# Hack the Web: The Secrets Behind How the Internet Really Works

**Hackers don’t break the rules. They learn how the rules are written.**

**Copyright © 2025 by Codelivly**

All rights reserved. No part of this book may be reproduced or distributed in any form without prior written permission from the author, except for brief quotations used in reviews or educational purposes under fair use.

The author has made every effort to ensure the accuracy of the content but assumes no responsibility for errors or omissions. This book is provided “as is” without any warranties, express or implied.

For inquiries, contact: **support@codelivly.com**

# Foreword

I want to let you in on a little secret: for the first year of my career in tech, I had no idea how the web *really* worked.

Sure, I could build a website. I knew about code and servers. But the magic that happened between you clicking a link and a secure page loading? The handshakes, the cryptography, the silent guardians working overtime to keep your data safe? I treated that like, well, magic. It was a black box, and I was just happy it worked.

Then, I started working in security. And let me tell you, the moment you peer inside that black box is the moment the web transforms from a magical convenience into the most beautifully complex and fascinating machine ever built.

I remember the first time I truly understood how the TLS handshake that "S" in HTTPS works. It wasn't with dry, academic texts. It was when someone drew me a simple diagram with envelopes, locks, and two colors of ink, explaining it like a secret message passed in class. The lightbulb went off. *Oh!* That's why it's secure! That's what those "certificate errors" actually mean!

That "***aha***!" moment is what this book is all about.

The world often makes web security sound intimidating. It's portrayed as a domain for genius hackers in dark rooms, filled with impenetrable jargon. But the truth is, the core principles are elegant, logical, and honestly, pretty cool. Understanding them doesn't just make you more secure; it makes you a more empowered citizen of the digital world. When you know how the locks on your doors are made, you're better at choosing which doors to walk through.

In these pages, you won't find a dense textbook. You'll find a friendly guide.

You'll learn how your browser proves a website is who it says it is. You'll understand how your password stays safe on its journey across the internet. You'll see the common tricks attackers use, not as scary boogeymen, but as puzzles with understandable solutions.

I wish I had this book when I was starting out. It would have saved me years of treating the most brilliant parts of the web as mere magic. My hope for you is that you close this

book with the same sense of wonder and clarity I felt all those years ago the wonder of seeing the incredible, secure machine we all use every day, finally, for what it is.

Now, turn the page, and let's start pulling back the curtain.

**Stay curious,**

Rocky

Man behind Codelivly

# Table Of Contents

**Introduction: The Illusion of Simplicity..... 11**
What Happens "Behind the Curtain"?..... 12
Who This Book Is For..... 13
A Note on the Mindset: Thinking Like a Defender (and an Attacker)..... 14
**Part I: The Foundation – The Language of the Web..... 16**
Chapter 1: It Starts with a Request..... 17
The Client-Server Model: A Digital Conversation..... 17
Deconstructing an HTTP Request: What Your Browser Actually Says..... 18
Understanding HTTP Responses: The Server's Reply..... 20
The Critical Upgrade: Why HTTPS is Non-Negotiable..... 22
Chapter 2: The Web's Address Book: DNS Explained..... 24
What is a Domain Name, Really?..... 24
The Journey of a DNS Lookup: From URL to IP Address..... 25
DNS Records: A, AAAA, CNAME, MX..... 27
The Security Risks: DNS Hijacking and Cache Poisoning..... 29
Chapter 3: Beyond the Page Refresh: WebSockets & Real-Time Communication..... 31
The Limits of HTTP: The Request-Response Cycle..... 32
What are WebSockets? Opening a Two-Way Street..... 33
Use Cases: Live Chat, Gaming, and Financial Tickers..... 34
Security Considerations for Persistent Connections..... 35
Chapter 4: Speaking in Code: How Browsers Understand Servers..... 37
The Role of HTML, CSS, and JavaScript..... 38
The Document Object Model (DOM): The Browser's Blueprint..... 41
Introduction to APIs: How Websites Talk to Each Other..... 43
The Rise of Single-Page Applications (SPAs)..... 45
**Part II: The Infrastructure – Where the Web Lives..... 47**
Chapter 5: Behind the Curtain: A Primer on Server Architecture..... 48
What is a Server, Actually? Hardware in a Data Center..... 48
Operating Systems, Web Servers (Nginx, Apache), and Runtime Environments.. 50
The Cloud Explained: IaaS, PaaS, and SaaS..... 51
Virtualization and Containers (Docker)..... 53
Chapter 6: The Invisible Shield: Content Delivery Networks (CDNs) & DDoS Protection..... 55
What is a CDN and How Does it Work?..... 55
How CDNs Improve Performance and Security..... 57

Mitigating DDoS Attacks: Absorbing the Digital Tsunami..... 58
Bot Management: Separating Humans from Malicious Automation.....60
**Part III: The Shield – Cryptography and Secure Connections.....63**
Chapter 7: The Bedrock of Trust: Introduction to Cryptography..... 64
Symmetric vs. Asymmetric Encryption: A Simple Analogy..... 65
Hashing: The Digital Fingerprint..... 67
Digital Signatures: Proving Identity and Integrity..... 70
Chapter 8: The TLS Handshake: The Secret Handshake of the Web..... 73
The "S" in HTTPS: What is TLS/SSL?..... 74
Step-by-Step: The TLS Handshake Demystified..... 75
The Role of Certificates and Certificate Authorities (CAs)..... 77
How Your Browser Verifies a Website's Identity..... 79
Chapter 9: Keys, Certificates, and the Chain of Trust..... 82
Public Key Infrastructure (PKI) in Plain English..... 82
What is an SSL/TLS Certificate?..... 83
Types of Validation: Domain, Organization, and Extended Validation..... 85
The Problem with Trust: CA Breaches and Mis-issuance..... 87
**Part IV: The Guardians – Protecting Data and Identity.....91**
Chapter 10: You Are What You Eat (Cookies): Session Management..... 92
Why the Web Needs a Memory: The Problem of Statelessness..... 92
First-Party vs. Third-Party Cookies..... 94
Session Cookies vs. Persistent Cookies..... 96
Secure and HttpOnly Flags: The Security You Don't See..... 98
Chapter 11: Proving Who You Are: Authentication Deep Dive..... 102
Beyond Usernames and Passwords..... 102
How Password Hashing Really Works (with Salts and Peppers)..... 104
The Magic of Tokens: JWT (JSON Web Tokens) Explained..... 107
The Modern Standard: OAuth 2.0 and OpenID Connect (OIDC)..... 110
Chapter 12: Deciding What You Can Do: Authorization..... 113
Authentication vs. Authorization: "Who are you?" vs. "What can you do?"..... 113
Common Models: Role-Based Access Control (RBAC)..... 115
Permission Checks in Modern Web Applications..... 119
**Part V: The Attackers – Common Threats and Vulnerabilities..... 125**
Chapter 13: The Classics: SQL Injection and Cross-Site Scripting (XSS)..... 126
How SQL Injection Turns a Input Box into a Database Peephole..... 126
Defensive Coding: The Power of Prepared Statements..... 129
Understanding Stored, Reflected, and DOM-based XSS..... 132
How Content Security Policy (CSP) Acts as a Last Line of Defense..... 135

Chapter 14: Tricking the User: Cross-Site Request Forgery (CSRF) and Phishing....140
The Silent Attack: How CSRF Makes Your Browser an Accomplice.....140
Modern Defenses: Anti-CSRF Tokens and SameSite Cookies.....143
The Human Element: Anatomy of a Phishing Attack.....147
Chapter 15: The Human Factor: Social Engineering and Psychological Attacks.....153
Beyond Phishing: Pretexting, Baiting, and Quid Pro Quo.....153
Why Strong Technology Can Be Defeated by a Simple Phone Call.....157
Cultivating a Security-Aware Culture.....160
Chapter 16: The OWASP Top Ten: A Rundown of Critical Risks.....165
Broken Access Control.....165
Cryptographic Failures.....167
Insecure Design.....169
Security Misconfiguration.....172
A High-Level Overview of the Other Critical Risks.....174
**Part VI: The Defense – Architecture and Best Practices.....179**
Chapter 17: Building a Fortress: Secure Architecture & Hardening.....180
The Principle of Least Privilege.....180
Defense in Depth: Layering Your Security.....183
Securing Servers: Firewalls, Updates, and Minimal Surfaces.....186
The Role of Web Application Firewalls (WAFs).....190
Chapter 18: Security in the Modern Workflow: DevSecOps.....196
Shifting Left: Integrating Security from the Start.....197
Automated Security Testing: SAST, DAST, and SCA.....200
Secrets Management: Never Hardcode a Password Again.....207
The Future: AI and Security.....211
**Part VII: The Bigger Picture – Privacy, Regulations, and The Future.....217**
Chapter 19: Your Digital Shadow: Data Privacy and Regulations.....218
What is Personal Identifiable Information (PII)?.....218
Understanding GDPR, CCPA, and Other Privacy Laws.....221
The Ethics of Data Collection and Usage.....226
Chapter 20: The Evolving Battlefield: Emerging Threats & Trends.....232
API Security: The New Attack Surface.....232
Supply Chain Attacks: Compromising the Foundation.....238
The Impact of Quantum Computing on Cryptography.....243
Chapter 21: Becoming a Security-Conscious Citizen of the Web.....250
Practical Security Tips for End Users.....250
How to Think Like a Security Professional.....255
Conclusion: The Never-Ending Journey.....260

Security is a Process, Not a Product....260
The Shared Responsibility Model....263
**Appendices....269**
Appendix A: Glossary of Key Terms....269
Appendix B: Further Reading & Resources....273
Essential Websites....273
Recommended Books and Courses....274
Security-focused Browser Extensions....275
Appendix C: A Developer's Security Checklist....276
Authentication & Authorization....276
Input Validation & Output Encoding....276
Database Security....277
Communication Security....277
Application Infrastructure....278
Security Headers....278
Dependencies & Third-Party Code....278
Security Testing....279
Error Handling & Logging....279
Deployment & Operations....279
Compliance & Privacy....280
Quick Security Review Before Deployment....281

# Acknowledgments

This book represents the collective wisdom of countless security professionals, researchers, and practitioners who have dedicated their careers to making the digital world safer for everyone. While any errors or omissions are my own, the insights contained in these pages stand on the shoulders of giants.

First, to the security researchers and engineers who tirelessly work to uncover vulnerabilities and build better defenses your work often goes unrecognized until something goes wrong, but it's essential to our collective safety. The white hats, the bug bounty hunters, the open-source maintainers are the unsung heroes of the digital age.

To the educators and mentors who patiently explain complex security concepts to new generations of professionals, your work ensures that knowledge is passed forward and that we continue to raise the bar for security across the industry.

To the technical reviewers who provided invaluable feedback on early drafts—your sharp eyes and deep expertise caught errors I missed and improved explanations throughout. This book is immeasurably better because of your contributions.

To the open-source community the developers who build the tools, libraries, and frameworks that power the modern web while maintaining remarkable security standards. Your work demonstrates that security and openness can coexist and even reinforce each other.

To the organizations that prioritize security even when it's not the most visible investment you prove that doing the right thing is also good business, and you set examples for others to follow.

To my colleagues and students over the years our conversations, debates, and collaborative problem-solving sessions have shaped my understanding of what makes security work in practice, not just in theory.

To the victims of security breaches who have shared their stories, your courage in speaking out helps others avoid similar fates and drives improvement across the industry.

And finally, to you, the reader, for investing your time in understanding these complex topics. By learning about security, you're not just protecting yourself; you're contributing

to a safer digital ecosystem for everyone. The most secure future is one where we all take responsibility for understanding the technology we depend on.

This book is dedicated to everyone who believes that technology should empower humanity without compromising our security, privacy, or autonomy. May we continue to build a web that is open, innovative, and safe for all who use it.

# Introduction: The Illusion of Simplicity

You are a magician.

Open your laptop or tap your phone. Type a web address `https://www.yourbank.com`, perhaps and press Enter. In less time than it takes to blink, a login page appears. You enter your credentials, and just like that, you're gazing at your financial life: your balance, your transactions, your security.

A seamless, simple, modern miracle. It feels like magic.

But as any good magician knows, the true wonder isn't the illusion itself: the woman sawed in half, the card pulled from thin air. The true wonder is the intricate, hidden machinery that makes the illusion possible. The trapdoors, the mirrors, the misdirection, and the years of practice operating flawlessly behind a velvet curtain.

That single click on your bank's URL is the same. The simplicity is the illusion. What happens in the few hundred milliseconds between your click and the rendered page is one of the most complex and fascinating ballets in the modern world. Your simple request embarks on an epic, invisible journey.

## What Happens "Behind the Curtain"?

This book is your backstage pass. We are going to pull back that velvet curtain and follow your click on its journey, demystifying the machinery that makes the web and its security work.

We will watch as your browser, the **client**, consults the world's distributed address book the Domain Name System (DNS) to turn a human-readable name into a machine-readable IP address. We will see it knock on a server's door and perform a secret, encrypted handshake (TLS) to create a secure tunnel, safe from prying eyes. This is the moment the `http://` becomes `https://`, the moment a simple pipe becomes a fortified passage.

We will journey with the request as it travels through **Content Delivery Networks (CDNs)**, digital shock absorbers that protect the server from tidal waves of traffic and speed up your experience. We will see how the server, a fortress in a data center, answers the request: how it verifies *who you are* (Authentication) without ever forgetting you between clicks (Sessions & Cookies), and then decides *what you're allowed to do* (Authorization).

Most importantly, we will uncover the hidden battles fought at every single step. We will meet the attackers the scripts, the bots, the human con artists who probe for weaknesses. We will see how a simple input box can be turned into a peephole into the database (SQL Injection), and how a seemingly harmless link can make your browser betray you (Cross-Site Scripting). And we will learn how the **defenders** the protocols, the code, the architects constantly adapt to protect the integrity of this digital ecosystem.

## Who This Book Is For

This book is for the curious. It is for anyone who has ever wondered, "How does this *actually* work?" and more importantly, "How is this *secure*?"

- **For the Developer** who can build a web application but wants to deeply understand the underlying protocols and security principles that make it robust.
- **For the Aspiring Security Professional** seeking a holistic foundation in web security, from networking to cryptography to human psychology.
- **For the Tech-Savvy Product Manager, Designer, or Founder** who wants to have more informed, critical conversations about security, privacy, and architecture with their engineering teams.
- **For the Power User** who is tired of the fear, uncertainty, and doubt surrounding online security and wants to replace anxiety with knowledge.

No prior expertise in security is required. We will build the concepts from the ground up, using analogies and clear explanations. A general familiarity with how to use the web is all you need to begin this journey.

## A Note on the Mindset: Thinking Like a Defender (and an Attacker)

Throughout this book, we will adopt a dual mindset. To build strong defenses, you must first understand the offense. We will, at times, "put on a black hat" to see how an attacker might exploit a tiny crack in the foundation. We will think about how to trick a database, hijack a session, or deceive a user.

We do this not to encourage malice, but to foster wisdom and resilience. This "security mindset" is not about paranoia; it is about prudent engineering. It is about thinking critically about how things can fail, and building them to be resilient from the very start.

Security is not a product you can buy; it is a process. It is a never-ending journey of learning, adapting, and vigilantly guarding the intricate machinery behind the illusion. It is a shared responsibility between the builders of the web and its citizens.

You are about to become a more knowledgeable member of that society. Let's begin