Bug Hunting on Autopilot, Free VPS Setup

Om Arora · Follow
Published in InfoSec Write-ups · 4 min read · Aug 19

Are you get tired of having to keep your PC on for hours for running the tools ?

Do you want to keep running tools without having your laptop on?

And even get notifications on your phone when you find something interesting?

You are at the right place!!

So What Is A VPS ?

Imagine you have a powerful computer that you can split into smaller parts. Each part acts like its own mini-computer with its own space and resources. This is similar to how a Virtual Private Server (VPS) works.

How Can it Help With Bug Bounties?

A VPS is like having a special remote computer that you can use just for these bug bounty hunts. It's not a physical computer, but it works like one. With a VPS, you can set up tools and programs to automatically search for security issues in websites and apps. This lets you hunt for bugs even when you're not using your personal computer, and it can run these tasks 24/7.

What are some of the platforms that provide VPS service ?

1. AWS EC2
2. DigitalOcean
3. Linode
4. Vultr
5. Google Cloud Platform (GCP)
6. Microsoft Azure
7. Oracle Cloud Infrastructure (OCI)
8. UpCloud
9. Hetzner Cloud

Are They Free?

These platforms provide a starting credit that is valid for 3–4 months after which you have to pay.

Today we will be using Digital Ocean because they provide a $200 credit for students which is valid for 1 whole year.

So all you need is a student email to get a free VPS and even if you can't get one don't worry you can use This Referral Link To get free $200 credit

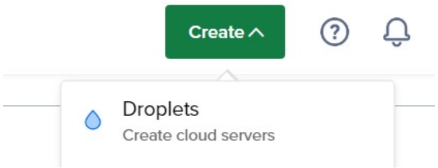
So Let's Get Started!

Registration

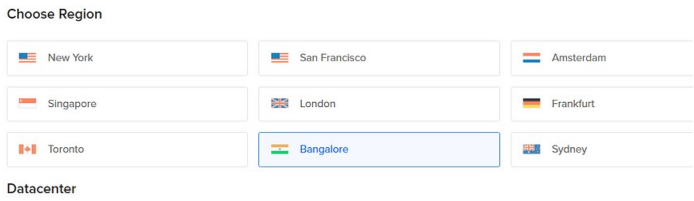
So first you need to create an account of course, if you are a student you can link your account with GitHub to claim the $200

If you are not a student you can use https://m.do.co/c/b5c80ea3da15 this referral link to create an account and get $200 credit and get started with the automation!

Once you are registered click on the Create button on the top right corner and select Droplets



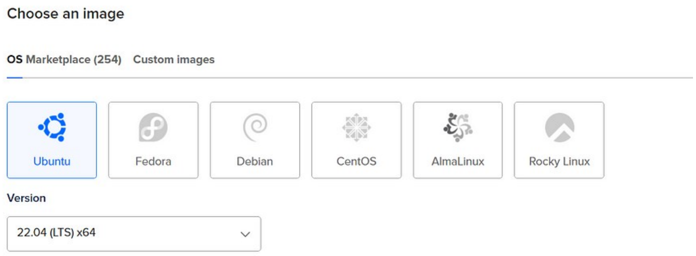
Then It asks you to choose a region, choose the one you live closest to.


Choose Region

New York	San Francisco	Amsterdam
Singapore	London	Frankfurt
Toronto	Bangalore	Sydney

Datacenter

Now Select an image, I am going to use ubuntu


Choose an image

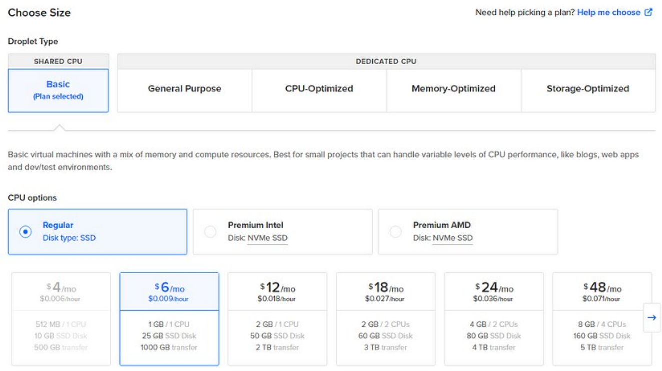
OS Marketplace (254)   Custom images

Ubuntu   Fedora   Debian   CentOS   AlmaLinux   Rocky Linux

Version

22.04 (LTS) x64

Now while selecting the plan you need to choose wisely, I will advice to start with the basic plan to get to know your needs and how much you use it.


Choose Size

Need help picking a plan? Help me choose

Droplet Type

SHARED CPU	DEDICATED CPU			
Basic (Plan selected)	General Purpose	CPU-Optimized	Memory-Optimized	Storage-Optimized

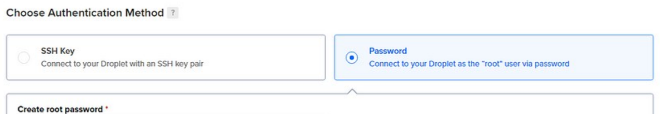
Basic virtual machines with a mix of memory and compute resources. Best for small projects that can handle variable levels of CPU performance, like blogs, web apps and dev/test environments.

CPU options

● Regular Disk type: SSD
○ Premium Intel Disk: NVMe SSD
○ Premium AMD Disk: NVMe SSD

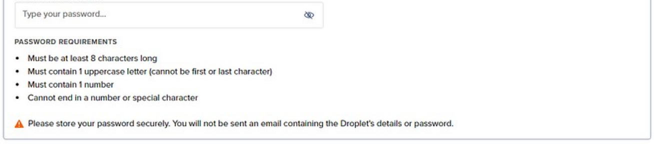
$4/mo	$6/mo	$12/mo	$18/mo	$24/mo	$48/mo
$0.006/hour	$0.009/hour	$0.018/hour	$0.027/hour	$0.036/hour	$0.071/hour
512 MB / 1 CPU 10 GB SSD Disk 500 GB transfer	1 GB / 1 CPU 25 GB SSD Disk 1000 GB transfer	2 GB / 1 CPU 50 GB SSD Disk 2 TB transfer	2 GB / 2 CPUs 60 GB SSD Disk 3 TB transfer	4 GB / 2 CPUs 80 GB SSD Disk 4 TB transfer	8 GB / 4 CPUs 160 GB SSD Disk 5 TB transfer

Now in the authentication method I prefer password but again its your own choice.


Choose Authentication Method ?

○ SSH Key Connect to your Droplet with an SSH key pair
● Password Connect to your Droplet as the "root" user via password

Create root password *



PASSWORD REQUIREMENTS

- Must be at least 8 characters long
- Must contain 1 uppercase letter (cannot be first or last character)
- Must contain 1 number
- Cannot end in a number or special character

⚠ Please store your password securely. You will not be sent an email containing the Droplet's details or password.

Now you can create a password and make sure to remember it!

After finishing you can click the create droplet button to create your own box!

Once it’s Done, you would see your box’s IP on the dashboard.

Connect to your VPS

To connect to your VPS, you can access via SSH. If you are using Mac or Unix-like system, just simply put in below command

```
ssh root@<your-vps-ip>
```

If you are using Windows, you might need to download putty to access via SSH.

After logging in, I advice to create a new user so that you don’t have to run everything as root.

How to utilize it in Bug Bounties?

You can use the screen command to keep the processes running even when your system is not turned on.

`screen` is a terminal multiplexer utility in Linux that allows you to create and manage multiple terminal sessions within a single terminal window or SSH session. It's particularly useful when working remotely, managing long-running processes, or handling multiple tasks simultaneously.

```
sudo apt-get install screen
```

To create a new screen:

```
screen -S new-screen-name
```

Then You can run the tool you want and exit the screen, the tool will keep running .

To join the screen:

```
screen -r name
```

To list all the screens:

```
screen -ls
```

To exit a screen use ctrl + A + D

Conclusion

In the world of bug bounty hunting, efficiency and automation are key to success. With the power of Virtual Private Servers (VPS), the journey becomes not only streamlined but also highly productive.VPS offers the freedom to run your bug bounty tools and scripts around the clock, increasing your chances of discovering vulnerabilities and securing those sought-after rewards.

That's it for this blog, if you want to know how to create a notification system with this so that you get the notifications of the automation in your mobile do let me know.

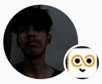
Please Consider following and liking.

You can also support me through:

https://www.buymeacoffee.com/omarora160w

Bug Bounty · Money · Hacking · Infosec · Cybersecurity

225 · 1



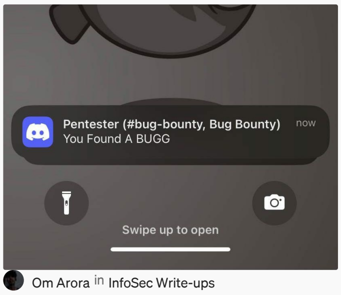
Written by Om Arora

Follow

382 Followers · Writer for InfoSec Write-ups

A 18yo Cyber Security Enthusiast currently pursuing Btech Cse 2nd year. linktr.ee/om1603

More from Om Arora and InfoSec Write-ups



Pentester (#bug-bounty, Bug Bounty) now
You Found A BUGG

Swipe up to open

Om Arora in InfoSec Write-ups

Find Bugs While Sleeping ? Get Phone Notifications When A Bug I...

Hello Everyone!

4 min read · Sep 16

302

iam_with_you11 in InfoSec Write-ups

Instagram Password Hacking

Hii Amigos in todays article we were going to learn how to hack Instagram passwords by...

2 min read · Feb 23

716 · 16

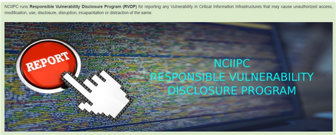
Rajneesh Kumar Arya in InfoSec Write-ups

How FBI hackers or Forensics Team identify fake Images

Hello learners, I am back with my new and very interesting blog on how the FBI or any...

5 min read · Jul 15

506 · 4



Om Arora in InfoSec Write-ups

How I Found My First 3 Bugs Within An Hour

Hey Everyone, Welcome to my Blog, Today I am going to discuss about how I found my fir...

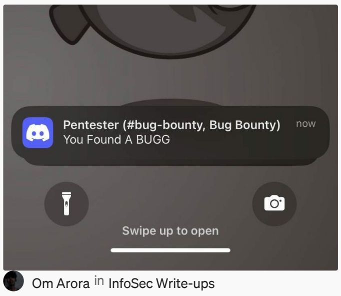
4 min read · Jul 27

458 · 4

See all from Om Arora

See all from InfoSec Write-ups

Recommended from Medium



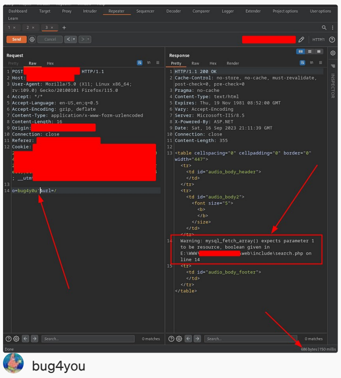
Om Arora in InfoSec Write-ups

Find Bugs While Sleeping ? Get Phone Notifications When A Bug I...

Hello Everyone!

4 min read · Sep 16

302



bug4you

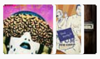
How I Got 4 SQLI Vulnerabilities At One Target Manually Using The...

Hi everyone, I'm Youssef, A Junior Computer Science Student, and Cyber Security...

18 min read · Sep 19

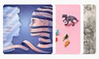
1K 14

Lists



Modern Marketing

34 stories · 186 saves



Some of My Favorite Personal Essays

18 stories · 383 saves

Self-Improvement 101

20 stories · 720 saves

Business 101

25 stories · 402 saves

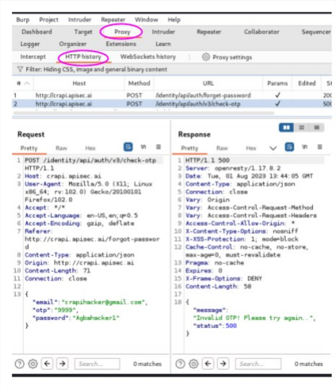
Takshal(tojojo)

How I Discovered Over 40+ Impactful Vulnerabilities Within 1...

Hello, I'm Takshal, aka tojojo. I hope you all are doing well. Today, I'm excited to share my...

3 min read · Aug 13

508 9



Isu Momodu Abdulrauf

Fuzzing APIs

Fuzzing or Fuzz testing is an automated testing method where random, invalid,...

8 min read · Sep 10

129

Parkerzanta

Earn Money with Fun! Find Vulnerability in Random Sites

This article I will tell you about how I make money from sites that do not have a Bug...

5 min read · 6 days ago

157 1

Shrirang Diwakar

Bypassing 403s like a PRO! ($2,100): Broken Access control

This article highlights my way of dealing with 403s and how I managed to get a P1 in...

3 min read · Apr 21

1.1K 8

See more recommendations