

Find Bugs While Sleeping ? Get Phone Notifications When A Bug Is Found

Hello Everyone!



Om Arora · Follow

Published in InfoSec Write-ups · 4 min read · Sep 16



302



In the last blog I posted about the free VPS setup and got amazing response.

So in this Blog I am going to show you how to get notifications on your phone while your scripts are running on the VPS, so you don't miss any updates.

For Example:

Suppose you have a script like this:

```
GNU nano 7.2 task1.sh
#!/bin/bash

# Notify when the task starts
echo "Task Starting" | notify --silent

# Define variables and perform calculations
a=4
b=6
c=$((a * b))

# Notify the result
printf "Total sum of a + b = %c\n" | notify --silent

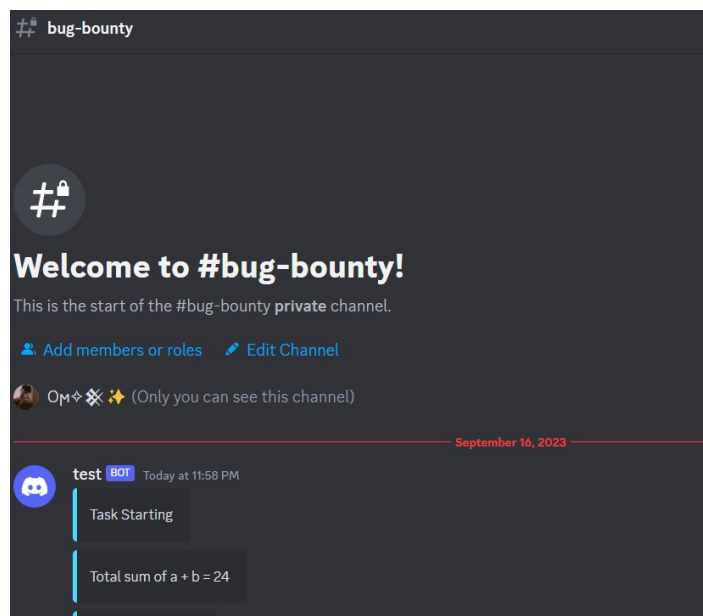
# Notify when the task finishes
echo "Finished the task" | notify --silent
```

Now we run this script on the VPS

```
./task1.sh
```

```
Task Starting
Total sum of a + b = 24
Finished the task
```

Now you will receive a notification on your discord as per your script as you can see:

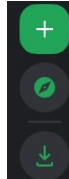


Now we are going to learn how to do this

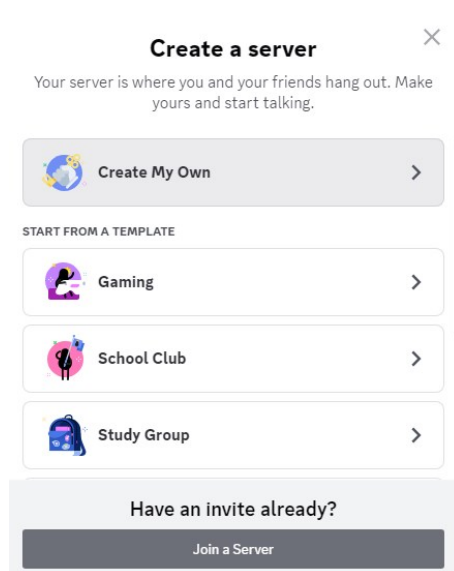
So Lets Get Started!!



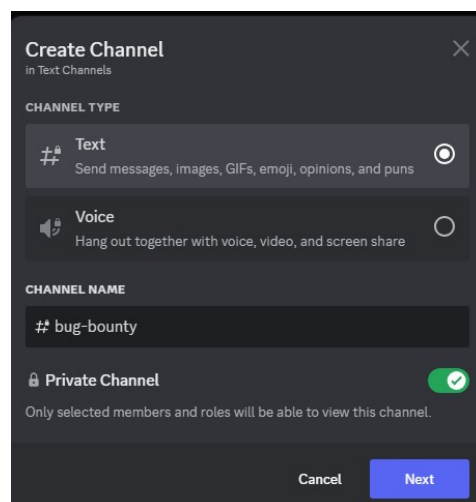
First Create a discord server:



Click on Create My Own



Now add a text channel to your server and make it a private channel



Now Click on Edit channel

Which can be created at \$HOME/.config/notify/provider-config.yaml

With the following content

You can comment out everything except the discord part

```
#slack:
# - id: "slack"
#   slack_channel: "recon"
#   slack_username: "test"
#   slack_format: "{{data}}"
#   slack_webhook_url: "https://hooks.slack.com/services/XXXXXX"
#
# - id: "vulns"
#   slack_channel: "vulns"
#   slack_username: "test"
#   slack_format: "{{data}}"
#   slack_webhook_url: "https://hooks.slack.com/services/XXXXXX"

discord:
- id: "crawl"
  discord_channel: "crawl"
  discord_username: "test"
  discord_format: "{{data}}"
  discord_webhook_url: "https://discord.com/api/webhooks/XXXXXXX"

# - id: "subs"
#   discord_channel: "subs"
#   discord_username: "test"
#   discord_format: "{{data}}"
#   discord_webhook_url: "https://discord.com/api/webhooks/XXXXXXX"

#telegram:
# - id: "tel"
#   telegram_api_key: "XXXXXXXXXXXX"
#   telegram_chat_id: "XXXXXX"
#   telegram_format: "{{data}}"
#   telegram_parsemode: "Markdown" # None/Markdown/MarkdownV2/HTML (https://core.telegram.org/bots/api#formatting-options)

#pushover:
#- id: "push"
#   pushover_user_key: "XXXX"
#   pushover_api_token: "YYYY"
#   pushover_format: "{{data}}"
#   pushover_devices:
#     - "iphone"

#smtp:
#- id: email
#   smtp_server: mail.example.com
#   smtp_username: test@example.com
#   smtp_password: password
#   from_address: from@email.com
#   smtp_cc:
#     - to@email.com
#   smtp_format: "{{data}}"
#   subject: "Email subject"
#   smtp_html: false
#   smtp_disable_starttls: false

#googlechat:
# - id: "gc"
#   key: "XXXXXXXXXX"
#   token: "XXXXXX"
#   space: "XXXXXX"
#   google_chat_format: "{{data}}"

#teams:
# - id: "recon"
#   teams_webhook_url: "https://<domain>.webhook.office.com/webhookb2/xx/xx/IncomingWebhook/xx"
#   teams_format: "{{data}}"

#custom:
# - id: webhook
#   custom_webhook_url: http://host/api/webhook
#   custom_method: GET
#   custom_format: '{{data}}'
#   custom_headers:
#     Content-Type: application/json
#     X-API-Key: XXXXX
#
#custom:
# - id: webhookJson
#   custom_webhook_url: http://host/api/webhook
#   custom_headers:
#     Content-Type: application/json
#     X-API-Key: XXXXX

#custom:
# - id: webhook
#   custom_webhook_url: http://host/api/webhook
#   custom_method: GET
#   custom_sprig: '{"text": "{{ .url }}"}'
#   custom_headers:
#     Content-Type: application/json
#     X-API-Key: XXXXX
```

Now you can paste your webhook URL here

```
14 discord:
15 - id: "crawl"
16   discord_channel: "crawl"
17   discord_username: "test"
18   discord_format: "{{data}}"
```

And You're Done!!

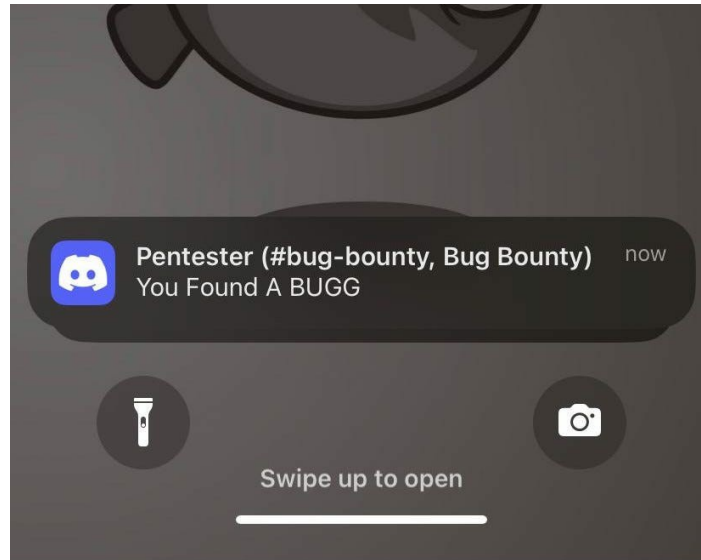
To make it work you just need to add:-

```
notify --silent
```

For Example-

```
echo "You Found A BUGG" | notify --silent
```

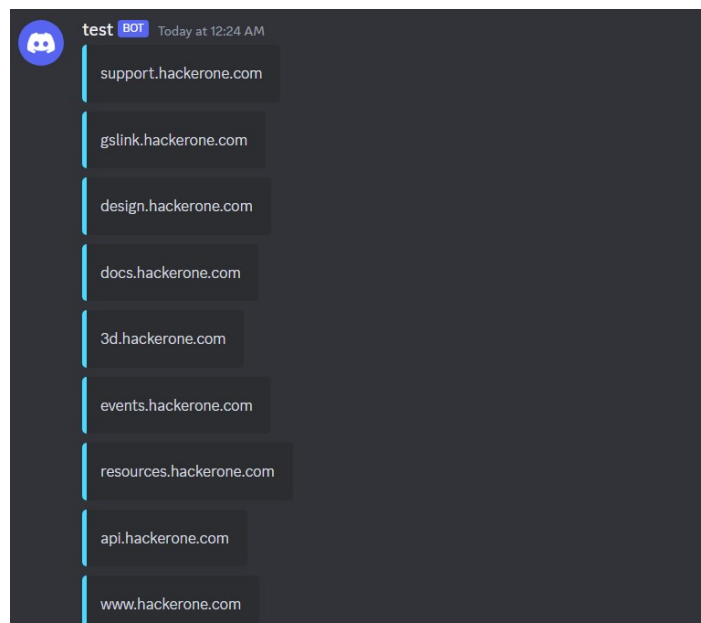
You can see I got the notification



Another Example:

```
subfinder -d hackerone.com | notify
```

On running this command:



We get the results!!

We can also use this tool for many other platforms like

- Slack / Discord / Telegram

- Pushover / Email
- Microsoft Teams / Google Chat

Here are some references for that:


- <https://slack.com/intl/en-it/help/articles/115005265063-Incoming-webhooks-for-Slack>
- <https://core.telegram.org/bots#3-how-do-i-create-a-bot>

Thank you for reading till the end

Please Consider following and liking.

You can also support me through:

Om Arora
I love supporting creators!
www.buymeacoffee.com



Bug Bounty


Bug Bounty Tips

Infosec

Hacking

Automation

302




Written by Om Arora

Follow

383 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



Om Arora

in InfoSec Write-ups

Bug Hunting on Autopilot, Free VPS Setup

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

4 min read · Aug 19

225

1



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



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...

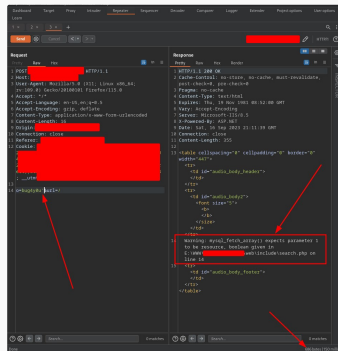
4 min read · Jul 27

458

4

[See all from Om Arora](#)[See all from InfoSec Write-ups](#)

Recommended from Medium

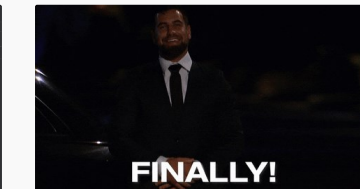
[bug4you](#)

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

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

18 min read · Sep 19

1K 14

[whit3r0s3](#) in InfoSec Write-ups

My debut with a Critical Bug: How I found my first bug (API...)

Finally, the day arrived when I could share my own findings, rather than just reading other...

4 min read · Sep 7

451 4

Lists



Coding & Development

11 stories · 216 saves



The New Chatbots: ChatGPT, Bard, and Beyond

13 stories · 142 saves



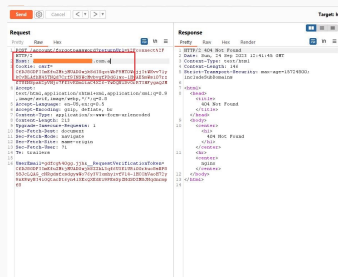
New_Reading_List

174 stories · 149 saves



Medium Publications Accepting Story Submissions

154 stories · 825 saves

[Salman Khan](#)

\$1,250 worth of Host Header Injection

What is Host Header Injection?

4 min read · Sep 24

713 9

[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

[Shrirang Diwakar](#)

API Information Disclosure Leading to Admin Account...

Hi everyone! In this project, my primary responsibility was to identify vulnerabilities i...

2 min read · Sep 18

 211  1

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