Bug Bounty Hand Book

A **bug bounty** program is a deal offered by many websites and software developers by which individuals can receive recognition and compensation for reporting **bugs**, especially those pertaining to exploits and vulnerabilities.

More : https://en.wikipedia.org/wiki/Bug_bounty_program

What is meant by bug bounty?

A **bug bounty program**, also called a vulnerability rewards **program** (VRP), is a crowdsourcing initiative that rewards individuals for discovering and reporting software **bugs**. ... **Bug** reports must document enough information for for the organization offering the **bounty** to be able to reproduce the vulnerability.

What is open bug bounty?

Open Bug Bounty, at xssposed.org, is a non-profit, **open** archive where security researchers can report Cross-Site Scripting (or XSS) vulnerabilities on any website while getting full credit for the report. ... When vulnerabilities are reported, they are verified, and credit is given to the security researcher.

What is a security disclosure policy?

Responsible **disclosure** is a computer **security** term describing a vulnerability **disclosure** model. It is like full **disclosure**, with the addition that all stakeholders agree to allow a period of time for the vulnerability to be patched before publishing the details.

Bug bounty platforms and programs -:

bugcrowd
https://www.bugcrowd.com/

hackerone
https://www.hackerone.com/

synack
https://www.synack.com/

Cobalt
https://cobalt.io/

Zerocopter
https://zerocopter.com/

HACKRFI

https://www.hackr.fi/

BOUNTYFACTORY

https://bountyfactory.io/

Training Labs :-

vulnhub
https://www.vulnhub.com/

Free capture the flag virtual machines to download, run, and practice against.

PentesterLab
https://pentesterlab.com

Free downloadable VMs and paid for online training and labs. Certainly worth checking out.

Tiredful-API
https://github.com/payatu/Tiredful-API

"Tiredful API is intentionally designed broken app. The aim of this web app is to teach developers, QA or security professionals about flaws present in webservices (REST API) due to insecure coding practice."

Books :-

Mastering Modern Web Penetration Testing, Prakhar Prasad, Oct 2016

The Web Application Hacker's Handbook (Second Edition), Dafydd Stuttard & Marcus Pinto, Oct 2011

The Bug Hunters Methodology, Jason Haddix, 2017+ (github)

IoT Pentesting Guide, Aditya Gupta, 2017+ (gitbook)

Videos :-

Bug Bounty PoC Playlist

How To Shot Web—Jason Haddix, 2015

Bug Bounty Hunting Methodology v2—Jason Haddix, 2017

Hunting for Top Bounties—Nicolas Grégoire, 2014

The Secret life of a Bug Bounty Hunter—Frans Rosén, 2016

Finding Bugs with Burp Plugins & Bug Bounty 101—Bugcrowd, 2014

How to hack all the bug bounty things automagically reap the rewards profit—Mike Baker, 2016

Common vulnerability guides :-

OWASP Top 10
OWASP Top 10, 2017 RC2 [PDF]

SSRF Bible Cheetsheet
https://docs.google.com/document/d/1v1TkWZtrhzRLy0bYXBcdLUedXGb9njTNIJXa3u9akHM/edit

File upload Stored XSS
https://brutelogic.com.br/blog/file-upload-xss/

Bug Bounty Writeups :-

Awesome Bug Bounty
https://github.com/djadmin/awesome-bug-bounty

hackerone.com hacktivity
https://hackerone.com/hacktivity?sort_type=popular&filter=type%3Aall&page=1&range=forever

Wordlists, Patterns, Payloads, etc.

ALL.txt
https://gist.github.com/jhaddix/86a06c5dc309d08580a018c66354a056

Jason Haddix's **enormous** list of subdomain strings. Built from publicly seen subdomains, folders, filenames, etc. Grab it and add your own findings if they're missing.

SecLists
https://github.com/danielmiessler/SecLists

A great collection of common filenames, payloads, and more. Have a look through yourself to understand the full scope of this excellent collection.

Passive Reconnaissance :-

Passive reconnaissance tools provide information without actually touching your target while also doing a lot of the hard work for you.

Shodan
https://www.shodan.io/

The search engine for things connected to the internet. IP, port, application, banners, etc.

BuiltWith
https://builtwith.com/

"Find out what websites are Built With"

Censys
https://censys.io/

Censys continually monitors every reachable server and device on the Internet, so you can search for and analyze them in real time. Understand your network attack surface". Check for open ports and applications on a specific IP without running a portscan yourself.

OSINT Toolkit
https://medium.com/osint/the-osint-toolkit-3b9233d1cdf9

Lots of passive reconnaissance tools in here and too many to repeat again.

cert.sh
https://crt.sh/

SSL Certificate allocation based DNS enumeration using the public record of SSL certificates.

Facebook Certificate Transparency Monitoring
https://developers.facebook.com/tools/ct/

“Certificate Transparency is an open framework to log, audit and monitor all publicly-trusted TLS certificates on the Internet. This tool lets you search for certificates issued for a given domain. Subscribe to email updates to be alerted when new certificates are issued.”

Find subdomains for *.example.com bounty scopes via SSL certificate registration information. You can also subscribe to find out when new certificates are issued for your target.

Google Certificate Transparency Monitoring
https://transparencyreport.google.com/https/certificates

Similar to that from Facebook and cert.sh, but from Google.

Forward DNS (FDNS)
https://scans.io/study/sonar.fdns_v2

A 20+GB compressed, 300+GB uncompressed JSON dataset containing the ANY and A/AAAA record query results for a huge number of domains. Download and search through it for a given list of names using a JSON parser or simply using zgrep.

DNS Trails
http://research.dnstrails.com/tools/lookup.htm?domain=example.com

If DNS records are being protected by a firewall such as Cloudflare or Akamai use this to see the DNS record history of a domain. Also useful for non-firewalled DNS entries to see where they pointed in the past in case services are still live or if IP addresses are running new services.

Source Code Analysis :-

GitMiner
https://github.com/UnkL4b/GitMiner

Tool for advanced mining for content on Github. Usernames, passwords, ssh keys, etc.

Link and domain takeovers :-

broken-link-checker
https://github.com/stevenvachon/broken-link-checker

Find broken links in websites. Run with:
blc -rfoi --exclude linkedin.com --exclude youtube.com --filter-level 3 https://example.com/

WAF Bypass

CloudFlair
https://github.com/christophetd/CloudFlair

"CloudFlair is a tool to find origin servers of websites protected by CloudFlare who are publicly exposed and don't restrict network access to the CloudFlare IP ranges as they should.

The tool uses Internet-wide scan data from Censys to find exposed IPv4 hosts presenting an SSL certificate associated with the target's domain name."

Active Reconnaisance :-

Massdns
https://github.com/blechschmidt/massdns

A high performance DNS subdomain enumeration tool. Combine with ALL.txt via the included subbrute.py

```
./subbrute.py ALL.txt example.com | ./bin/massdns -r resolvers.txt -t A -a -o -w results.txt -
```

Gobuster
https://github.com/OJ/gobuster

A high performance directory enumeration tool written in Go. Lightening fast. Combine with ALL.txt

Teh S3 Bucketeers
https://github.com/tomdev/teh_s3_bucketeers/

The replacement for Sandcastle S3, the S3 bucket enumeration and permission check tool. Use with common_bucket_prefixes.txt instead of the default list. There's a lot of scope here to customise the prefix and target list but the foundations of the tool are sound. Combine with the output from massdns for better results.

AWSBucketDump
https://github.com/jordanpotti/AWSBucketDump

A similar tool to The S3 Bucketeers. Combine with the output from massdns for better results.

OSINT Toolkit
https://medium.com/osint/the-osint-toolkit-3b9233d1cdf9

A few active reconnaissance tools in here and again too many to repeat.

IoT Hacking :-

IoT Reading Materials :-

IoT Firmware Analysis
https://www.owasp.org/index.php/IoT_Firmware_Analysis

A quick start guide to analysing and dissecting firmware binaries.

Firmware Analysis Basics
http://iotpentest.com/firmware-analysis-basics/

A similar guide to the OWASP publication with a bit more detail on how to obtain firmware and analyse it. A good accompaniment.

Bug Hunting Drilling Into the Internet of Things (IoT)
https://duo.com/assets/ebooks/Duo-Labs-Bug-Hunting-Drilling-Into-the-Internet-of-Things-IoT.pdf

A very good guide on IoT hardware/app security analysis. The appendix contains a proven process for bypassing certificate pinning on android devices.

IoT Hacking Tools :-

Firmware Analysis Toolkit
https://github.com/attify/firmware-analysis-toolkit

A bundle containing:

- binwak
- firmadyne
- firmwalker
- firmware-mod-kit

Thanks I will Write 2nd Part 😊

Sajibe Kanti

Info Sec Researcher Yogosha SAS