Open in app ↗

Sign up

Sign In

Published in The Gray Area

GZ

Graham Zemel Follow

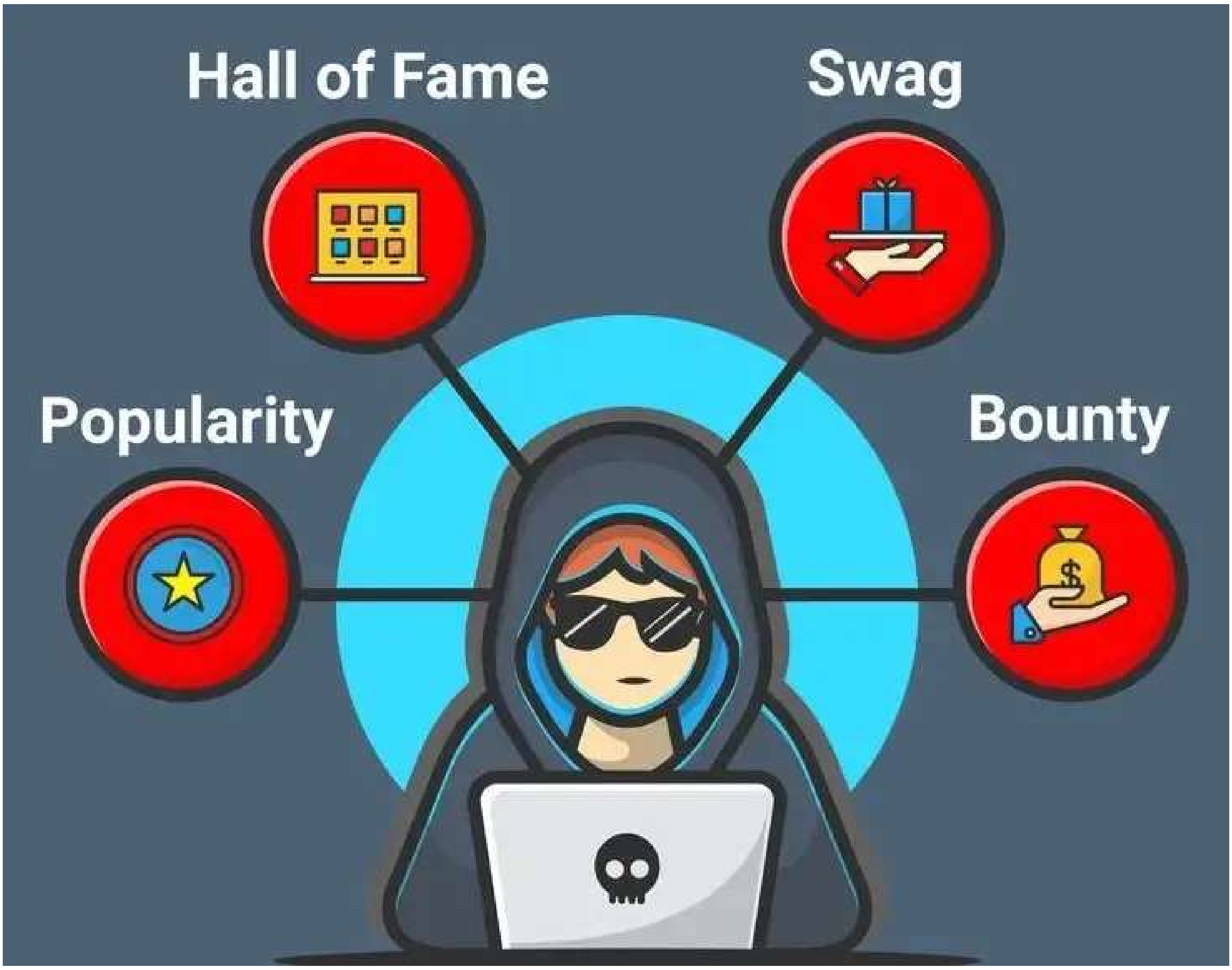
Dec 1 · 7 min read · ✦ · ▶ Listen

Save

The Ultimate List of Bug Hunting Resources for Beginners

TL;DR- If you're new to cybersecurity, you'll absolutely want to take a look at one of the highest earning activities for white-hat hackers — Bug Bounties.

143



Introduction

In this post, I'll be reviewing the absolute basics of bug hunting, and a ton of great tools and resources. We'll take a look at **what bug bounties are**, **basic tech skills**, and **how to become a skilled pen-tester**.

If you're into programming, you can even **develop your own bug hunting toolkit**! Stick around and I'll showcase my personal scripts that I've used for numerous bounties.

> *Note: This post does contain affiliate links for some of the resources, which don't add any extra cost to your purchase, but helps me out through a small portion of the proceeds.*

What is bug hunting?

More and more organizations and companies are starting to create programs that allow vulnerabilities to be reported ***legally***, and with **monetary** rewards. While you could utilize vulnerabilities you've found to expose user data on the dark web (like a **black-hat hacker**), there's also a great ***legal*** option.

These programs enable developers to identify and fix bugs before the general public is aware of them, preventing widespread abuse. A large number of organizations, including **Facebook, Google, Twitter, Microsoft, Uber, Github,** and many others have implemented these sorts of programs.

Lockdown Mode

Lockdown Mode is an extreme, optional protection that should only be used if you believe you may be personally targeted by a highly sophisticated cyberattack. Most people are never targeted by attacks of this nature.

Apple taunting hackers with a $2m bounty for hacking their new feature, Lockdown Mode

Companies like **Yahoo** and **Uber** frequently pay out ***$50K+ bounties,*** with some of the highest payouts coming from Google and Apple at ***$170K*** and ***over $2m*** respectively.

Even companies outside of the technology industry, including government branches such as the **US Department of Defense**, have started to use bug bounty programs hosted on **HackerOne**.

Remember…

1- You'll have plenty of help from others, but you'll need to put in a lot of work to see significant results.

2- You will **not** become a world famous bug hunter overnight.

3- Bug bounties are **very competitive**. You'll want to **start small**, not even worrying about the money aspect until you get good enough to move to websites with small bug-hunting programs. Here are a few tips —

The Best Vulnerability Disclosure Programs (Less Competitive Bounties)

TL;DR- There's a ton of programs for bug bounties and vulnerability disclosure, but they're usually filled with…

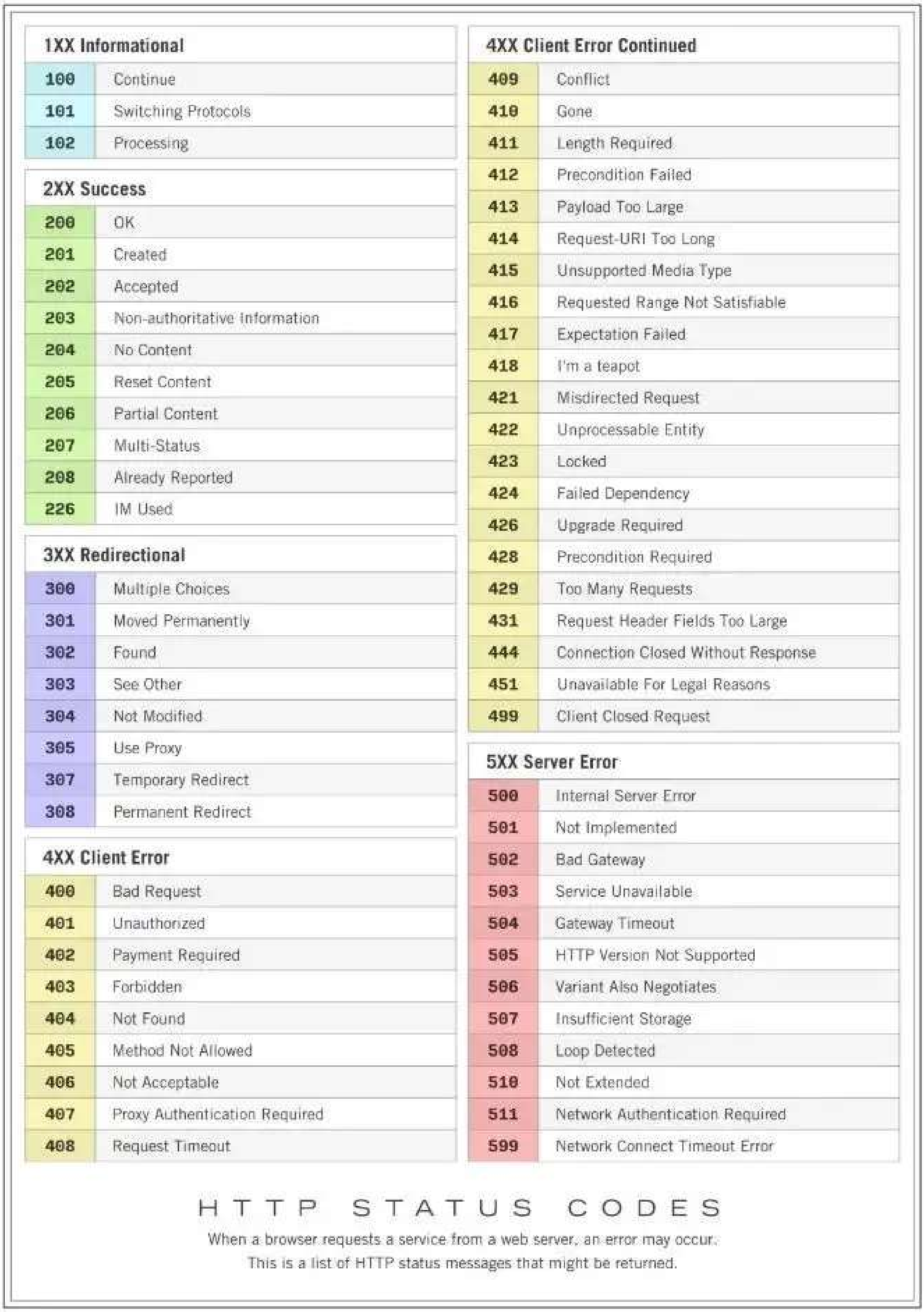
blog.grahamzemel.com

Basic tech & terminology:

You need to have a **basic** understanding of how the internet works. You can reach out to find help on **social media** and certain **forums**, but there's a ton of trial and error in bug hunting. Here are a few important topics —

HTTP/HTTPS

HTTP is a method of communication, which stands for **HyperText Transfer Protocol**. It was created to allow web browsers and web servers to communicate with each other. I'd **highly** recommend you read the following resources to get a basic understanding of **HTTP protocols**, **HTTP requests**, **responses**, **status codes**, **encoding/decoding**, and more.



1XX Informational	
100	Continue
101	Switching Protocols
102	Processing

2XX Success	
200	OK
201	Created
202	Accepted
203	Non-authoritative Information
204	No Content
205	Reset Content
206	Partial Content
207	Multi-Status
208	Already Reported
226	IM Used

3XX Redirectional	
300	Multiple Choices
301	Moved Permanently
302	Found
303	See Other
304	Not Modified
305	Use Proxy
307	Temporary Redirect
308	Permanent Redirect

4XX Client Error	
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required
408	Request Timeout

4XX Client Error Continued	
409	Conflict
410	Gone
411	Length Required
412	Precondition Failed
413	Payload Too Large
414	Request-URI Too Long
415	Unsupported Media Type
416	Requested Range Not Satisfiable
417	Expectation Failed
418	I'm a teapot
421	Misdirected Request
422	Unprocessable Entity
423	Locked
424	Failed Dependency
426	Upgrade Required
428	Precondition Required
429	Too Many Requests
431	Request Header Fields Too Large
444	Connection Closed Without Response
451	Unavailable For Legal Reasons
499	Client Closed Request

5XX Server Error	
500	Internal Server Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Timeout
505	HTTP Version Not Supported
506	Variant Also Negotiates
507	Insufficient Storage
508	Loop Detected
510	Not Extended
511	Network Authentication Required
599	Network Connect Timeout Error

HTTP STATUS CODES

When a browser requests a service from a web server, an error may occur.
This is a list of HTTP status messages that might be returned.

You can more or less break these status codes down into 200's succeeding and anything in the 400+ range failing (for various reasons). You'll want to learn a bunch more than that though if you're looking to **find good bugs.**

You'll absolutely want to familiarize yourself with HTTP requests, responses, and everything in between for bug hunting →

HTTP: The Protocol Every Web Developer Must Know-Part 1

Learning the fundamentals of the World Wide Web is crucial, especially if you are planning to build web apps. And HTTP...

code.tutsplus.com

Links from TutorialsPoint on HTTP →

- https://www.tutorialspoint.com/http/http_status_codes.htm
- https://www.tutorialspoint.com/http/http_url_encoding.htm
- https://www.tutorialspoint.com/http/http_requests.htm
- https://www.tutorialspoint.com/http/http_responses.htm

Basic Networking:

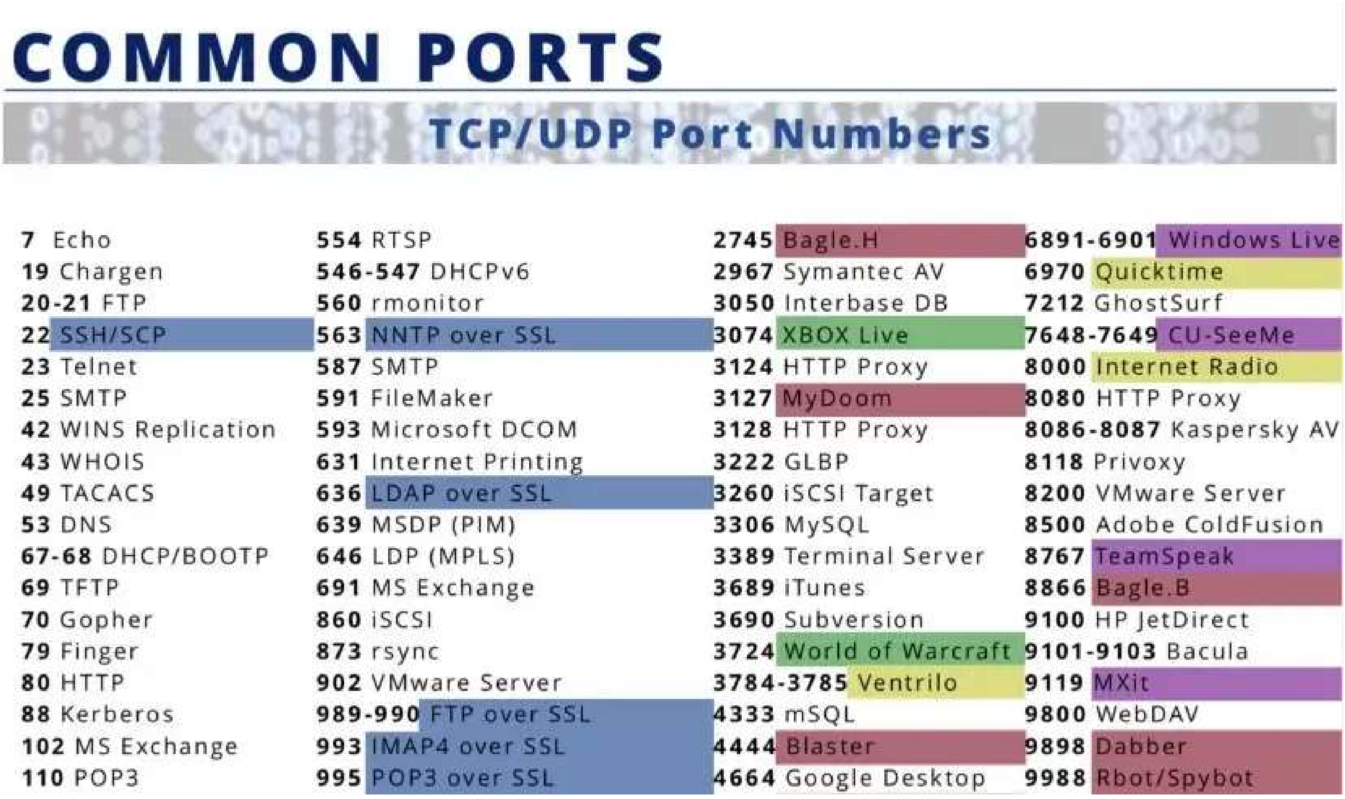
This is a helpful skill if you're getting into cybersecurity, and knowing the absolute basics about things like IP addresses and networking packets can be helpful when exploiting websites. Here are some great, fundamental resources that I've used myself →

TCP/IP Model - GeeksforGeeks

Prerequisite - Layers of OSI Model The OSI Model we just looked at is just a reference/logical model. It was designed...

www.geeksforgeeks.org

Common ports for machines (web servers, computers, gaming consoles, the whole lot) →



COMMON PORTS

TCP/UDP Port Numbers

7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Server
53	DNS	639	MSDP (PIM)	3306	MySQL	8500	Adobe ColdFusion
67-68	DHCP/BOOTP	646	LDP (MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula
80	HTTP	902	VMware Server	3784-3785	Ventrilo	9119	MXit
88	Kerberos	989-990	FTP over SSL	4333	mSQL	9800	WebDAV
102	MS Exchange	993	IMAP4 over SSL	4444	Blaster	9898	Dabber
110	POP3	995	POP3 over SSL	4664	Google Desktop	9988	Rbot/Spybot

More links and information on DNS (Domain Name Servers) and network security →

- https://www.wpbeginner.com/glossary/dns/
- https://www.cloudflare.com/learning/dns/what-is-dns/

- https://www.slideshare.net/variwalia/basic-to-advanced-networking-tutorials
- https://www.digitalocean.com/community/tutorials/an-introduction-to-networking-terminology-interfaces-and-protocols

Linux Commands →

It’s a great idea to start with a knowledge of different Linux operating systems, and be able to use the **command line** (preferably on a variety of platforms).

If you’re not familiar with Linux, I suggest purchasing one of the **popular books below** or reading **online articles** to learn more.

LinuxCommand.org: Learning the shell.

Why do you need to learn the command line anyway? Well, let me tell you a story. Many years ago we had a problem where…

linuxcommand.org

LinuxCommand.org: Writing shell scripts.

Bash shell scripting tutorial: Introduction

linuxcommand.org

A Deep Dive Into the Foundation Of Linux

TL;DR- An in-depth article exploring Linux. We’ll be looking at core concepts and functionalities, it’s origin, and…

thegrayarea.tech

Three great books I’ve read on Linux:

The Ultimate Kali Linux Book

The Linux Command Line, 2nd Edition

Linux for Beginners: A Practical and Comprehensive Guide to Learn Linux

Programming/Coding:

You don’t *need* to know how to program in order to be a successful bug bounty hunter, but it does help with **troubleshooting** and allows access to **more potential bounties.**

If you understand the code, you can increase your chances of successfully identifying and exploiting vulnerabilities.

You might also need to understand the syntax of a target website’s code to escalate a bug to a much **higher severity**, landing **3 or 4 times the original bounty.**

Here are some resources on each programming language prominent in bug hunting →

HTML

Learn HTML | Codecademy

Checker Dense Start at the beginning by learning HTML basics - an important foundation for building and editing web...

www.codecademy.com

HTML Tutorial

With our "Try it Yourself" editor, you can edit the HTML code and view the result: Click on the "Try it Yourself"...

www.w3schools.com

HTML Advanced Tutorial

Exploring the depths of HTML5, some advanced, rather specific applications of the markup language for ultimate...

htmldog.com

PHP

PHP Tutorial

PHP is a server scripting language, and a powerful tool for making dynamic and interactive Web pages. PHP is a...

www.w3schools.com

PHP Tutorial for Beginners: Learn in 7 Days

PHP is the most popular scripting language on the web. Without PHP Facebook, Yahoo, Google wouldn't have exist. The...

www.guru99.com

JavaScript

Learn JavaScript | Codecademy

Checker Dense Learn how to use JavaScript - a powerful and flexible programming language for adding website...

www.codecademy.com

JavaScript Tutorial

JavaScript is the world's most popular programming language. JavaScript is the programming language of the Web...

www.w3schools.com

SQL (Structured Query Language)

SQL Tutorial

SQL is a standard language for storing, manipulating and retrieving data in databases. Our SQL tutorial will teach you...

www.w3schools.com

Learn SQL | Codecademy

Checker Dense Learn to communicate with databases using SQL, the standard data management language. Start 945,000...

www.codecademy.com

Automation in cybersecurity:

Understanding the languages listed below will allow you to **code your own tools, comprehend** many other widely used tools, and **modify** them as you see fit.

I'd *highly* suggest getting a subscription to Amazon's Kindle Unlimited, it's **cheap** and there's a ton of surprisingly **up-to-date resources** for hacking and bug hunting tips.

Personally, I use **Bash** to code scripts for **hacking automation**, here's one of them if you're interested →

GitHub - grahamzemel/WebHeckScanner: A hacking tool for bug bounties. Sharing and modifying is…

Written by Graham Zemel, using Nikto, Nuclei, Sqlmap, Anew, Gau, and more! This is a bash script designed to scan web…

github.com

Bash

Learning The Bash Shell

Shell Scripting Tutorial

A shell script is a computer program designed to be run by the Unix/Linux shell which could be one of the following…

www.tutorialspoint.com

Learn Shell - Free Interactive Shell Tutorial

Welcome to the learnshell.org interactive Shell Programming tutorial. Whether you are an experienced programmer or not…

www.learnshell.org

Ruby

Learn Ruby - Free Interactive Ruby Tutorial

Welcome to the learnrubyonline.org free interactive Ruby tutorial. Whether you are an experienced programmer or not…

www.learnrubyonline.org

Learn Ruby | Codecademy

Checker Dense Learn to program in Ruby, a flexible and beginner-friendly language used to create sites like Codecademy...

www.codecademy.com

Python

Hecker Bot Source Code

This product gives you access to my personal hacking bot coded in python, containing many functions and is constantly updated. Ther...

grahamzemel.gumroad.com

Python Web Penetration Testing Cookbook

Great resource links →

- https://www.nopsec.com/5-python-libraries-every-pentester-should-be-using/
- https://www.tutorialspoint.com/python_penetration_testing/index.htm

Golang

A Tour of Go

Edit description

tour.golang.org

[Mastering Go: Create GoLang Production Applications]

[Go Programming Cookbook: Over 85 Recipies]

GitHub - cristaloleg/go-advice: List of advice and tricks for Go ʕ◔ϖ◔ʔ

(Some of advices are implemented in go-critic) Don't communicate by sharing memory, share memory by communicating…

github.com

Take these tips one step further if you're advanced enough, and check out another post on **becoming a skilled red-team hacker** →

The Road to Professional Red-Team Hacker

TL;DR: All of the physical tools, repositories, websites, and operating systems you could possibly need to become a…

thegrayarea.tech

Hopefully you learned some helpful tips and got a couple of resources that you can use as a starting point. If you enjoyed this post, check out similar articles on **bug bounties** and **computer science** from The Gray Area.

Support my writing and help me create more content by subscribing to a Medium membership with **my referral link**, giving you access to **all of my posts** (*and* everyone else's on Medium)! →

Join Medium with my referral link - Graham Zemel

Read all of Graham Zemel's posts, and any other post from thousands of Medium writers! You'll get full access to every...

blog.grahamzemel.com

Thanks!

Bug Bounty Cybersecurity Hacking Bugs Bug Bounty Tips

Enjoy the read? Reward the writer.Beta

Your tip will go to Graham Zemel through a third-party platform of their choice, letting them know you appreciate their story.

Give a tip