RESOURCES

What is Hacker101?

Hacker101 is a free educational resource developed by HackerOne to grow and empower the hacker community at large. We have video lessons and curated resources to help you learn the concepts of hacking and a Capture the Flag where you can turn that theory into practice.

What is the Hacker101 CTF?

The Hacker101 CTF – or Capture the Flag – is a game where you hack through levels to find bits of data called flags. These flags mark your progress and allow you to receive invitations to private programs on HackerOne, where you can use your newly-learned skills.

I'm new to all of this; how do I get started?

Congratulations on taking the first step to becoming a hacker! We recommend starting with our Hacker101 for Newcomers and Burp Suite playlists. Once you've completed that, start working through the Hacker101 CTF and watching the other video lessons as you need them. While there are no prerequisites for Hacker101, strictly speaking, there are things you can learn to accelerate your hacking education. Note that you don't need to know all of this – or any – to get started. Here's a curated list of resources:

- Programming
  - JavaScript: This is the language used on the majority of web pages. Understanding it is useful for bug hunting because many bugs actually stem from JS code.
  - Python: Commonly used for automating various activities during testing, as well as being useful for general programming.
  - SQL: Used by most applications for accessing and manipulating data. Knowledge of SQL will help in discovering and exploiting critical SQL Injection vulnerabilities.
- Networking
  - Terminology guide: You'll hear many terms from IP address to port to DNS. This guide will help you understand that.
  - Common Port Numbers: A useful list of common port numbers and the associated services.
- Linux
  - Setting up your own web server: While not security-related in itself, this will teach you many of the commands and concepts you need to know to become a great hacker.
  - Setting up Kali Linux on Virtualbox: Kali is a hacking-oriented Linux distribution, used by many bug hunters. This guide will help you set it up in a virtual machine.
  - Command Line Guide: You'll end up using many command-line tools as a hacker, so a familiarity with its structure and use is valuable.

I've been hacking for a while now; how do I get into bug bounties?

We recommend signing up for a HackerOne account and checking out our extensive programs. Additionally, you can earn invitations to private programs on HackerOne via the Hacker101 CTF. This gets you into programs with fewer hackers, often making it easier to find interesting and impactful bugs.

Programming languages

Programming is an important part of being a successful hacker. This isn't a comprehensive list of programming languages and nearly any can be used for most hacking tasks, especially on the web, but rather a list of languages we find especially useful or notable.

- Python and Ruby: Useful for automation and quick testing and analysis, particularly for web hacking.
- JavaScript: Can be used for the same tasks as Python and Ruby (albeit with fewer relevant libraries), but mostly useful to know for analysis of code on the web, as well as exploitation.
- Objective-C and Swift: The ability to read these will be essential if you plan to do source code review of iOS applications.
- Java and Kotlin: The ability to read these will be essential if you plan to do source code review of Android applications. Java is produced by decompilers for Android applications, which allows you to read code (roughly) equivalent to the original source, even when you only have a compiled application.
- AArch64 assembly: For advanced embedded and mobile hacking, understanding the very lowest level of abstraction is essential.

Web hacking tools

This is a curated list of web hacking tools and is not intended to be comprehensive; rather, we want to highlight the tools we find especially useful.

- Altdns: Altdns is a DNS recon tool that allows for the discovery of subdomains that conform to patterns. Altdns takes in words that could be present in subdomains under a domain (such as test, dev, staging), as well as a list of known subdomains.

- Amass: The OWASP Amass Project performs network mapping of attack surfaces and external asset discovery using open source information gathering and active reconnaissance techniques.
- Aquatone: Aquatone is a tool for visual inspection of websites across a large number of hosts, which provides a convenient overview of HTTP-based attack surface.
- BBHT: Bug Bounty Hunting Tools is a script to install the most popular tools used while looking for vulnerabilities for a bug bounty program.
- Burp Suite: This is the most popular proxy in web hacking circles due to its cross-platform nature and extensive featureset. See our playlist to make the most of it. Also see our "Burp Suite Plugins" list for useful plugins to use.
- chaos: Chaos actively scans and maintains internet-wide assets' data. This project is meant to enhance research and analyze changes around DNS for better insights.
- Commit-stream: Commit-stream extracts commit logs from the Github event API, exposing the author details (name and email address) associated with Github repositories in real time.
- Dirb: DIRB is a web content scanner. It launches a dictionary based attack against a web server and analyzes the response.
- Dirsearch: a simple command line tool designed to brute force directories and files in websites.
- Dngrep: A utility for quickly searching presorted DNS names. Built around the Rapid7 rdns & fdns dataset.
- Dnscan: dnscan is a python wordlist-based DNS subdomain scanner
- Dnsgen: This tool generates a combination of domain names from the provided input. Combinations are created based on wordlist. Custom words are extracted per execution.
- Dnsprobe: DNSProbe is a tool built on top of retryabledns that allows you to perform multiple dns queries of your choice with a list of user supplied resolvers.
- EyeWitnees: EyeWitness is designed to take screenshots of websites, provide some server header info, and identify any default credentials. EyeWitness is designed to run on Kali Linux. It will auto detect the file you give it with the -f flag as either being a text file with URLs on each new line, nmap xml output, or nessus xml output. The –timeout flag is completely optional, and lets you provide the max time to wait when trying to render and screenshot a web page.
- Ffuf: A fast web fuzzer written in Go.
- Findomain: Findomain offers a dedicated monitoring service hosted in Amazon (only the local version is free), that allows you to monitor your target domains and send alerts to Discord and Slack webhooks or Telegram chats when new subdomains are found.
- Gau: getallurls (gau) fetches known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl for any given domain. Inspired by Tomnomnom's waybackurls.
- gitGraber: gitGraber is a tool developed in Python3 to monitor GitHub to search and find sensitive data in real time for different online services.
- Httprobe: Takes a list of domains and probes for working http and https servers.
- Jok3r: Jok3r is a framework that helps penetration testers with network infrastructure and web security assessments. Its goal is to automate as much as possible in order to quickly identify and exploit "low-hanging fruit" and "quick win" vulnerabilities on most common TCP/UDP services and most common web technologies (servers, CMS, languages...).
- JSParser: A python 2.7 script using Tornado and JSBeautifier to parse relative URLs from JavaScript files. This is especially useful for discovering AJAX requests when performing security research or bug bounty hunting.
- Knockpy: Knockpy is a python tool designed to enumerate subdomains on a target domain through a word list. It is designed to scan for a DNS zone transfer and bypass the wildcard DNS record automatically, if it is enabled. Knockpy now supports queries to VirusTotal subdomains, you can set the API_KEY within the config.json file.
- lazyrecon: This is an assembled collection of tools for performing recon.
- lazys3: A Ruby script to brute-force for AWS s3 buckets using different permutations.
- Masscan: This is an Internet-scale port scanner. It can scan the entire Internet in under 6 minutes, transmitting 10 million packets per second, all from a single machine.
- Massdns: MassDNS is a simple high-performance DNS stub resolver targeting those who seek to resolve a massive amount of domain names in the order of millions or even billions. Without special configuration, MassDNS is capable of resolving over 350,000 names per second using publicly available resolvers.
- Meg: Meg is a tool for fetching lots of URLs without taking a toll on the servers. It can be used to fetch many paths for many hosts, or fetching a single path for all hosts before moving on to the next path and repeating.
- mitmproxy: This is an open-source proxy written in Python. Not recommended for beginners, but this can be a powerful tool.
- Naabu: naabu is a port scanning tool written in Go that allows you to enumerate valid ports for hosts in a fast and reliable manner. It is a really simple tool that does fast SYN scans on the host/list of hosts and lists all ports that return a reply.
- Nikto2: Like DirBuster, but also does some basic checks for known vulnerabilities.
- Nuclei: Nuclei is a fast tool for configurable targeted scanning based on templates offering massive extensibility and ease of use.
- OWASP Zed: OWASP Zed Attack Proxy (ZAP) is an open source tool which is offered by OWASP (Open Web Application Security Project), for penetration testing of your website/web application. It helps you find the security vulnerabilities in your application.
- Recon_profile: This tool is to help create easy aliases to run via an SSH/terminal.
- Recon-ng: Recon-ng is a full-featured reconnaissance framework designed with the goal of providing a powerful environment to conduct open source, web-based reconnaissance quickly and thoroughly.
- Shhgit: Shhgit finds secrets and sensitive files across GitHub code and Gists committed in nearly real-time by listening to the GitHub Events API.
- Shuffledns: shuffleDNS is a wrapper around massdns written in go that allows you to enumerate valid subdomains using active bruteforce, as well as resolve subdomains with wildcard handling and easy input-output support.

- sqlmap: This allows for easy discovery and exploitation of SQL injection vulnerabilities. It **will not** catch every bug or even be able to exploit some known SQLi bugs. What it will do is make your life much easier in the 80% of cases it will work for.
- SSL Labs Server Test: This is an easy to use webapp for testing the SSL configuration of web servers.
- Subfinder: subfinder is a subdomain discovery tool that discovers valid subdomains for websites by using passive online sources. It has a simple modular architecture and is optimized for speed. subfinder is built for doing one thing only - passive subdomain enumeration, and it does that very well.
- Subjack: Subjack is a Subdomain Takeover tool written in Go designed to scan a list of subdomains concurrently and identify ones that are able to be hijacked. With Go's speed and efficiency, this tool really stands out when it comes to mass-testing. Always double check the results manually to rule out false positives.
- Sublert: Sublert is a security and reconnaissance tool that was written in Python to leverage certificate transparency for the sole purpose of monitoring new subdomains deployed by specific organizations and an issued TLS/SSL certificate. The tool is supposed to be scheduled to run periodically at fixed times, dates, or intervals (Ideally each day). New identified subdomains will be sent to Slack workspace with a notification push. Furthermore, the tool performs DNS resolution to determine working subdomains.
- Sublist3r: Sublist3r is a python tool designed to enumerate subdomains of websites using OSINT. It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS.
- Teh_s3_bucketeers: Teh_s3_bucketeers is a security tool to discover S3 buckets on Amazon's AWS platform.
- Unfurl: Unfurl is a tool that analyzes large collections of URLs and estimates their entropies to sift out URLs that might be vulnerable to attack.
- Virtual-host-discovery: This is a basic HTTP scanner that enumerates virtual hosts on a given IP address. During recon, this might help expand the target by detecting old or deprecated code. It may also reveal hidden hosts that are statically mapped in the developer's /etc/hosts file.
- Waybackurls: Accept line-delimited domains on stdin, fetch known URLs from the Wayback Machine for *.domain and output them on stdout.
- Webscreenshot: A simple script to screenshot a list of websites, based on the url-to-image PhantomJS script.
- Wfuzz: Wfuzz has been created to facilitate the task in web applications assessments and it is based on a simple concept: it replaces any reference to the FUZZ keyword by the value of a given payload.
- Whatweb: WhatWeb recognises web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices. WhatWeb has over 1800 plugins, each to recognise something different. WhatWeb also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.
- Wpscan: WPScan is a free (for non-commercial use) black box WordPress security scanner written for security professionals and bloggers to test the security of their sites.
- nmmapper: A Collection of 8 subdomain finders hosted online for quick usage, this include, sublist3r, amass, findomain,knocky,anubis subdomain finder, dnscan, nmap subrute,lepu subdomain and even waybackurl.

Burp Suite plugins

Burp Suite: The quintessential web app hacking tool. Once you hit 500 reputation on HackerOne, you are eligible for a free 3-month license of Burp Suite Pro!

This is a curated list of Burp plugins and is not intended to be comprehensive; rather, we want to highlight the plugins we find especially useful.

- ActiveScan++: ActiveScan++ extends Burp Suite's active and passive scanning capabilities. Designed to add minimal network overhead, it identifies application behavior that may be of interest to advanced testers.
- Autorepeater Burp: Automated HTTP request repeating with Burp Suite.
- Autorize Burp: Autorize is an extension aimed at helping the penetration tester to detect authorization vulnerabilities —one of the more time-consuming tasks in a web application penetration test.
- BurpSentinel: With BurpSentinel it is possible for the penetration tester to quickly and easily send a lot of malicious requests to parameters of a HTTP request. Not only that, but it also shows a lot of information of the HTTP responses, corresponding to the attack requests. It's easy to find low-hanging fruit and hidden vulnerabilities like this, and it also allows the tester to focus on more important stuff!
- Flow: This extension provides a Proxy history-like view along with search filter capabilities for all Burp tools.
- Headless Burp: This extension allows you to run Burp Suite's Spider and Scanner tools in headless mode via the command-line.
- Logger++: Logger++ is a multi-threaded logging extension for Burp Suite. In addition to logging requests and responses from all Burp Suite tools, the extension allows advanced filters to be defined to highlight interesting entries or filter logs to only those which match the filter.
- WSDL Wizard: This extension scans a target server for WSDL files. After performing normal mapping of an application's content, right click on the relevant target in the site map, and choose "Scan for WSDL files" from the context menu. The extension will search the already discovered contents for URLs with the .wsdl file extension, and guess the locations of any additional WSDL files based on the file names known to be in use. The results of the scanning appear within the extension's output tab in the Burp Extender tool.

Mobile hacking tools

This is a curated list of mobile hacking tools and is not intended to be comprehensive; rather, we want to highlight the tools we find especially useful.

- dex2jar: Converts dex code (Android bytecode) into Java JAR files for manipulation or decompilation.
- dotPeek: A .NET decompiler, for use with Xamarin Android applications.
- Frida "Universal" SSL Unpinner: Universal unpinner.
- Frida: This is an instrumentation system allowing injection of JavaScript or native libraries into arbitrary mobile applications on iOS and Android. In essence, it makes it painless to change, enhance, or disable functionality in applications.
- Genymotion: Cross-platform Android emulator for developers & QA engineers. Develop & automate your tests to deliver best quality apps.
- Jadx: Jadx is a dex to Java decompiler. The command line and GUI tools for producing Java source code from Android Dex and Apk files.
- JD-GUI: This is a Java decompiler, useful after dex2jar for easy analysis of Android apps.
- MobSF: An automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.
- Online Decompiler: APK, JAR and .NET online decompiler.
- Radare2: A free/libre toolchain for easing several low level tasks, such as forensics, software reverse engineering, exploiting, debugging, etc. It is composed by a large number of libraries (which are extended with plugins) and programs that can be automated with almost any programming language.

Android hacking tools

This is a curated list of Android hacking tools and is not intended to be comprehensive; rather, we want to highlight the tools we find especially useful.

Videos

- Hacker101 - Android Quickstart
- Hacker101 - Mobile Hacking Crash Course
- Hacker101: Common Android Bugs Pt. 1
- Hacker101: Common Android Bugs Pt. 2
- Android Pentesting Video Playlist
- Low Competition Bug Hunting (What to Learn) - ft. #AndroidHackingMonth

Blog Posts

- #Androidhackingmonth: Introduction to Android Hacking by @0xteknogeek
- QA with Android Hacker: Bagipro
- Hacking SMS API Service Provider of a Company - Android App Static Security Analysis
- Getting Started in Android Apps Pen-testing (Part-1)

Example Reports

- Periscope android app deeplink leads to CSRF in follow action
- Twitter lite(Android): Vulnerable to local file steal, Javascript injection, Open redirect
- Golden techniques to bypass host validations in Android apps
- SQL Injection found in NextCloud Android App Content Provider
- Quora Android - Possible to steal arbitrary files from mobile device
- Opening arbitrary URLs/XSS in SAMLAuthActivity
- Access of Android protected components via embedded intent

Other Resources

- The Mobile Hacking CheatSheet
- Mobile App Pentest Cheatsheet
- Awesome Mobile Security
- Mobile Penetration Testing Kit
- Periscope android app deeplink leads to CSRF in follow action

Practice Labs

- Damn Insecure and vulnerable App for Android
- InjuredAndroid
- Android-InsecureBankv2

Desktop / embedded hacking tools

This is a curated list of hacking tools for native applications and embedded devices and is not intended to be comprehensive; rather, we want to highlight the tools we find especially useful.

- american fuzzy lop: AFL is an extremely powerful fuzzer, enabling detection of complicated bugs in many applications and libraries.
- Binary Ninja: Another low-cost alternative to IDA. Its API is perhaps the most powerful of the three for automating analysis of code.
- Binwalk: Used for firmware analysis and extraction. This is primarily useful for embedded Linux devices.
- dotPeek: A powerful decompiler for .NET assemblies.
- GNU strings: Finds strings in arbitrary binaries. While not strictly for reverse-engineering, it is among the most useful tools around.
- Hopper: This is a fantastic, low-cost disassembler and decompiler that runs on macOS and Linux. While it's no replacement for IDA, it is a great choice for most applications.
- HxD (Windows) 0xED (macOS): These are graphical hex editors, useful for analysis and manipulation of files and block devices.
- IDA Pro and Hex-Rays Decompiler: IDA is the absolute gold standard for disassemblers and its decompiler plugins are the gold standard for decompilation. It is a wonderful tool with support for nearly every obscure platform and an extensive (if confusing) SDK to add nearly any feature you can imagine. However, its price makes it difficult to justify.
- PE Explorer: This is a great tool for analyzing the PE binaries used on Windows. It allows for exploration of the structures of the executable itself, as well as resources.
- PEiD: Tool for detecting cryptors, packers, and encryption routines in Windows PE binaries.
- QEMU: An emulator and virtual machine supporting a large number of systems/architectures. This makes it useful for things like running embedded firmware, but also includes debugging facilities that make it an optimal tool for hacking. Can be combined with AFL for fuzzing of binaries that aren't for your native architecture.
- Radare2: This is a set of tools for doing analysis of binaries. It includes everything from disassembly to debugging and more.
- Unicorn Engine: This is a library rather than a standalone tool, but it makes writing quick emulators a breeze. Particularly useful for reverse-engineering.

Exploitation resources

This is a curated list of exploitation resources and is not intended to be comprehensive; rather, we want to highlight the tools we find especially useful.

- NoSQLMap: NoSQLMap is an open source Python tool designed to audit for, as well as automate injection attacks, and exploit default configuration weaknesses in NoSQL databases and web applications using NoSQL to disclose or clone data from the database.
- Retire.JS: Scanning website for vulnerable js libraries.
- Spiderfoot: SpiderFoot is an open source intelligence (OSINT) automation tool. It integrates with just about every data source available, and automates OSINT collection so that you can focus on data analysis.
- sqlmap: sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester, and a broad range of switches including: database fingerprinting, over data fetching from the database, accessing the underlying file system, and executing commands on the operating system via out-of-band connections.
- SQLNinja: Sqlninja is a tool targeted to exploit SQL Injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end.
- SSRFTest: SSRF testing tool.
- XSS Hunter: XSS Hunter allows you to find all kinds of cross-site scripting vulnerabilities, including the often-missed blind XSS. The service works by hosting specialized XSS probes which, upon firing, scan the page and send information about the vulnerable page to the XSS Hunter service.
- Ysoserial: A proof-of-concept tool for generating payloads that exploit unsafe Java object deserialization.

Scanners / frameworks

This is a curated list of scanners and frameworks and is not intended to be comprehensive; rather, we want to highlight the tools we find especially useful.

- Canvas: CANVAS offers hundreds of exploits, an automated exploitation system, and a comprehensive, reliable exploit development framework to penetration testers and security professionals worldwide.
- IronWASP: IronWASP (Iron Web Application Advanced Security testing Platform) is an open source tool used for web application vulnerability testing. It is designed in such a way that users having the right knowledge can create their own scanners using this as a framework. IronWASP is built using Python and Ruby and users having knowledge of them would be able to make full use of the platform. However, IronWASP provides a lot of features that are simple to understand.
- Lazyrecon: LazyRecon is a script written in Bash, intended to automate the tedious tasks of reconnaissance and information gathering. The information is organized in an html report at the end, which helps you identify next steps.
- Maltego: Maltego is an open source intelligence (OSINT) and graphical link analysis tool for gathering and connecting information for investigative tasks.
- Metasploit: Metasploit is an open source penetration testing framework.

- Nikto: Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.
- Nmap: Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.
- OpenVAS: OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated testing, authenticated testing, various high level and low level Internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.
- Osmedeus: Osmedeus allows you to automatically run the collection of awesome tools for reconnaissance and vulnerability scanning against the target.
- Reconness: ReconNess helps you to run and keep all your #recon in the same place allowing you to focus only on the potentially vulnerable targets without distraction and without requiring a lot of bash skill, or programming skill in general.
- Sn1per: Sn1per Community Edition is an automated scanner that can be used during a penetration test to enumerate and scan for vulnerabilities. Sn1per Professional is Xero Security's premium reporting addon for Professional Penetration Testers, Bug Bounty Researchers and Corporate Security teams to manage large environments and pentest scopes.
- Wapiti: Wapiti allows you to audit the security of your websites or web applications. It performs "black-box" scans (it does not study the source code) of the web application by crawling the web pages of the deployed webapp, looking for scripts and forms where it can inject data.

Datasets / freemium services

This is a curated list of datasets and freemium services and is not intended to be comprehensive; rather, we want to highlight the tools we find especially useful.

- C99.nl: Subdomain Finder is a scanner that scans an entire domain to find as many subdomains as possible.
- Censys: Censys scans the most ports and houses the biggest certificate database in the world, and provides the most up-to-date, thorough view of your known and unknown assets.
- Payloads All The Things: A list of useful payloads and bypasses for Web Application Security. Feel free to improve with your payloads and techniques.
- Rapid7 Forward DNS (FDNS): This dataset contains the responses to DNS requests for all forward DNS names known by Rapid7's Project Sonar.
- Seclists: SecLists is the security tester's companion. It's a collection of multiple types of lists used during security assessments, collected in one place. List types include usernames, passwords, URLs, sensitive data patterns, fuzzing payloads, web shells, and many more. The goal is to enable a security tester to pull this repository onto a new testing box and have access to every type of list that may be needed.
- Shodan: Shodan provides a public API that allows other tools to access all of Shodan's data. Integrations are available for Nmap, Metasploit, Maltego, FOCA, Chrome, Firefox and many more.

Miscellaneous hacking tools

This is a curated list of miscellaneous hacking tools and is not intended to be comprehensive; rather, we want to highlight the tools we find especially useful.

- Altair: Altair GraphQL Client helps you debug GraphQL queries and implementations - taking care of the hard part so you can focus on actually getting things done.
- BuiltWith: BuiltWith's goal is to help developers, researchers and designers find out what technologies web pages are using, which may help them decide what technologies to implement themselves.
- Ettercap: Ettercap is a comprehensive suite which features sniffing of live connections, content filtering, and support for active and passive dissection of many protocols, including multiple features for network and host analysis.
- Foxyproxy: FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.
- John the Ripper: John the Ripper is free and Open Source software, distributed primarily in a source code form.
- Swiftness X: A note taking tool for BB and pentesting.
- THC Hydra: This tool is a proof-of-concept code, designed to give researchers and security consultants the possibility to show how easy it would be to gain unauthorized access from remote to a system.
- Transformations: Transformations makes it easier to detect common data obscurities, which may uncover security vulnerabilities or give insight into bypassing defenses.
- Wappalyzer: Wappalyzer is a browser extension that uncovers the technologies used on websites. It detects content management systems, eCommerce platforms, web servers, JavaScript frameworks, analytics tools and many more.
- Wireshark: Wireshark® is a network protocol analyzer that lets you capture and interactively browse the traffic running on a computer network.

Jump to

- What is Hacker101?
- What is the Hacker101 CTF?