn traces the origins of ethical hacking back more than two decades, portraying young hackers grappling with the ethical implications of their knowledge and abilities at a time when the world was growing more connected. Individually and collectively, these technologists have had an enormous influence on the way we think about information—and its protection.

The Art of Deception: Controlling the Human Element of Security

Kevin D. Mitnick & William L. Simon

After serving time for his computer crimes, famed hacker Kevin Mitnick went straight and began sharing his knowledge as a security consultant and writer. In *The Art of Deception,* he covers a critical and deeply interesting area of information security—human behavior. A master of social engineering, Mitnick illuminates the many ways that human nature can be exploited by attackers.

The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations

Gene Kim, Jez Humble, Patrick Debois & John Willis

This is one of the most comprehensive texts on the subject that brings together a lot of the core ideas that go into implementing DevOps. Its authors bring their experience as consultants on the subject as well as their personal DevOps experiences within their own organizations.

The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win

Gene Kim, Kevin Behr & George Spafford

This classic is a novelization of the experience that a company might have in rolling out DevOps processes throughout their organization. Sometimes oversimplified, but by using a fictional narrative rather than technical and process descriptions, the book helps readers visualize how DevOps may work in their own teams.

01 CONTRIBUTORS

KAYLA FIRESTACK
Dynamic Scan Engineer

SARAH GIBSON
Application Penetration Tester

RUTH HATCH
Associate Software Engineer

JON JANEGO
Product Manager

TIM JARRETT
Director, Product Management

CHRIS KIRSCH
Director, Product Marketing

TYLER KRAUSE FERRIS
Application Security Consultant

MARK KRIEGSMAN
Director, Developer Research

DAN MURPHY
Senior Principal Software Engineer

ATHENA WASHINGTON
Software Engineer

DIVE INTO THE CLASSICS with Dan Murphy

Shakespeare. Brontë. Dickens. In literature, the classics have long been a staple of summer reading lists. Computer security has its own share of classics — reference points that serve as a foundation for understanding the field's ever-changing chessboard of attack and defense. This list of computer security summer reading can be enjoyed either lounging on the beach with sand beneath your toes, or curled up in bed with your face lit by the blue-filtered midnight glow of a tablet. Whether you are a new developer interested in learning more about computer security, or a seasoned practitioner looking to revisit some of the seminal works in the field, I hope that you enjoy the articles below as much as I did when I first stumbled across them!

DIVE INTO MORE CLASSICS AT
VERACODE.COM/DIVEINTOTHECLASSICS

Smashing the Stack for Fun and Profit

phrack.org/issues/49/14.html

Aleph One's *Smashing the Stack for Fun and Profit* was truly eye-opening when it was first introduced. Sometimes the answer to "what does this block of code do?" can be "anything the caller wants it to!" This concept lives on in more modern incarnations like XSS and SQL injection, but Smashing the Stack is the granddaddy of code injection. I originally encountered it independently, and was pleasantly surprised years later when it resurfaced as legitimate assigned reading for a grad class. Taking the time to write some shell code is valuable to understanding the fundamentals of how code executes, and is a great puzzle.

Check out travisf.net/smashing-the-stack-today for tips on recreating the environment today.

OG ODBC

phrack.org/issues/54/8.html

Under the inauspicious heading of "ODBC and MS SQL server 6.5," this article explores a simple concept: what could happen if a web application copies the strings received from HTML form elements directly to SQL statements? We all know how that one ended. Twenty years later, there are more than 37 million Google hits for "sql injection." By now, **Bobby Tables** is applying for his first job after graduating from "University'); DROP TABLE applicants; --", and still getting results!

Tick TOC Tick TOU

usenix.org/legacy/events/fast05/tech/full_papers/wei/wei.pdf

Another class of attacks worth some summer reading is Time-of-Check to Time-of-Use. Sometimes the security put in place to thwart an attack has a race condition that can still allow an attacker to circumvent it. *TOCTTOU Vulnerabilities in UNIX-Style File Systems: An Anatomical Study* is a great introduction to the concept, with some specific examples. You can get a more hands-on appreciation by doing (spoiler alert!) Level 2 of overthewire.org's Leviathan challenge at **overthewire.org/wargames/leviathan/**.

While the specifics for these classes of attacks have changed, the concepts are still very relevant: this spring (May 2019), a high-profile Docker bug — attributed to a TOCTOU flaw — allowed containers to break out and overwrite any file on the host as root. See **duo.com/decipher/docker-bug-allows-root-access-to-host-file-system** and **seclists.org/oss-sec/2019/q2/131**.

PODCASTS

Darknet Diaries

darknetdiaries.com

Darknet Diaries turns real security events into suspenseful and insightful stories. I often find myself spending a few minutes in the car after I've arrived, just so that I can listen to how the story evolves. You'll feel more like you're listening to a spy thriller or heist movie than an industry podcast.

— CHRIS KIRSCH

SANS Internet Storm Center's Stormcast

isc.sans.edu/podcast.html

The SANS Internet Storm Center is a global, cooperative monitoring and alerting system featuring daily handler diaries summarizing and analyzing new threats to networks and Internet security events. Every day I listen to the *Stormcast* on the way to work; it's a 5–10 minute podcast that covers "what's burning on the Internet security fire today?" It's a daily reminder to think about things like hardcoded passwords, [de]serialization bugs, and more.

— MARK KRIEGSMAN

Risky Business

risky.biz

Risky Business is my go-to podcast for keeping up-to-date on current events in information security, both from a technical and political perspective. Each podcast starts out with a discussion of the week's security news as a conversation between two experts that is engaging to listen to. Then, the podcast goes into a feature interview with truly interesting people and closes with a short vendor interview that is refreshingly honest.

— CHRIS KIRSCH

HANDS-ON

Hands-on experience with security vulnerabilities can be hard to come by. These two projects are learning tools to acquaint you with how vulnerabilities work in the wild. Even if you're only interested in knowing how your own code might misbehave, these are great resources for getting started learning how security flaws manifest, what attackers do to trigger them, and what an attacker can do once the flaw has been exploited.

Google XSS Game

xss-game.appspot.com

The *Google XSS* game walks you through different types of cross-site scripting (XSS), while also showing how some mitigations can be circumvented. Don't forget the hints! These levels can be hard if it's your first time popping XSS.

OWASP Juice Shop

owasp.org/index.php/OWASP_Juice_Shop_Project

The *OWASP Juice Shop* project is a known vulnerable web app designed with a modern client-side framework. Security findings are a little different when the processing of an application moves to the browser. This is a fun project for finding bugs and getting points in an up-to-date application.

BLOGS

Schneier on Security

schneier.com

Internationally renowned cryptography expert, author, and public-interest technologist Bruce Schneier has been writing about wide-ranging security and privacy issues on his immensely popular blog since 2004 and in his monthly Crypto-Gram newsletter since 1998.

Krebs on Security

krebsonsecurity.com

Investigative reporter and author Brian Krebs built his knowledge and reputation as a technology and security reporter for *The Washington Post*. Through his tenacious reporting and unparalleled network of sources in the cybercrime underground, Krebs has become known for his work exposing and reporting on massive data breaches. His highly regarded blog covers cybercrime.

The Security Ledger

securityledger.com

The widely read *Security Ledger* and its associated podcast offer security news, analysis, and opinion, all informed by the experience and perspective of publisher and editor-in-chief Paul Roberts, a veteran security reporter and analyst with 15 years' experience covering the industry. Contextualized and in-depth, the content has a particular focus on the intersection of cybersecurity with the Internet of Things.

VERACODE

Visit the **Veracode Community**, a supportive community of developers and security practitioners sharing knowledge about all things application security.