Bug Bounty for Beginners

Part -1

Index

Introduction

Imagine yourself as a modern-day Sherlock Holmes, except instead of dusty crime scenes, you delve into the intricate digital landscapes of websites and apps. Bug bounties are your invitation to put on your detective hat and help organizations uncover hidden weaknesses in their systems.

Scope means the area in which we can or allow bug hunting beyond the scope It is invalid but if we can prove that the bug is affecting the organization we will have a high chance of getting rewarded

So basically, in the scope, there are generally three types they are

- Small Scope
- Medium Scope
- Large Scope

Crack the Code on a Tiny Case (Small Scope): Starting out? Small scope programs are your training ground. Focus on specific app features, like a website's login system. Think of it as mastering the security of a single room in a house.

Unravel a Multi-Room Mystery (Medium Scope): Ready to up the ante? Medium scope programs offer broader hunting grounds. You might explore multiple features, delve into an app's internal workings (APIs), and unearth more complex vulnerabilities. Imagine confidently securing an entire floor of a house.

Become a Master Hacker (Large Scope): Feeling adventurous? Large scope programs let you unleash your full security expertise. Explore an organization's entire digital empire, from websites and apps to their cloud storage. This is like securing a sprawling mansion, top to bottom. The potential rewards for critical vulnerabilities can be substantial!

Bonus Tool: Google Dorking - Your Digital Magnifying Glass

Security researchers use a cool technique called Google Dorking. It's like crafting magic search queries using Google's secret codes to unearth hidden clues about a

target system. Remember, use this power responsibly and always follow the program's rules!

Now Let’s Get Ready to Join the Thrill of the Hunt.

Bug bounties are an exciting way to test your skills, sharpen your mind, and make a real difference in the digital world. By helping organizations plug security holes, you're contributing to a safer online space for everyone. Here's a roadmap to get you started:

Become a Bounty Hunter: Explore platforms like HackerOne, Bugcrowd, and BountyFactory to find bug bounty programs. Burp Suit, Wireshark, and Nmap will be the common tools over here

Study about OWASP top 10 vulnerabilities it will helps us to understand major types of bugs

Sharpen Your Skills: Websites like Bugcrowd Blog and PortSwigger Web Security Academy as well as we will use some tools that are available on GitHub offer fantastic resources for aspiring bug bounty hunters.

Small Scope

When the organization allows testing on one or two subdomains, it is called a small Scope.

Like example

- Test.example.com
- Pord.example.com

Now we will discuss various techniques that are used to hunt on small-scope

1. Directory Brute force

   We will try to look into the subdomains directory where we will have chances to exploit a bug over here.

   The tools we will use in this case are
   - Dirsearch
   - Gobuster
   - Feroxbuster

2. Fuzzing and Seclist

   In the text field of the website, we will want to try to enter the wrong format of input to analyze the behavior of the website and sometimes it may lead to a bug. For giving a parameter in the fuzzing we need a dedicated wordlist to perform the attack for that purpose we will seclist to create a wordlist

   The tools we will use in this case are
   - Ffuf for Fuzzing Link: https://github.com/ffuf/ffuf.git
   - Wappalyzer to know what technology is used on that website
   - Whatweb Kali Linux tool

3. Port scanning

   It will helps us to understand that in the port the website is hosted so by the port we can specifie our attack

   The tools we will use in this case are
   - Nmap it is best tool
   - Naabu

4. Js analysis

   In these, we will try to understand the JavaScript version as well as which library is used to build that we will have an easy way to find the vulnerabilities based on the version they used to develop the website and there are chances where we will find API keys that are used for that website

   The tools we will use in this case are

   - Secretfinder link: https://github.com/m4ll0k/SecretFinder.git
   - Js link finder its one of the burp suite feature

5. Way back URLs

   It will help us to find at which time the website looked like there are chances like where they will not update some files or version on that website and it will potentially leads to a big bug for the organization.

   Wayback Url: https://wayback-api.archive.org/

6. Data breach Analysis

   There are chances data might get link in the organization but they were not aware about it. It might available in the dark web and some telegram channels and if u find it and report to organization you will have chance to get rewarded

Medium Scope

In these, we will have multiple subdomains to hunt in that organization so we will have higher chances of getting bugs as compare to small scope

As we know we will use all techniques of small scope over her and we will discuss that are not mention in small scope

Like example

*.example.com

Now we will see various techniques that are used in medium-scope

1. Finding subdomains

   It's important stage where we need to find all the subdomains of the website so that we will have the range and actual target on that organization.

   The tools we will use in this case are

   - Google docking
   - Sub finder link: https://github.com/projectdiscovery/subfinder.git
   - Amass link: https://github.com/owasp-amass/amass.git
   - Crt.sh link: https://github.com/az7rb/crt.sh

2. Filter live subdomains

   After finding all sub domains we need to filter out which are active state so that it will helps to find bugs much easier way

   The tools we will use in this case are

   - Httpx link: https://github.com/projectdiscovery/httpx.git

3. Eye witness

   After filtering live subdomains some time it may lead to a big list but if we use eyewitness technique we can take screenshot of each and every running subdomain website and stored in image form and it will helps to look entire subdomains.

   The tools we will use in this case are

   - Link https://github.com/RedSiege/EyeWitness.git

4. Template-based scan

   security template is a pre-defined format or structure used to write clear and comprehensive reports about discovered security vulnerabilities. It acts as a guide for ethical hackers (security researchers) to ensure their reports contain all the essential information a company needs to effectively understand, evaluate, and address the security issue.

   The tools we will use in this case are

   - Nuclei link: https://github.com/projectdiscovery/nuclei.git to make vulnerability scan

Large Scope

We will full scope on the entire organization so that we will have a high chance of getting bugs in that website.

As of now, we have seen tools that are used in each dedicated process so we will discuss Frameworks that will contain most of the tools

Frameworks that are used in these scenarios

- Reconftw link: https://github.com/six2dez/reconftw.git
- Arsenal link: https://github.com/Orange-Cyberdefense/arsenal.git

Every tool of Bug Bounty will be available in the framework but my suggestion is that every three months you need to reinstall it so that the tools might get updated and if you are a beginner try to install and use every tool individually so that you will understand bug bounty concept easily and efficiently.

Google Docking

As a bug bounty hunter, you're always on the lookout for ways to uncover hidden vulnerabilities and sensitive information on websites. One powerful technique that can help you do just that is Google Dorking, also known as Google Hacking. In this article, we'll dive into the world of Google Dorking, exploring its basics, advanced techniques, and tools to help you get started.

Basic Dorks: The Building Blocks

Before we dive into the advanced stuff, let's cover the basics. Google Dorks are essentially custom search queries that help you find specific information on the web. Here are a few examples to get you started:

Subdomain Discovery: Use site:example.com -inurl:www to find subdomains on a website.

Directory Discovery: Try site:example.com "index of" to uncover directories indexed by Google.

File Discovery: Use site:example.com filetype:pdf to find PDF files on a website.

Advanced Dorks: Uncovering Hidden Gems

Now that you've got the basics down, let's move on to some more advanced techniques. These dorks can help you uncover vulnerabilities, sensitive data, and error messages on websites:

Vulnerability Detection: Use inurl:wp-admin to find WordPress administrative pages that might be vulnerable to attacks.

Sensitive Data Discovery: Try site:example.com "password" to find pages containing the word "password".

Error Message Detection: Use site:example.com "404 Not Found" to find pages with a 404 error message.

Automation with Pagodo: Taking it to the Next Level

Manually searching for dorks can be time-consuming. That's where Pagodo comes in – a Python tool that automates Google Dorking for you. With Pagodo, you can query hundreds of dorks on Google and save the results for later use. Here's how to get started:

Install Pagodo: Clone the repository from GitHub and install the required dependencies.

Update GHDB: Run the GHDB scraper to update your database with the latest dorks.

Run Pagodo: Use the command-line interface to run Pagodo with your target website and chosen dorks.

Tools and Resources: Your Google Dorking Arsenal

To take your Google Dorking skills to the next level, you'll need some additional tools and resources:

Google Hacking Database (GHDB): A vast collection of Google Dorks and vulnerability reports from multiple tools.

Cheatsheets and Guides: Detailed instructions and guides on how to use Google Dorking effectively.

Important Considerations: Playing by the Rules

Remember, with great power comes great responsibility. Always ensure you have permission to perform these searches, and be cautious with your search history to avoid raising any red flags.

By mastering the art of Google Dorking, you'll be able to uncover hidden vulnerabilities and sensitive information on websites, making you a more effective bug bounty hunter.