Bug bounty resources & advices

Gökhan Güzelkokar

Follow

Apr 7 · 6 min read

https://blog.gnosis.pm/2020-dex-bug-bounty-210f2b67a764

Hey guys, in this story I'm going to share some resources for every hacker and advices for beginners…

Advices for Beginners

Before starting bug bounty.

1- Learn basics of internet.

2- Learn http very well. (request, response, headers, cookies, http status, body, request types (GET, POST, PUT, DELETE, OPTIONS, HEAD) etc)

3- Learn basics of html, css and javascript.

4- Learn basics of golang, sql, ruby and python. Just install it and print hello world. (for now)

5- Learn basics of networking (DHCP, DNS, routers, server, client, IP, TCP, UPD, SMTP, Ports, Subnetting etc.)

6- Learn how to use google. Learn Google Dorks…

7- Be patient and read a lot. (Blogs, tweets, write-ups etc.)Nobody starts earning thousands of dollars as soon as they start.

8- Use social media to improve yourself. Become an information exploiter. I will share a lot of twitter accounts below.

9- Don't start searching before learning to least 10 tools and learn the basics of all vulnerabilities. (xss, idor, ssrf, rce, crlf, sqli etc.)

10- Understand what is being done on the site where you will search for the vulnerability. Understand business logic.

11- Inputs are our biggest weapon.

12- Examine JS files well for valuable information...

13- Stay safe and healthy…

Tools I use

[tomnomnom/assetfinder](#)

[Find domains and subdomains potentially related to a given domain. If you have Go installed and configured (i.e. with...](#)

[github.com](#)

[tomnomnom/httprobe](#)

[Take a list of domains and probe for working http and https servers. ▶ go get -u github.com/tomnomnom/httprobe httprobe...](#)

[github.com](#)

[tomnomnom/waybackurls](#)

[Accept line-delimited domains on stdin, fetch known URLs from the Wayback Machine for *.domain and output them on...](#)

[github.com](#)

[tomnomnom/meg](#)

[meg is a tool for fetching lots of URLs but still being 'nice' to servers. It can be used to fetch many paths for many...](#)

[github.com](#)

[GerbenJavado/LinkFinder](#)

[A python script that finds endpoints in JavaScript files - GerbenJavado/LinkFinder](#)

[github.com](#)

[s0md3v/Arjun](#)

[HTTP Parameter Discovery Suite Web applications use parameters (or queries) to accept user input, take the following...](#)

[github.com](#)

[maurosoria/dirsearch](#)

[Current Release: v0.3.9 (2019.11.26) dirsearch is a simple command line tool designed to brute force directories and...](#)

[github.com](#)

[sullo/nikto](#)

[Nikto web server scanner. Contribute to sullo/nikto development by creating an account on GitHub.](#)

[github.com](#)

[maaaaz/webscreenshot](#)

[A simple script to screenshot a list of websites, based on the url-to-image PhantomJS script.](#)

[github.com](#)

[FortyNorthSecurity/EyeWitness](#)

[EyeWitness is designed to take screenshots of websites provide some server header info, and identify default...](github.com)

github.com

[OWASP/Amass](github.com)

[The OWASP Amass Project has developed a tool to help information security professionals perform network mapping of...](github.com)

github.com

[smicallef/spiderfoot](github.com)

[SpiderFoot is an open source intelligence (OSINT) automation tool. It integrates with just about every data source...](github.com)

github.com

[sqlmapproject/sqlmap](github.com)

[sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection...](github.com)

github.com

Web tools

http://dns.bufferover.run/dns?q=domain.com

[crt.sh | Certificate Search](crt.sh)

Free CT Log Certificate Search Tool from Sectigo (formerly Comodo CA)

crt.sh

[Visual Site Mapper - Create a visual map of your site](www.visualsitemapper.com)

Visual Site Mapper is a free service that can quickly show an interactive visual map of your site.

www.visualsitemapper.com

[Unicode Converter - Decimal, text, URL, and unicode converter](www.branah.com)

This site uses cookies and other tracking technologies to assist with your ability to provide feedback, analyze your…

www.branah.com

[Crunchbase: Discover innovative companies and the people behind them](www.crunchbase.com)

Crunchbase is the leading destination for company insights from early-stage startups to the Fortune 1000. Get insights…

www.crunchbase.com

[Gain control over your JWTs](www.jsonwebtoken.io)

signupFields.successMessage }} We have generated code samples based on the input above for different languages. Select…

www.jsonwebtoken.io

https://bgp.he.net/

https://spyse.com/

All Resources (medium, twitter, youtube, blogs etc)

[OWASP Top Ten](#)

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad…

owasp.org

[RBleug](#)

Regilero's blog; Mostly tech things about web stuff.

regilero.github.io

[PortSwigger Blog](#)

Articles and product insights from the PortSwigger team. Keep up to date with Burp Suite and the world of web security…

portswigger.net

[Nahamsec](#)

Nahamsec creates educational hacking videos for anyone with an interest in web application hacking with a focus on bug…

www.youtube.com

[jhaddix](#)

Edit description

www.youtube.com

[CVE security vulnerability database. Security vulnerabilities, exploits, references and more](#)

CVSS Score Number Of Vulnerabilities Percentage Total 123454 Weighted Average CVSS Score: 6.6 703 914 4880 4556 27455…

www.cvedetails.com

[InfoSec Write-ups](#)

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub…

medium.com

[tomnomnom - Overview](#)

Dismiss Sign up for your own profile on GitHub, the best place to host code, manage projects, and build software…

github.com

[s0md3v - Overview](#)

Dismiss Sign up for your own profile on GitHub, the best place to host code, manage projects, and build software…

github.com

[danielmiessler - Overview](#)

Dismiss Sign up for your own profile on GitHub, the best place to host code, manage projects, and build software…

github.com

codingo - Overview

Dismiss Sign up for your own profile on GitHub, the best place to host code, manage projects, and build software…

github.com

James Kettle

The latest Tweets from James Kettle (@albinowax). Director of Research at PortSwigger Web Security aka @Burp_Suite…

twitter.com

todayisnew

The latest Tweets from todayisnew (@codecancare). May you be well on your side of the screen. Ontario, Canada

twitter.com

Ron Chan

The latest Tweets from Ron Chan (@ngalongc). Security Engineer at Gitlab. This is a personal stream, opinions expressed…

twitter.com

CVE

The latest Tweets from CVE (@CVEnew). Official account maintained by the CVE Team to notify the community of new CVE…

twitter.com

Exploit Database

The latest Tweets from Exploit Database (@ExploitDB). The Exploit Database - ultimate archive of #Exploits, #Shellcodes…

twitter.com

A hacker's life

The latest Tweets from A hacker's life (@Unknownuser1806). ▄▖▗█▌[Fall in love with hacking]▌▄▖▗. In your r00t

twitter.com

STÖK

The latest Tweets from STÖK (@stokfredrik). Hi.. im that hacker that your friends told you about. I used to travel the…

twitter.com

Random Robbie

The latest Tweets from Random Robbie (@Random_Robbie). #infosec ¯_(ツ)_/¯ - I find your shit that only has an IP and...

twitter.com

debsec

The latest Tweets from debsec (@deb_security). Cobalt Core 🦑 Team Alertot https://t.co/CVcsTscywz...

twitter.com

Brute Logic

The latest Tweets from Brute Logic (@brutelogic). #Hacking Research & Development. Helping people to #XSS stuff. Also...

twitter.com

Kenan

The latest Tweets from Kenan (@kenanistaken). Information Security Enthusiast, Top 40 hacker, Bug bounty hunter...

twitter.com

YourNextBugTip

The latest Tweets from YourNextBugTip (@YourNextBugTip). #bugbounty Everyone is sharing something and I am sharing all...

twitter.com

Emad Shanab

The latest Tweets from Emad Shanab (@Alra3ees). A Lawyer & A noooob. Every Law has its own Bugs. mrweb@protonmail.com...

twitter.com

Cyber Advising

The latest Tweets from Cyber Advising (@cyber_advising). Cyber Security Consulting. Trento, Italy

twitter.com

spaceraccoon 🦝

The latest Tweets from spaceraccoon 🦝 (@spaceraccoonsec). Here to learn! Hackerone: https://t.co/UK9KDsRVlL...

twitter.com

The Cyber Mentor

The latest Tweets from The Cyber Mentor (@thecybermentor). 👨 Husband | 🇺🇸 Vet | Founder @TCMSecurity | 🎥 YouTuber...

twitter.com

dawgyg

The latest Tweets from dawgyg (@thedawgyg). 1 of 8 Millionaire Hackers thanks to @hacker0x01 #h1415 2020 MVH, Bug…

twitter.com

mpgn

The latest Tweets from mpgn (@mpgn_x64). Flibustier du net ⌐╦╦═─=(*•)=─═╦╦¬ . Aix-en-Provence, France

twitter.com

NahamSec

The latest Tweets from NahamSec (@NahamSec). ɪʀ Co-founder @bugbountyforum | Head of Hacker Education @Hacker0x01 |…

twitter.com

HackRead.com

The latest Tweets from HackRead.com (@HackRead). Official Twitter account of HackRead! Bringing the best hacking, cyber…

twitter.com

SecurityTrails

The latest Tweets from SecurityTrails (@securitytrails). We strive to make the biggest treasure-trove of cyber…

twitter.com

GoSecure

The latest Tweets from GoSecure (@GoSecure_Inc). GoSecure leverages its @CounterTack Platform as well as its unique…

twitter.com

List of bug bounty writeups

Home AMA Challenges Cheatsheets Conference notes The 5 Hacking NewsLetter The Bug Hunter Podcast Tips & Tricks…

pentester.land

Offensive Security's Exploit Database Archive

The GHDB is an index of search queries (we call them dorks) used to find publicly available information, intended for…

www.exploit-db.com

Jonathan Bouman - Medium

Read writing from Jonathan Bouman on Medium. Medical doctor / Web developer / Security researcher …

medium.com

Gujjuboy10x00 - Medium

Read writing from Gujjuboy10x00 on Medium. security analyst | Keep calm and hack the planet…

I will update this constantly. You are welcome to add everyone I forgot as a comment, I will add to the list instantly. We are stronger together. Please write your suggestions in the comments and we will create a resource pool for everyone. Stay safe and healthy.