hackerone

Bug Bounty and Web Hacking Tools

Tools and Resources to Start Your Journey

Bug Bounty and Web Hacking Tools

Welcome to the world of bug bounty hunting and web hacking! Whether you're a student or a young adult starting to explore the exciting field of ethical hacking, this document will introduce you to a variety of essential tools and resources to help you get started on your journey.

Proxy & Network Sniffer

Proxy tools allow you to intercept and manipulate web traffic, making them invaluable for identifying vulnerabilities in web applications.

- Burp Suite: A versatile proxy for intercepting and manipulating web traffic. It comes in both free and paid versions and is a must-have for any web security enthusiast.
- OWASP Zap Proxy: A free and powerful proxy tool to intercept and manipulate web traffic, essential for ethical hackers.
- Caido: A lightweight web security auditing toolkit designed to help you find vulnerabilities effectively.
- Wireshark: A network protocol analyzer that lets you capture and inspect network packets, a fundamental tool for understanding network communications.

Burp Extensions

Burp extensions enhance the functionality of Burp Suite, making it an even more powerful tool for web security testing.

- Logger++: This extension logs requests and responses made by all Burp tools, making it easier to analyze and manipulate traffic.
- AuthMatrix: AuthMatrix simplifies testing authorization in web apps and services, helping you define user roles and requests.
- Autorize: Autorize is designed to detect authorization vulnerabilities.
- Burp Bounty: This extension helps you build custom scan checks for Burp Scanner.
- Param Miner: Param Miner identifies hidden, unlinked parameters, a valuable tool for hunting web cache poisoning vulnerabilities.
- Collaborator Everywhere: This extension augments your in-scope proxy traffic by injecting non-invasive headers designed to reveal backend systems by causing pingbacks to Burp Collaborator.

Asset Discovery

Asset discovery and finding additional subdomains are useful to cybersecurity researchers because they provide a comprehensive understanding of an organization's digital footprint and find more attack surface.

- Amass: Amass uses various techniques to gather subdomains and create a network map of the target.
- BuiltWith: A browser extension that quickly identifies the technologies used by a web application.
- subfinder: A tool for discovering valid subdomains using passive online sources.
- dnsgen: Generates domain name combinations from provided input.
- meg: Fetches URLs efficiently, useful for hunting multiple paths across many hosts.
- httpx: A fast and versatile HTTP toolkit for running multiple probes.
- hakrawler: A web crawler designed for quick discovery of endpoints and assets.
- waybackurls: Fetches all URLs archived by the Wayback Machine for a domain.
- aquatone: Aquatone is a tool for visual inspection of websites across a large amount of hosts and is convenient for quickly gaining an overview of HTTP-based attack surface.

Recon Framework

Reconnaissance frameworks are valuable because they streamline and automate the process of discovering vulnerabilities and potential attack vectors by providing pre-built templates and plugins, saving time and enhancing your efficiency.

- nuclei: A fast and configurable scanning tool based on templates, offering extensibility and ease of use.
- sn1per: Discover hidden assets and vulnerabilities.
- Spiderfoot: An open-source intelligence (OSINT) automation tool that integrates with various data sources.
- reNgine: A web application reconnaissance suite with a highly configurable recon process.
- AutoRecon: A multi-threaded network reconnaissance tool designed for time-saving in penetration testing environments.
- Osmedeus: A flexible workflow engine for offensive security, allowing you to run reconnaissance on multiple targets.
- reconFTW: reconFTW automates the entire process of reconnaissance for you. It outperforms the work of subdomain enumeration along with various vulnerability checks and obtaining maximum information about your target.

OSINT Search Engines

Open Source Intelligence (OSINT) search engines help you gather intelligence about your target.

- hunter.io: Email enumeration for large corporations.
- intelx.io: A versatile OSINT tool for various data sources.
- Shodan: A search engine for systems connected to the internet with advanced filters.
- Censys: A public search engine for internet hosts and networks.
- crt.sh: A tool for searching SSL certificates.
- VirusTotal: A comprehensive tool for WHOIS, DNS, and subdomain reconnaissance.
- ZoomEye: A search engine for specific network components.
- NerdyData: A search engine for source code.
- Crunchbase: For finding information about businesses and their acquisitions.
- Searchcode: Helps you find real-world examples of functions, APIs, and libraries in various languages.

Scanners

Scanners help identify vulnerabilities in target systems.

- Nmap: A powerful tool for port scanning and network discovery.
- Masscan: An internet-scale port scanner that can scan the entire internet in minutes.
- Nmap Command Helper: Assists with Nmap commands and includes training features.
- wpscan: WPScan is a free black box WordPress security scanner

Exploitation

Exploitation tools assist in discovering and exploiting vulnerabilities via automation.

- sqlmap: Automates the detection and exploitation of SQL injection flaws and database takeovers.
- ezXSS: An easy way to test (blind) Cross-Site Scripting.
- Metasploit: A comprehensive tool for penetration testing, vulnerability exploitation, and IDS signature development.
- thc-hydra: Hydra is a parallelized login cracker which supports numerous protocols to attack.

Wordlists

Collections of wordlists to aid in password cracking and testing.

- SecLists: A massive collection of wordlists for hacking.
- AssetNote's Wordlists: Wordlists created by AssetNote for various purposes.
- PayloadsAllTheThings: A list of useful payloads and bypass for Web Application Security and Pentest/CTF
- RockYou: A plain text file that contains a list of commonly used password words. This file contains over 14,341,564 passwords that were previously leaked in data breaches.

Others

- CyberChef: An awesome tool for encoding and decoding data.
- webhook.site: A tool for testing, inspecting, and forwarding incoming HTTP requests.
- requestcatcher: Creates a subdomain to test applications by forwarding requests to your browser.
- canarytokens: A tool for detecting unauthorized access to files and systems.
- Axiom: A set of utilities for managing dynamic infrastructure for bug bounty and pentesting.
- KeyHacks: A repository showing how leaked API keys can be checked for validity.
- Updog: A replacement for Python's SimpleHTTPServer with added features.
- PenTest.ws: A penetration testing web application for organizing hosts, services, vulnerabilities, and credentials.

Fuzzing

The value of fuzzing tools lies in their ability to automatically and systematically test software for vulnerabilities and discover content by inputting malformed or unexpected data, helping to uncover unknown or overlooked weaknesses or endpoints that could be exploited by attackers.

- FFuF: A fast fuzzing tool for brute-forcing directories and parameters.
- dirsearch: A command-line tool for brute-forcing directories and files.
- FeroxBuster: A fast content discovery tool written in Rust.
- gobuster: Directory/File, DNS and VHost busting tool written in Go

Notes & Organization

Keeping meticulous notes and maintaining a well-organized approach is not just good practice; it's a crucial element of your success in order to produce an efficient workflow and collaboration.

- Reconness: Helps organize your reconnaissance and focus on potentially vulnerable targets.
- Notion: An all-in-one tool for writing, planning, and organizing.
- Joplin: A free, open-source note-taking and to-do application.
- Xmind: A mind mapping and brainstorming tool.

Now that you're familiar with these tools, dive into the world of bug bounty hunting and ethical hacking. Remember to use them responsibly and adhere to ethical hacking principles. Good luck, and happy hunting!

Note: This is not an exhaustive list of tools, and their inclusion here does not imply endorsement or promotion. These tools are provided as a starting point for educational purposes in bug bounty hunting and web security research and we encourage everyone to adapt and leverage the tools in the way that works best with their methodology.