

VINNY TROIA

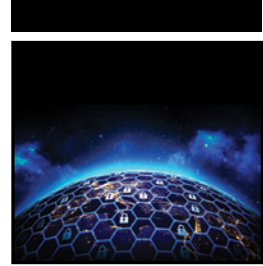
HUNTING CYBER CRIMINALS

A Hacker's Guide to
Online Intelligence Gathering
Tools and Techniques



WILEY

Hunting Cyber Criminals



Hunting Cyber Criminals

A Hacker's Guide to
Online Intelligence Gathering
Tools and Techniques

Vinny Troia, PhD

WILEY

Copyright © 2020 by John Wiley & Sons, Inc., Indianapolis, Indiana
Published simultaneously in Canada

ISBN: 978-1-119-54092-2

ISBN: 978-1-119-54089-2 (ebk)

ISBN: 978-1-119-54099-1 (ebk)

Manufactured in the United States of America

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2019940773

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

To my beautiful daughter, Aria, and my incredible wife, Jess. I never realized what a joy it would be to become a father, and I am thankful every day that you have both given me the most amazing gift of my life.



About the Author

Vinny Troia, PhD, CEH, CHFI, currently serves as head of Night Lion Security, a St. Louis–based cybersecurity consulting firm dedicated to providing top-tier ethical hacking and risk management services.

Troia has been recognized as a thought leader in cybersecurity and has become a go-to media expert for security-related discussions about major corporate data breaches, cyber law and legislation, airline and automobile hacking, and cyber-related scandals.

His experience in IT security stems from a lifetime of coding, complex problem solving, and self-taught computer skills. Troia now travels the globe speaking at conferences and security-related events and spends most of his free time hunting for data breaches and infiltrating private criminal circles on the darkweb.

With each new breach, valuable clues are left behind as to the evolution of an attacker’s methods. During his speeches, Troia uses that information to teach and inform others on ways to increase their defenses and put necessary response strategies in place for when incidents do occur.

Prior to starting Night Lion Security, Troia spent nearly a decade working on security- and risk-related projects for the U.S. Department of Defense.

Troia holds a PhD from Capella University and is a Certified Ethical Hacker and Certified Hacking Forensic Investigator.

For more information, including samples of Troia’s talks, please visit www.vinnytroia.com.

You can also connect with Vinny on LinkedIn at <https://linkedin.com/in/vinnytroia> or via Twitter at <http://www.twitter.com/vinnytroia>.



About the Technical Editor

Rhia Dancel conducts information security assessments throughout the United States, focusing on OSINT and risk-based management platforms with key engagements within the DoD and private sector space.

Rhia's technical and analytical background originated from a chemistry degree applied within the pharmaceutical industry for over 15 years. Rhia now supports organizations in their effort to implement security controls and achieve information security objectives across multiple security programs. Rhia also continues to provide technical input on risk- and security-based projects.



Acknowledgments

I would like to acknowledge and graciously thank the following people:

My Wife, for putting up with my countless sleepless nights and non-stop obsessing while I worked to crack this puzzle.

Bev Robb, without you, I don't think I would have been able to solve the mystery of TDO. Sometimes the most random connections and pieces of information can lead to the most significant discoveries, and that is exactly what happened. Thank you so much for putting up with my millions of questions and late-night text messages. I am eternally grateful to you and hope I can one day repay the favor.

Christopher Meunier, for never letting go of that easily identifiable chip on your shoulder that relentlessly muttered statements like this, giving me all the motivation I needed to keep pressing on:

*whitepacket@xmpp.is: I'm sorry man but you sound like you're either LE or a f***ing retard, probably the latter.*

Dennis Karvouniaris, Thanks for all the info and help you gave me along the way. I'm sorry things had to work out this way. I always enjoy our chats and hope that by the time you read this you will have taken my advice.

Chris "The Human Hacker" Hadnagy, for believing in me enough to connect me with the fine folks at Wiley, ultimately landing me this book deal.

Alex Heid and Jesse Burke, for all the back and forth and continued help pulling some of these pieces together.

And to all of this book's guest experts, I can't thank you enough for volunteering your time to contribute your stories and opinions for this book. I will be giving you all proper credits in the first chapter, but I had to give you all an extra shout-out here as well.



Contents at a Glance

Prologue		xxv
Chapter 1	Getting Started	1
Chapter 2	Investigations and Threat Actors	19
Part I	Network Exploration	43
Chapter 3	Manual Network Exploration	45
Chapter 4	Looking for Network Activity (Advanced NMAP Techniques)	67
Chapter 5	Automated Tools for Network Discovery	83
Part II	Web Exploration	119
Chapter 6	Website Information Gathering	121
Chapter 7	Directory Hunting	143
Chapter 8	Search Engine Dorks	159
Chapter 9	WHOIS	175
Chapter 10	Certificate Transparency and Internet Archives	201
Chapter 11	Iris by DomainTools	221
Part III	Digging for Gold	243
Chapter 12	Document Metadata	245
Chapter 13	Interesting Places to Look	267
Chapter 14	Publicly Accessible Data Storage	293

Part IV	People Hunting	323
Chapter 15	Researching People, Images, and Locations	325
Chapter 16	Searching Social Media	349
Chapter 17	Profile Tracking and Password Reset Clues	377
Chapter 18	Passwords, Dumps, and Data Viper	407
Chapter 19	Interacting with Threat Actors	433
Chapter 20	Cutting through the Disinformation of a 10-Million-Dollar Hack	453
	Epilogue	483
	Index	487



Contents

Prologue	xxv
Chapter 1 Getting Started	1
Why This Book Is Different	2
What You Will and Won't Find in This Book	2
Getting to Know Your Fellow Experts	3
A Note on Cryptocurrencies	4
What You Need to Know	4
Paid Tools and Historical Data	5
What about Maltego?	5
Prerequisites	5
Know How to Use and Configure Linux	5
Get Your API Keys in Order	6
Important Resources	6
OSINT Framework	6
OSINT.link	6
IntelTechniques	7
Termbin	8
Hunchly	9
Wordlists and Generators	9
SecLists	9
Cewl	10
Crunch	10
Proxies	10
Storm Proxies (Auto-Rotating)	10
Cryptocurrencies 101	11
How Do Cryptocurrencies Work?	12
Blockchain Explorers	13

	Following the Money	15
	Identifying Exchanges and Traders	17
	Summary	18
Chapter 2	Investigations and Threat Actors	19
	The Path of an Investigator	19
	Go Big or Go Home	20
	The Breach That Never Happened	21
	What Would You Do?	22
	Moral Gray Areas	24
	Different Investigative Paths	25
	Investigating Cyber Criminals	26
	The Beginning of the Hunt (for TDO)	27
	The Dark Overlord	27
	List of Victims	28
	A Brief Overview	29
	Communication Style	30
	Group Structure and Members	30
	Cyper	31
	Arnie	32
	Cr00k (Ping)	35
	NSA (Peace of Mind)	36
	The Dark Overlord	38
	Summary	41
Part I	Network Exploration	43
Chapter 3	Manual Network Exploration	45
	Chapter Targets: Pepsi.com and Cyper.org	46
	Asset Discovery	46
	ARIN Search	47
	Search Engine Dorks	48
	DNSDumpster	49
	Hacker Target	52
	Shodan	53
	Censys (Subdomain Finder)	56
	Censys Subdomain Finder	56
	Fierce	57
	Sublist3r	58
	Enumall	59
	Results	60
	Phishing Domains and Typosquatting	61
	Summary	64
Chapter 4	Looking for Network Activity (Advanced NMAP Techniques)	67
	Getting Started	67
	Preparing a List of Active Hosts	68
	Full Port Scans Using Different Scan Types	68
	TCP Window Scan	70
	Working against Firewalls and IDS	70

Using Reason Response	71
Identifying Live Servers	71
Firewall Evasion	73
Distributed Scanning with Proxies and TOR	73
Fragmented Packets/MTU	74
Service Detection Trick	74
Low and Slow	76
Bad Checksums, Decoy, and Random Data	76
Firewalking	79
Comparing Results	79
Styling NMAP Reports	81
Summary	82
Chapter 5 Automated Tools for Network Discovery	83
SpiderFoot	84
SpiderFoot HX (Premium)	91
Intrigue.io	95
Entities Tab	96
Analyzing uberpeople.net	99
Analyzing the Results	104
Exporting Your Results	105
Recon-NG	107
Searching for Modules	111
Using Modules	111
Looking for Ports with Shodan	115
Summary	116
Part II Web Exploration	119
Chapter 6 Website Information Gathering	121
BuiltWith	121
Finding Common Sites Using Google Analytics Tracker	123
IP History and Related Sites	124
Webapp Information Gatherer (WIG)	124
CMSMap	129
Running a Single Site Scan	130
Scanning Multiple Sites in Batch Mode	130
Detecting Vulnerabilities	131
WPScan	132
Dealing with WAFs/WordPress Not Detected	136
Summary	141
Chapter 7 Directory Hunting	143
Dirhunt	143
Wfuzz	146
Photon	149
Crawling a Website	151
Intrigue.io	152
Summary	157

Chapter 8	Search Engine Dorks	159
	Essential Search Dorks	160
	The Minus Sign	160
	Using Quotes	160
	The site: Operator	161
	The intitle: Operator	161
	The allintitle: Operator	162
	The filetype: Operator	162
	The inurl: Operator	163
	The cache: Operator	165
	The allinurl: Operator	165
	The filename: Operator	165
	The intext: Operator	165
	The Power of the Dork	166
	Don't Forget about Bing and Yahoo!	169
	Automated Dorking Tools	169
	Inurlbr	169
	Using Inurlbr	171
	Summary	173
Chapter 9	WHOIS	175
	WHOIS	175
	Uses for WHOIS Data	176
	Historical WHOIS	177
	Searching for Similar Domains	177
	Namedroppers.com	177
	Searching for Multiple Keywords	179
	Advanced Searches	181
	Looking for Threat Actors	182
	Whoisology	183
	Advanced Domain Searching	187
	Worth the Money? Absolutely	188
	DomainTools	188
	Domain Search	188
	Bulk WHOIS	189
	Reverse IP Lookup	189
	WHOIS Records on Steroids	190
	WHOIS History	192
	The Power of Screenshots	193
	Digging into WHOIS History	193
	Looking for Changes in Ownership	194
	Reverse WHOIS	196
	Cross-Checking <i>All</i> Information	197
	Summary	199
Chapter 10	Certificate Transparency and Internet Archives	201
	Certificate Transparency	201
	What Does Any of This Have to Do with Digital Investigations?	202
	Scouting with CTFR	202

	Crt.sh	204
	CT in Action: Side-stepping Cloudflare	204
	Testing More Targets	208
	CloudFlair (Script) and Censys	209
	How Does It Work?	210
	Wayback Machine and Search Engine Archives	211
	Search Engine Caches	212
	CachedView.com	214
	Wayback Machine Scraper	214
	Enum Wayback	215
	Scraping Wayback with Photon	216
	Archive.org Site Search URLs	217
	Wayback Site Digest: A List of Every Site URL Cached by Wayback	219
	Summary	220
Chapter 11	Iris by DomainTools	221
	The Basics of Iris	221
	Guided Pivots	223
	Configuring Your Settings	223
	Historical Search Setting	224
	Pivootttt!!!	225
	Pivoting on SSL Certificate Hashes	227
	Keeping Notes	228
	WHOIS History	230
	Screenshot History	232
	Hosting History	232
	Bringing It All Together	234
	A Major Find	240
	Summary	241
Part III	Digging for Gold	243
Chapter 12	Document Metadata	245
	Exiftool	246
	Metagoofil	248
	Recon-NG Metadata Modules	250
	Metacrawler	250
	Interesting_Files Module	252
	Pushpin Geolocation Modules	254
	Intrigue.io	257
	FOCA	261
	Starting a Project	262
	Extracting Metadata	263
	Summary	266
Chapter 13	Interesting Places to Look	267
	TheHarvester	268
	Running a Scan	269
	Paste Sites	273

	Psbdmp.ws	273
	Forums	274
	Investigating Forum History (and TDO)	275
	Following Breadcrumbs	276
	Tracing Cyper's Identity	278
	Code Repositories	280
	SearchCode.com	281
	Searching for Code	282
	False Negatives	283
	Gitrob	284
	Git Commit Logs	287
	Wiki Sites	288
	Wikipedia	289
	Summary	292
Chapter 14	Publicly Accessible Data Storage	293
	The Exactis Leak and Shodan	294
	Data Attribution	295
	Shodan's Command-Line Options	296
	Querying Historical Data	296
	CloudStorageFinder	298
	Amazon S3	299
	Digital Ocean Spaces	300
	NoSQL Databases	301
	MongoDB	302
	Robot 3T	302
	Mongo Command-Line Tools	305
	Elasticsearch	308
	Querying Elasticsearch	308
	Dumping Elasticsearch Data	311
	NoScrape	311
	MongoDB	313
	Elasticsearch	314
	Scan	314
	Search	315
	Dump	317
	MatchDump	317
	Cassandra	318
	Amazon S3	320
	Using Your Own S3 Credentials	320
	Summary	321
Part IV	People Hunting	323
Chapter 15	Researching People, Images, and Locations	325
	PIPL	326
	Searching for People	327
	Public Records and Background Checks	330

Ancestry.com	331
Threat Actors Have Dads, Too	332
Criminal Record Searches	332
Image Searching	333
Google Images	334
Searching for Gold	335
Following the Trail	335
TinEye	336
EagleEye	340
Searching for Images	340
Cree.py and Geolocation	343
Getting Started	343
IP Address Tracking	346
Summary	347
Chapter 16 Searching Social Media	349
OSINT.rest	350
Another Test Subject	355
Twitter	357
SocialLinks: For Maltego Users	358
Skiptracer	361
Running a Search	361
Searching for an Email Address	361
Searching for a Phone Number	364
Searching Usernames	366
One More Username Search	368
Userrecon	370
Reddit Investigator	372
A Critical “Peace” of the TDO Investigation	374
Summary	375
Chapter 17 Profile Tracking and Password Reset Clues	377
Where to Start (with TDO)?	377
Building a Profile Matrix	378
Starting a Search with Forums	379
Ban Lists	381
Social Engineering	381
SE’ing Threat Actors: The “Argon” Story	383
Everyone Gets SE’d—a Lesson Learned	387
The End of TDO and the KickAss Forum	388
Using Password Reset Clues	390
Starting Your Verification Sheet	391
Gmail	391
Facebook	393
PayPal	394
Twitter	397
Microsoft	399

Instagram	400
Using jQuery Website Responses	400
ICQ	403
Summary	405
Chapter 18 Passwords, Dumps, and Data Viper	407
Using Passwords	408
Completing F3ttywap’s Profile Matrix	409
An Important Wrong Turn	412
Acquiring Your Data	413
Data Quality and Collections 1–5	413
Always Manually Verify the Data	415
Where to Find Quality Data	420
Data Viper	420
Forums: The Missing Link	421
Identifying the Real “Cr00k”	422
Tracking Cr00k’s Forum Movements	423
Timeline Analysis	423
The Eureka Moment	427
Vanity over OPSEC, Every Time	429
Why This Connection Is Significant	429
Starting Small: Data Viper 1.0	430
Summary	431
Chapter 19 Interacting with Threat Actors	433
Drawing Them Out of the Shadows	433
Who Is WhitePacket?	434
The Bev Robb Connection	435
Stradinatras	436
Obfuscation and TDO	437
Who Is Bill?	439
So Who Exactly Is Bill?	440
YoungBugsThug	440
How Did I Know It Was Chris?	441
A Connection to Mirai Botnet?	442
Why Was This Discovery So Earth-Shattering?	444
Question Everything!	445
Establishing a Flow of Information	446
Leveraging Hacker Drama	447
Was Any of That Real?	448
Looking for Other Clues	449
Bringing It Back to TDO	450
Resolving One Final Question	451
Withdrawing Bitcoin	451
Summary	452

Chapter 20	Cutting through the Disinformation of a 10-Million-Dollar Hack	453
	GnosticPlayers	454
	Sites Hacked by GnosticPlayers	456
	Gnostic’s Hacking Techniques	457
	GnosticPlayers’ Posts	459
	GnosticPlayers2 Emerges	461
	A Mysterious Third Member	462
	NSFW/Photon	463
	The Gloves Come Off	464
	Making Contact	465
	Gabriel/Bildstein aka Kuroi’sh	465
	Contacting His Friends	467
	Weeding through Disinformation	468
	Verifying with Wayback	468
	Bringing It All Together	469
	Data Viper	469
	Trust but Verify	472
	Domain Tools’ Iris	474
	Verifying with a Second Data Source	475
	The End of the Line	476
	What Really Happened?	476
	Outofreach	476
	Kuroi’sh Magically Appears	477
	What I Learned from Watching Lost	477
	Who Hacked GateHub?	478
	Unraveling the Lie	479
	Was Gabriel Involved? My Theory	479
	Gabriel is Nclay: An Alternate Theory	479
	All roads lead back to NSFW	480
	Summary	481
	Epilogue	483
	Index	487



Prologue

One of the more recent investigations I worked on involved the hack of a multi-billion dollar organization. Their stolen data was posted for sale in private circles, and upon finding this out, I immediately contacted the organization. The organization had many questions, and given my prior investigative work, I was able to reach out to the threat actor on their behalf and obtain information on how the breach occurred.

The following text is a portion of the writeup provided by NSFW, a threat actor we will be covering in much greater detail throughout this book, where he describes, in detail, how he was able to hack this organization's network. The process he used was sophisticated, and by no means a run-of-the-mill drive-by hack.

This was very well planned and executed.

All identifying information has been changed.

HACK WRITEUP: NSFW

Firstly I realised that GitHub is adding new device verification within the week, therefore I tried to identify as many developers as possible and sign into their GitHub account to access organisation private repo's.

I then identified software developers working for Company using LinkedIn. Partially doxing each one to obtain Gmail accounts, I found Bob.

Performing database lookups in hope for password reuse (or rules to be applied to their previous password) in order to login with valid credentials.

The way I got into the GitHub was due to Bob, who reused the password "BobsTiger66" (Which GitHub had told was insecure with a red banner, yet he chose to ignore it), and was reused on multiple private databases and one public database (ArmorGames).

Once logged in I had to act quick to avoid GitHub's new ML algorithm to lock accounts out of using new IPs, so I immediately used ssh-keygen to add a new public SSH key to the user profile, I had realised you had added Okta SSO preventing the clone of private repos, in order to bypass this I looked at potential integrations.

CircleCI is a popular CI/CD tool which is inherently linked to organisations via either SSH key linkage or PAT's, therefore I realised the build processes could be exploited in order to obtain private repos, however this was not needed. You guys had added a weird implementation of Okta STS with AWS, producing time-limited tokens, I realised these were spawned everytime a new build process was triggered, therefore I accessed Circle debug mode and managed to extract these time limited tokens, and used them to download your internal datalakes.

Unfortunately these tokens were not given any further privileges, therefore you got lucky or else I would have gained access to RDS via CLI and cloned a snapshot.

When I read this, I was immediately impressed by the level of effort he put into the hack. And despite the outcome, the client was, too.

In the end, this breach had a happy ending, because I was able to provide useful intel to the customer that allowed them to identify how the breach happened, and to also put in proper safeguards to ensure that this did not happen again.

That's ultimately the point, right?

Not to provide customers with a useless writeup of generic TTPs (tactics, techniques, and procedures) regarding assumed threat actors—which is what so many threat intelligence companies do—but to actually provide useful context for how a threat actor breaches their systems.

So many companies just rely on providing existing reports on threat actor groups and never actually get to the core of how an attack happened. Sometimes it takes actually hunting down the threat actors and speaking to them directly. They are usually pretty open and willing to brag about how they did it, because on some level all hackers want to be famous; and as we will see in future chapters, *vanity always trumps OPSEC* (operational security).

In this particular case, I was already speaking to NSFW about several other hacks he is associated with, so it was no issue to ask how he was able to pull this off.

And if you are paying close attention, you will have noticed several misspellings and important "tells" associated with his writeup. Common misspellings or even regional differences in spelling (e.g., organisation vs. organization) can be very important investigative clues that we will discuss in future chapters.

But before we dive into all that, I feel it is important to shed some light on who I am, so you can get to know me a little better, understand what makes me tick, and maybe get accustomed to some of the dry humor and sarcasm that you will find sprinkled throughout this book.

My Story

When I started writing this book, I asked myself a simple question: Am I qualified to write this book? To this day, my answer is still “probably not.” I don’t believe one person can know everything there is to know about a topic, which is why you will find tips and stories from other industry experts throughout this book.

I admire and respect each of the people that I have asked to contribute to this book. I know their work firsthand, which is why I feel they each bring their own unique perspective that complements and reinforces the topics I will be putting forward.

But before we get to that, here is some insight into who I am and what makes me tick.

History

I was about 10 years old when my dad brought home an IBM PS/2. I had no idea what it was or what it could do, but I was mesmerized. This was before the Windows 3.1 days. I remember turning it on and staring at a DOS prompt and just hacking my way through it. The whole thing was like a giant puzzle, which is probably why it sucked me in.

I am a huge puzzle junkie. The more complex, the better. One of my strengths (and also admittedly a weakness) is that I can be relentless when I am trying to find a solution to a complex problem. Some have referred to this behavior as “obsessive.” I get it, and I acknowledge the behavior.

There are nights where I am still cranking away at 4 a.m. because I just can’t stop. It’s part of who I am, and it is a big part of why I feel that I am very good at what I do—whether that be trying to hack into a system or assembling the story behind a criminal investigation.

Roots and Raves

In case you are wondering, I started out my career as a web developer writing HTML and JavaScript in the late ‘90s. I grew up in New Jersey and was always into electronic music. Naturally, I was also entranced with the rave culture. Nightclubs like Limelight and Tunnel were the big thing, and I wanted to be a part of it.

Unfortunately these clubs had a 21+ age requirement, which was a problem because I was 16. So I taught myself HTML and offered to build a free website for one of the club’s resident DJs. From then on, I could just walk in with him because I was his “web guy.” Problem solved.

Penetration testing is not much different, which is why I have been doing it (in one form or another) all my life. It's all a matter of understanding what the rules are, then figuring out a way to circumvent them.

I have always been good at finding ways to get around the rules, which I think is a trait shared by most penetration testers.

Don't get me wrong, rules are important. Some people like living their lives in a well-defined sandbox, while others enjoy the challenge of trying to find ways to break out of it. I am the latter.

Developing a Business Model (with Lasers!!)

One evening circa 2011, I was browsing the Internet the same way most people do: with Burp suite active and running passive recon on all sites that I visited.

I was telling my wife about an awesome site that sells high-powered lasers in different colors, hoping she would let me buy one. That was a hard no, but much to my surprise, Burp suite found a passive SQL injection vulnerability in the site.

I had to check it out, and before I knew it, I was able to see the site's user accounts with hashed passwords. Logging in to the site with one of the admin accounts meant having to crack the admin's password hash, which wasn't difficult using any number of online hash crackers given that the password was some variation of Admin123.

I logged in to the site and voilà! I had full access to everything. System records, user accounts, order information, and all.

NOTE Yes, I now realize this action was not exactly "legal," but don't judge. We all have to start somewhere. Plus, this story has a happy ending.

It was that exact moment that I felt the entrepreneurial spark. What if I could take this information and give it to the site's owners so they could fix the injection bug, preventing others from accessing the site in the same way? Surely they would repay this random act of kindness with some of their badass high-power lasers?

I am now the proud owner of a 2,000mW blue laser, and a 1,000mW green laser! Nice, right? The lasers actually burn stuff. They are pretty bad-ass.

More importantly, the site closed the SQL injection vulnerability, and I had a model for a business to provide services that could actually help people.

In the process, I also learned an extremely valuable lesson: If you hack into a website first, *then* try to offer the solution to the customer and ask for a "tip" in the form of a product from their website, it could be interpreted as extortion.

Oops. That clearly wasn't my intent, which I think came off in my email with the CEO, but looking back, I am sure I could have been in some trouble. So while this particular exercise worked out well for everyone, I clearly had to do some work in refining the business model.