**ETHICAL HACKING**

****

**UNIVERSITY OF MUMBAI**

PROJECT ENTITLED

**“Cross Site Scripting (Location Tracking)”**

SUBMITTED BY

Mr. Ronak Patra

ROLL NO

8284

UNDER GUIDANCE OF

***Prof. Simran Shinde***

SUBMITTED FOR THE FULFILLMENT OF THE CURRICULUM OF DEGREE

OF BACHELOR OF SCIENCE

IN COMPUTER SCIENCE

**PILLAI COLLEGE OF ARTS, COMMERCE &**

**SCIENCE, NEW PANVEL**

**2022-2023**

**Certificate**

This is to certify that Mr. Ronak Patra of **T.Y B.Sc. C.S. Semester VI** has completed the project work in the Subject of Ethical Hacking during the academic year 2022-23 under the guidance of Prof. Simran Shinde being the partial requirement for the fulfillment of the curriculum of **Degree of Bachelor of Science in Computer Science, University of Mumbai.**

**Place:**

**Date:**

Name & Signature of faculty Name & Signature of external

Name & Signature of Co-ordinator

**ACKNOWLEDGEMENT**

**Cross Site Scripting (Location Tracking)** project is created by Ronak Patra student of Pillai College of Arts, Commerce & Science would like to express our sincere gratitude towards the Computer Science Department.

I would like to thank lecturer **Prof. Simran Shinde** and for their constant support during the project. Last but not least we thank all my colleagues for being with me throughout the project, which leads to a successful completion of my project. The project would not have been completed without creativity and energy, which our friends provided.

Yours faithfully,

Ronak Patra

**INDEX**

## **SR.NO TOPIC SIGN**

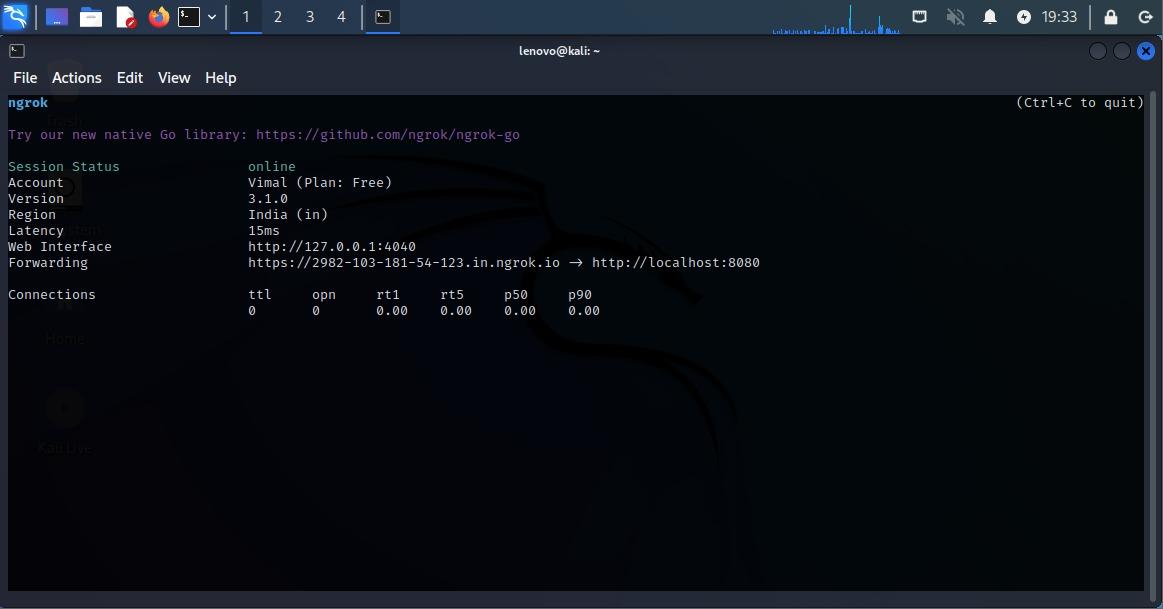
| 1. | Project Overview |
| --- | --- |
| 2. | Server Connection |
| 3. | Location Tracking using NearYou |
| 4. | Location Tracking using Google Drive |
| 5. | Location Tracking using Whatsapp |
| 6. | Location Tracking using Zoom |
| 7. | Location Tracking using Telegram |

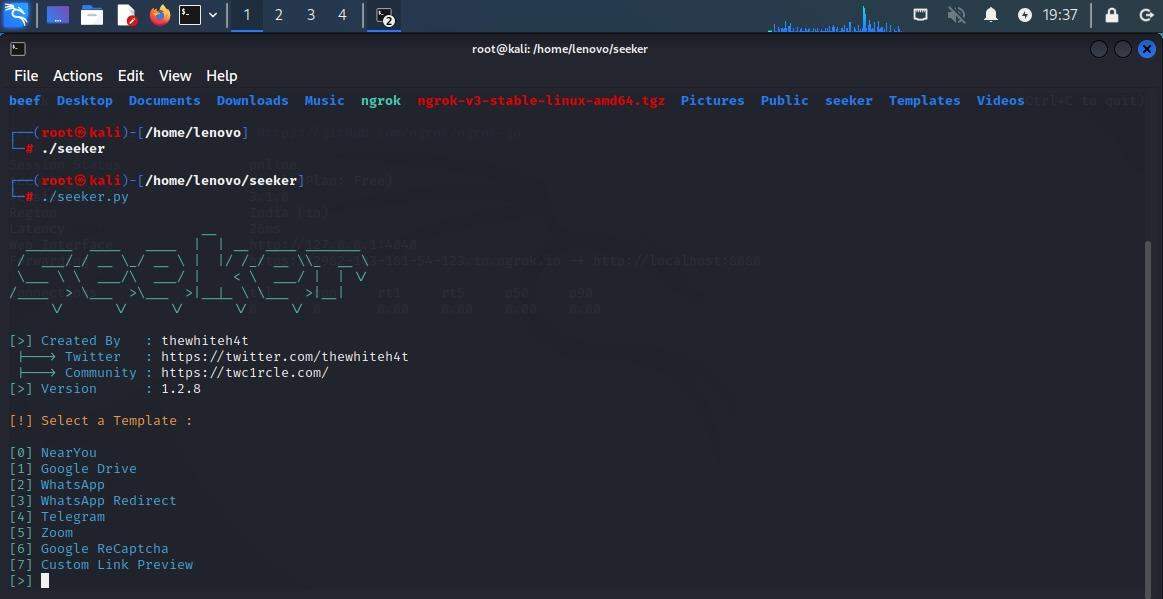
Project Overview:

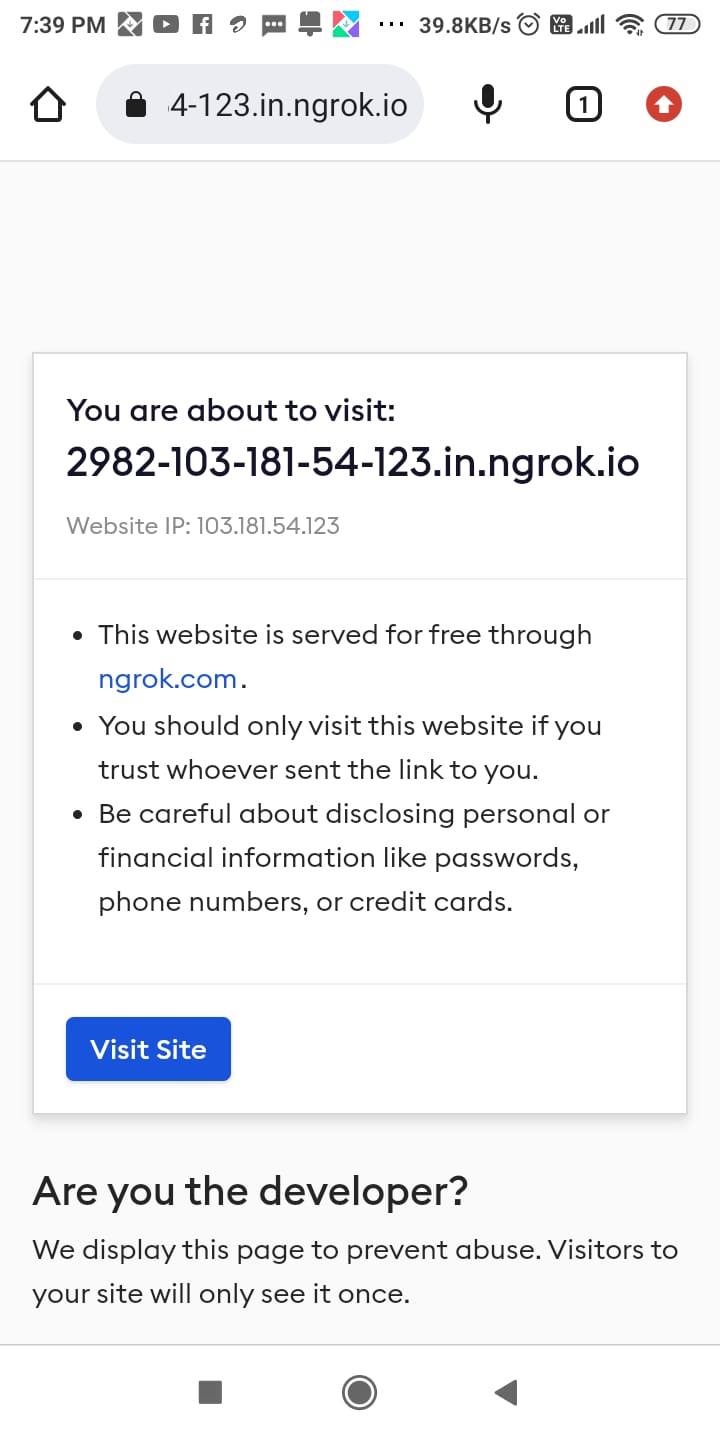
Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

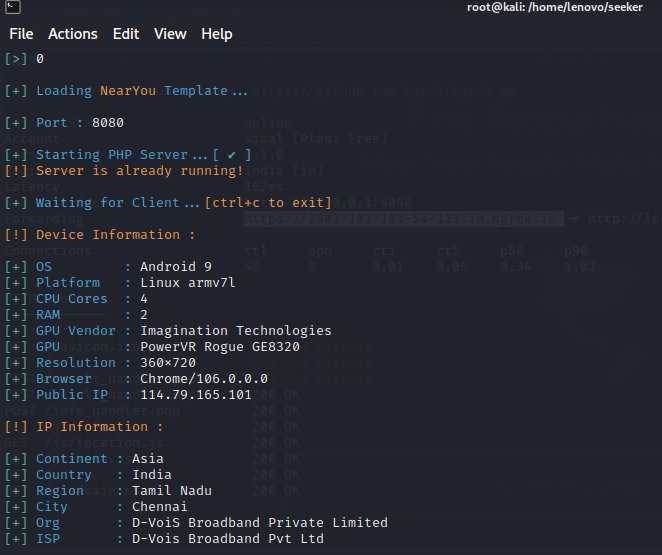
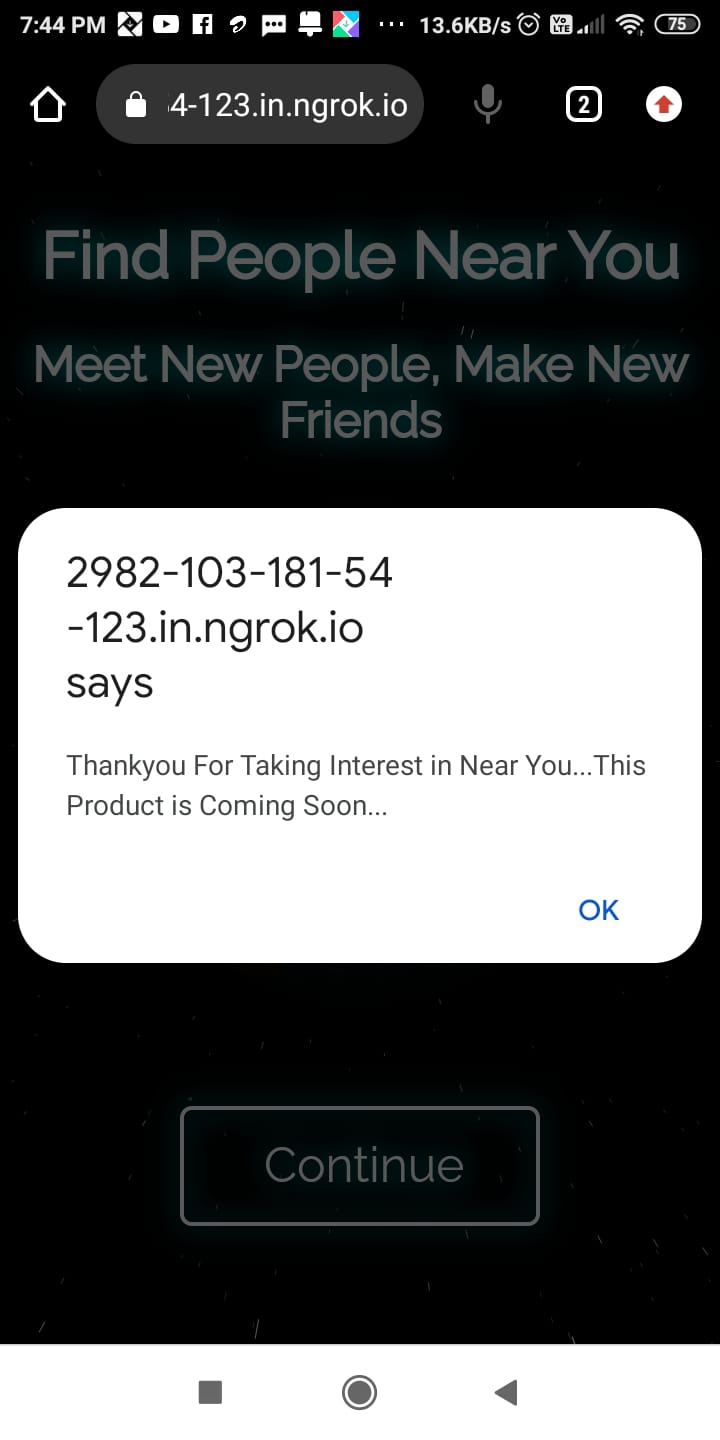
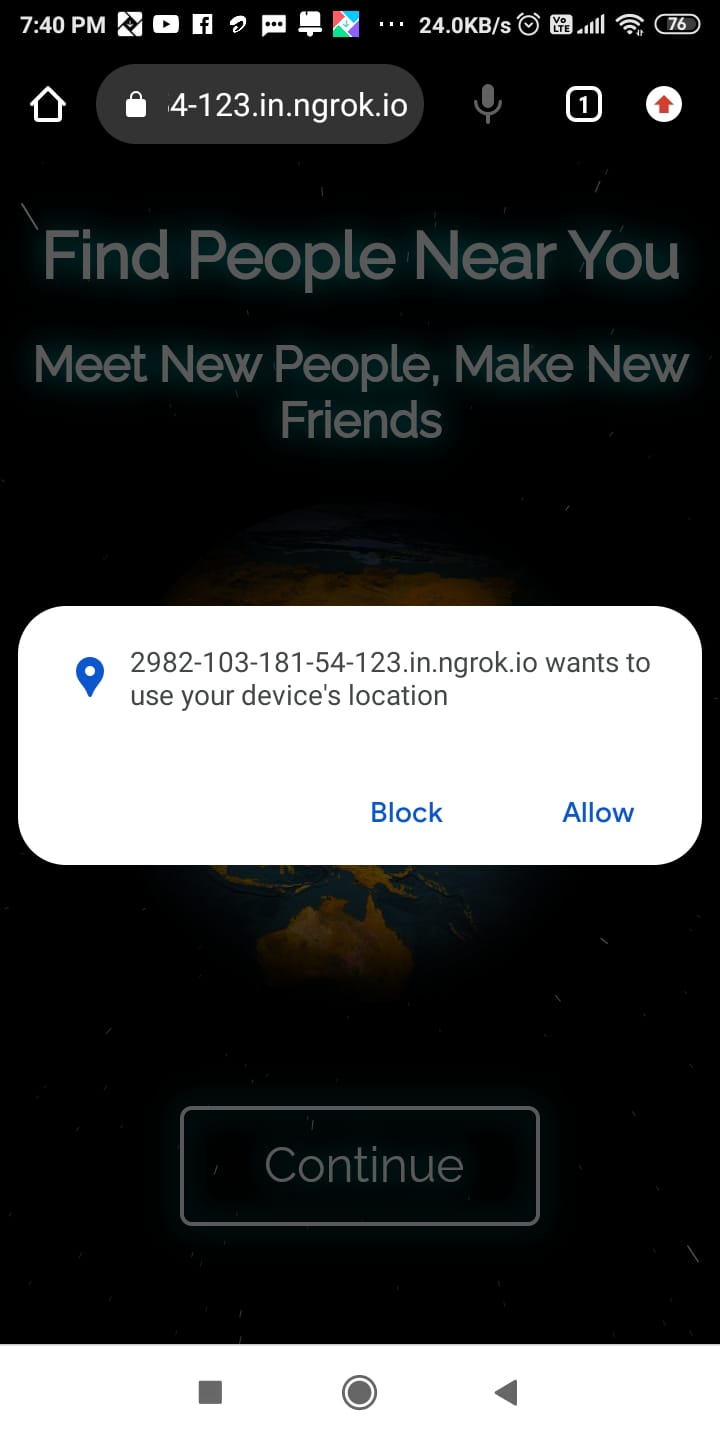
An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

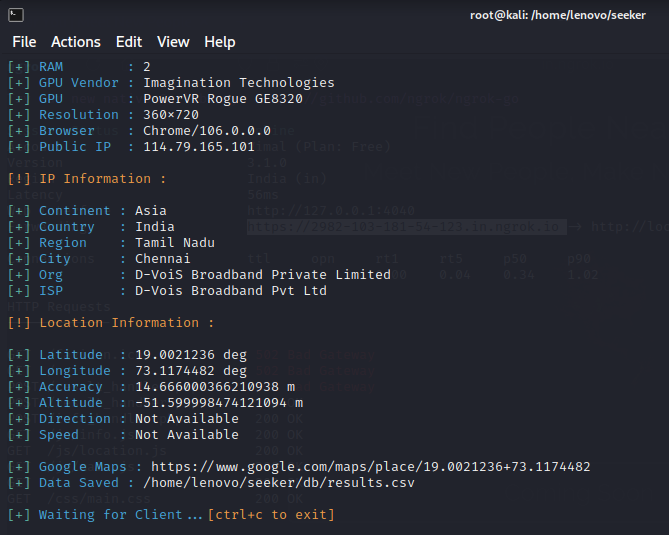
**NearYou:**

****

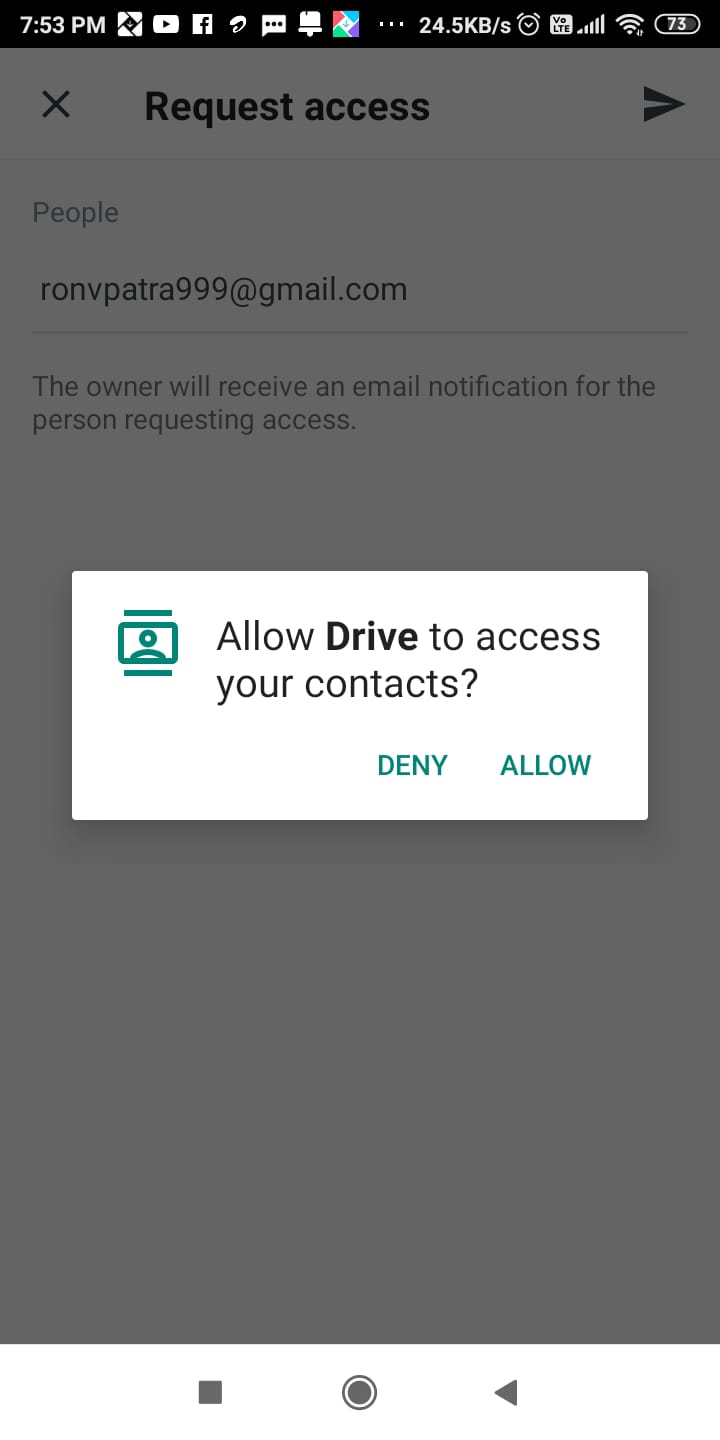
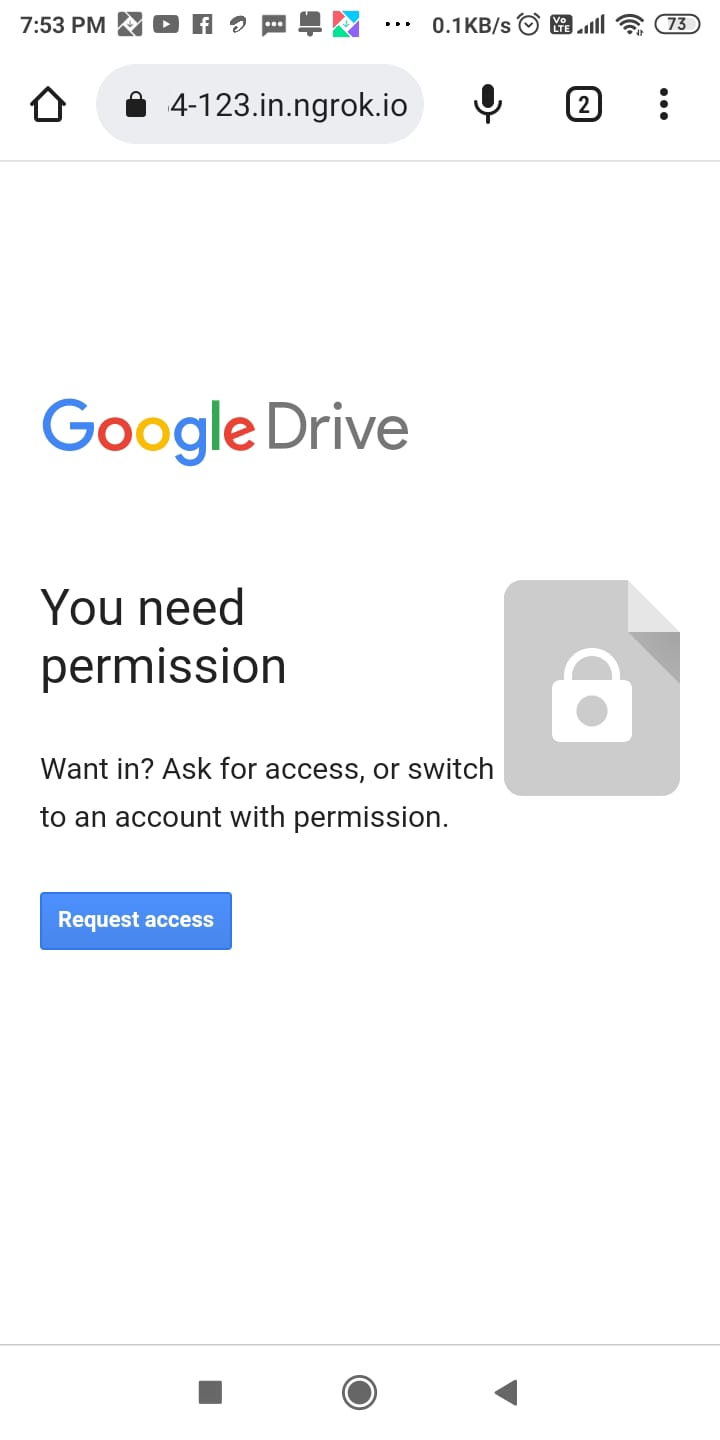
****

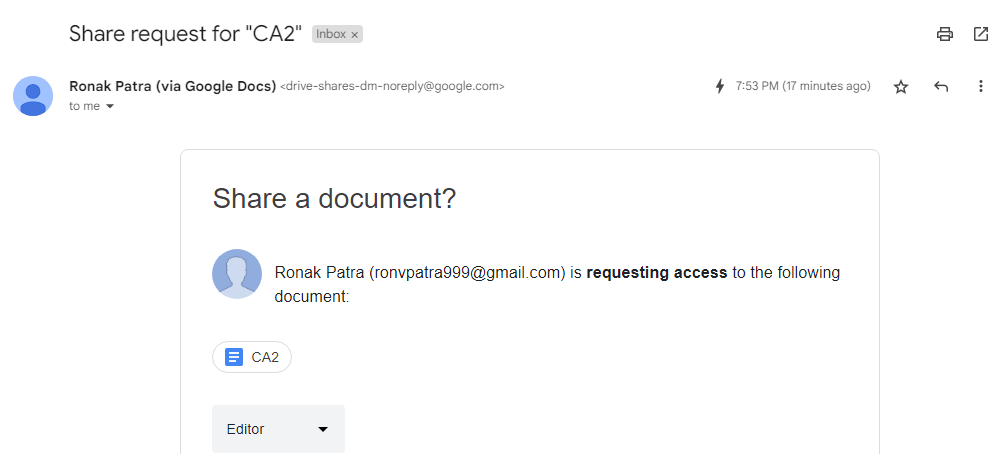
****

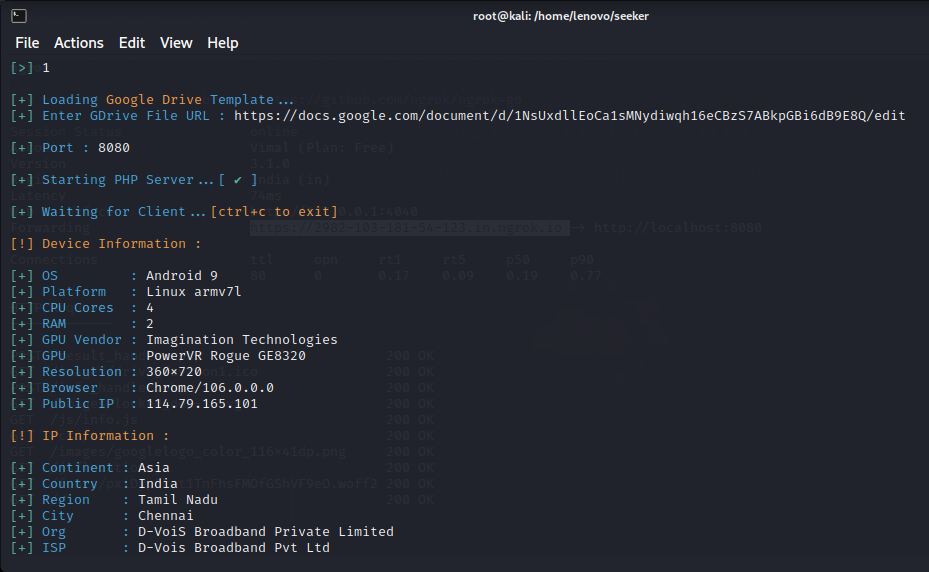
****

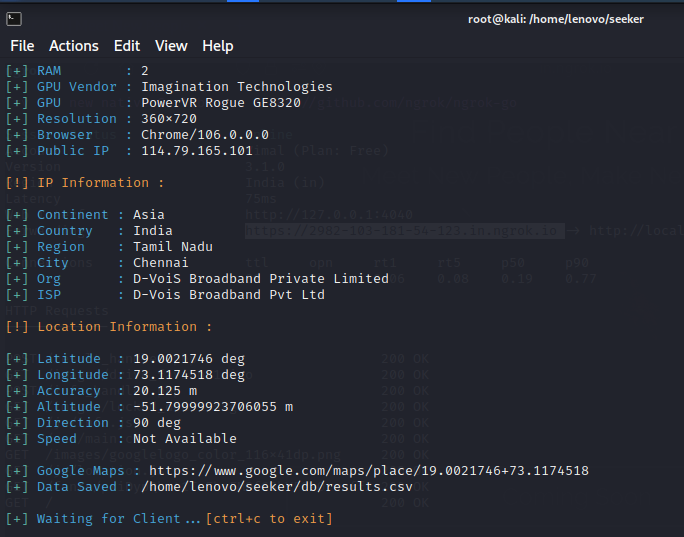
****

**Google Drive:**

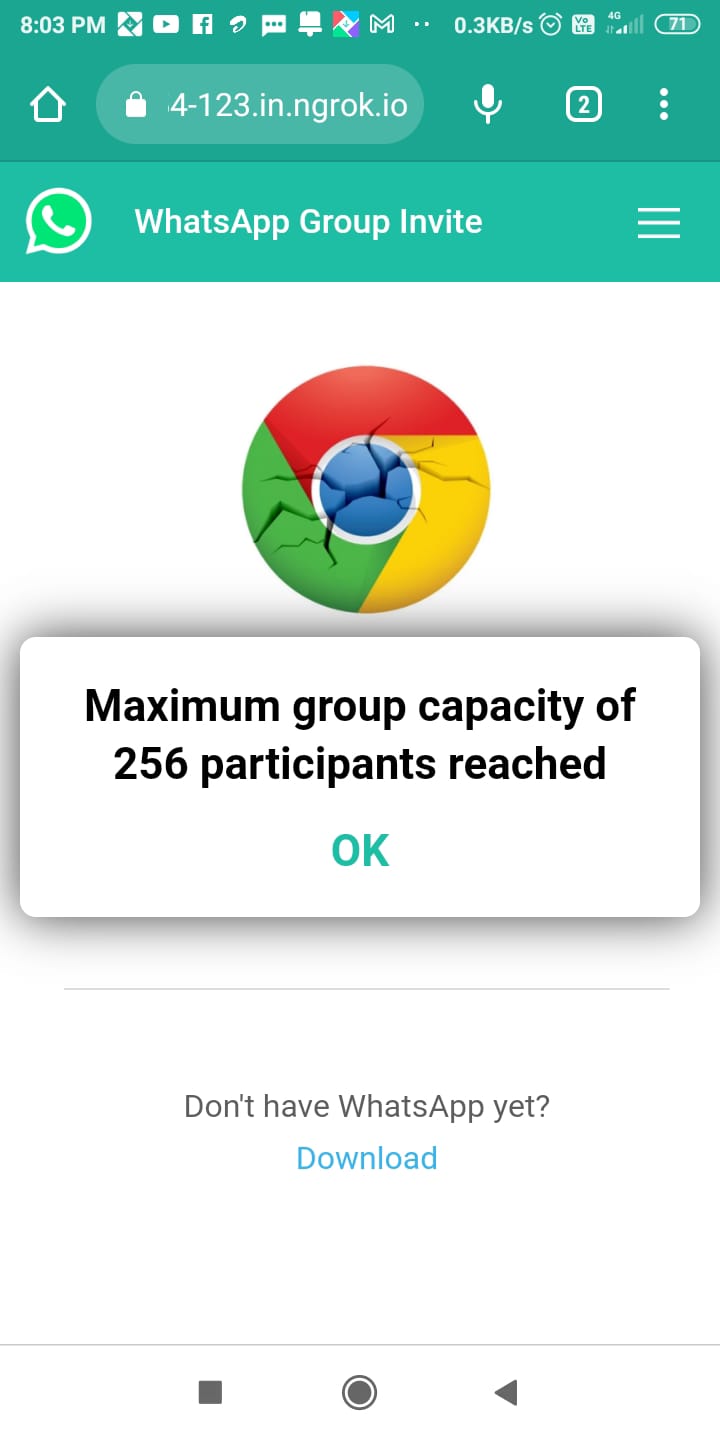
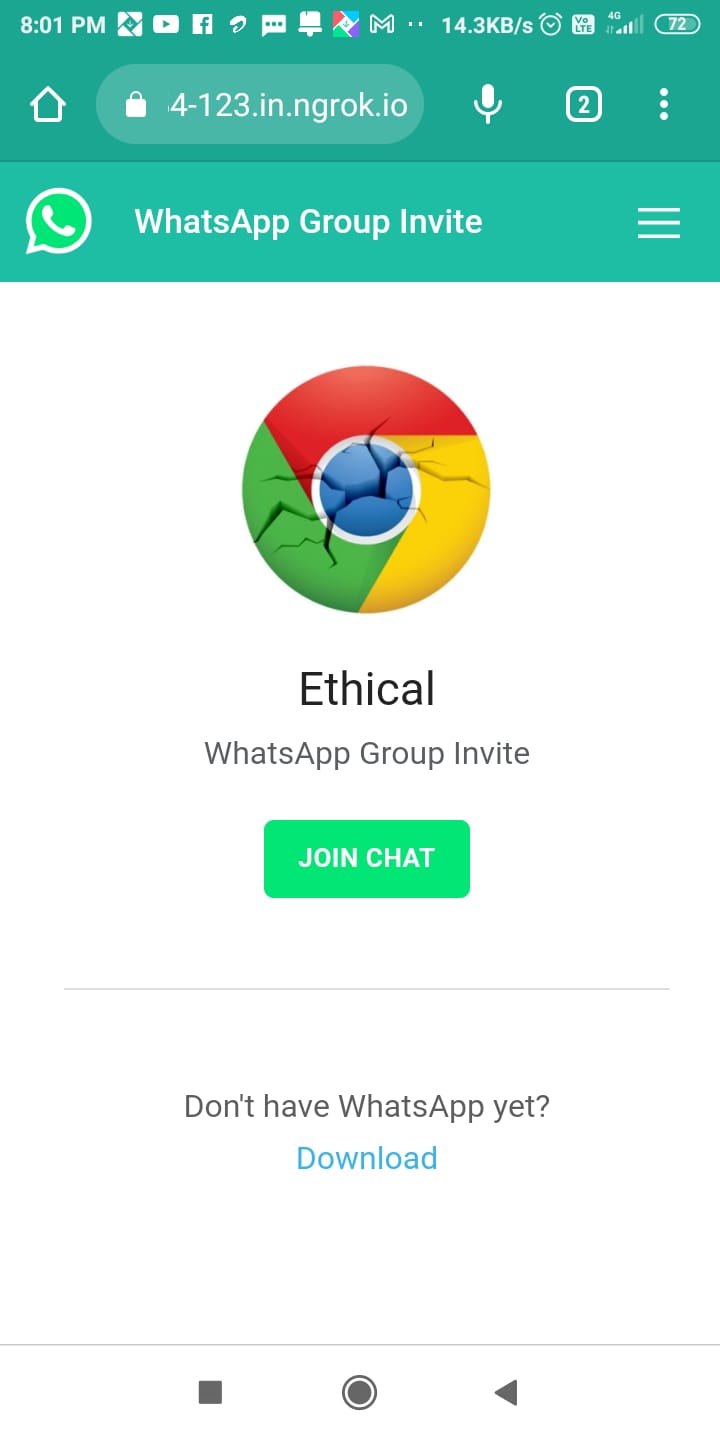
****

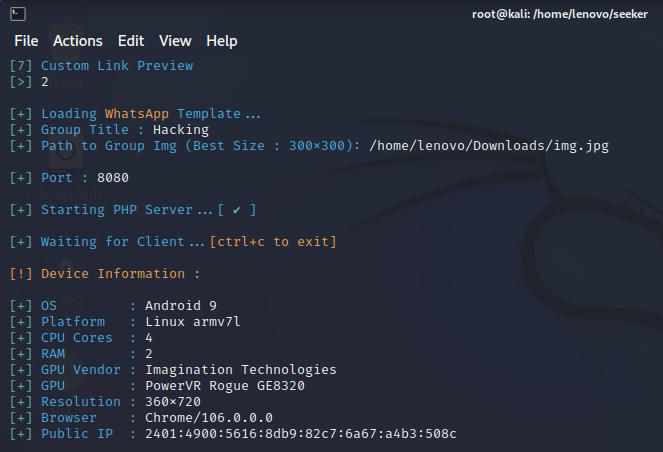
****

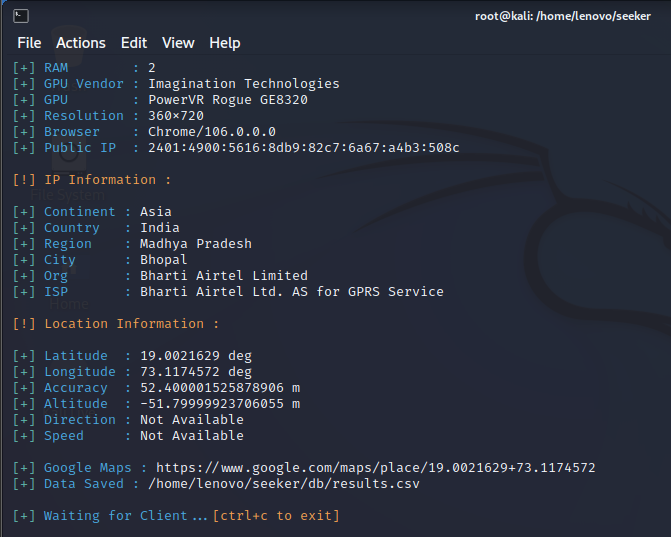
****

****

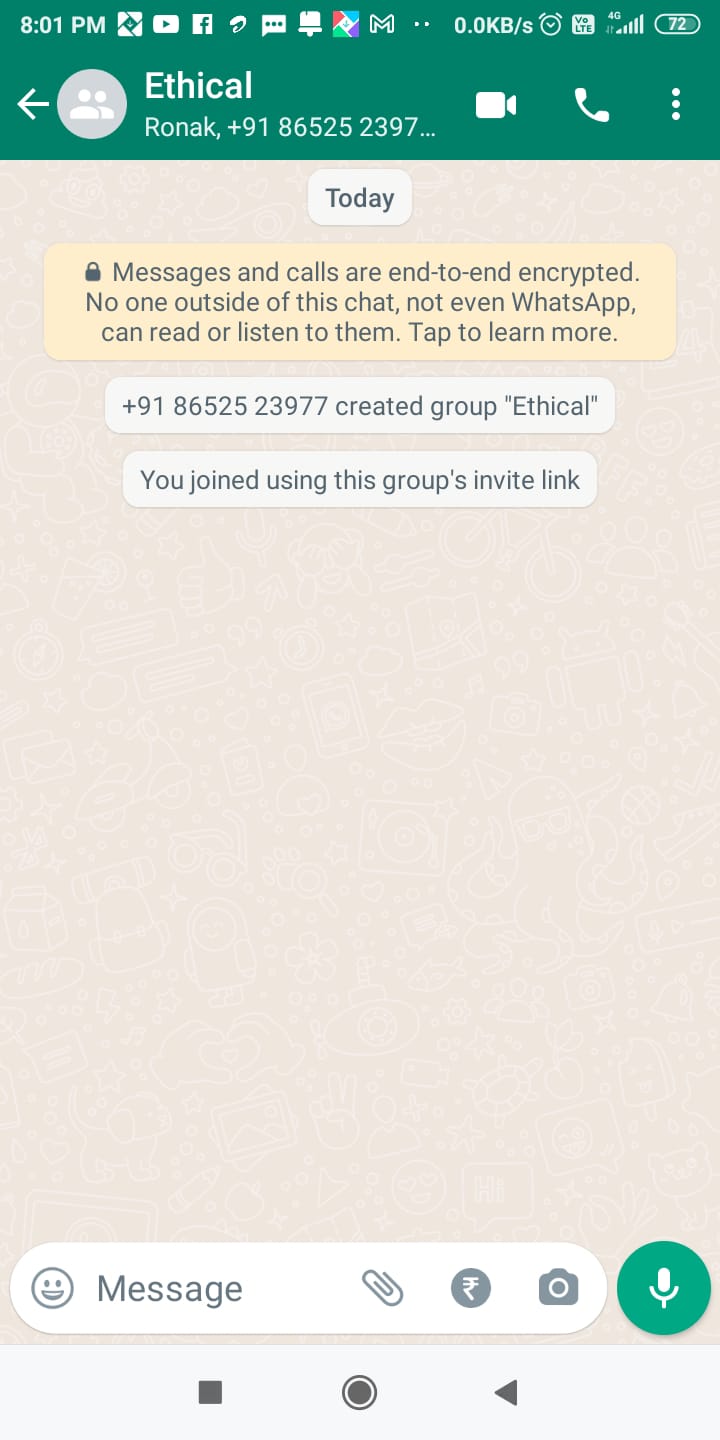
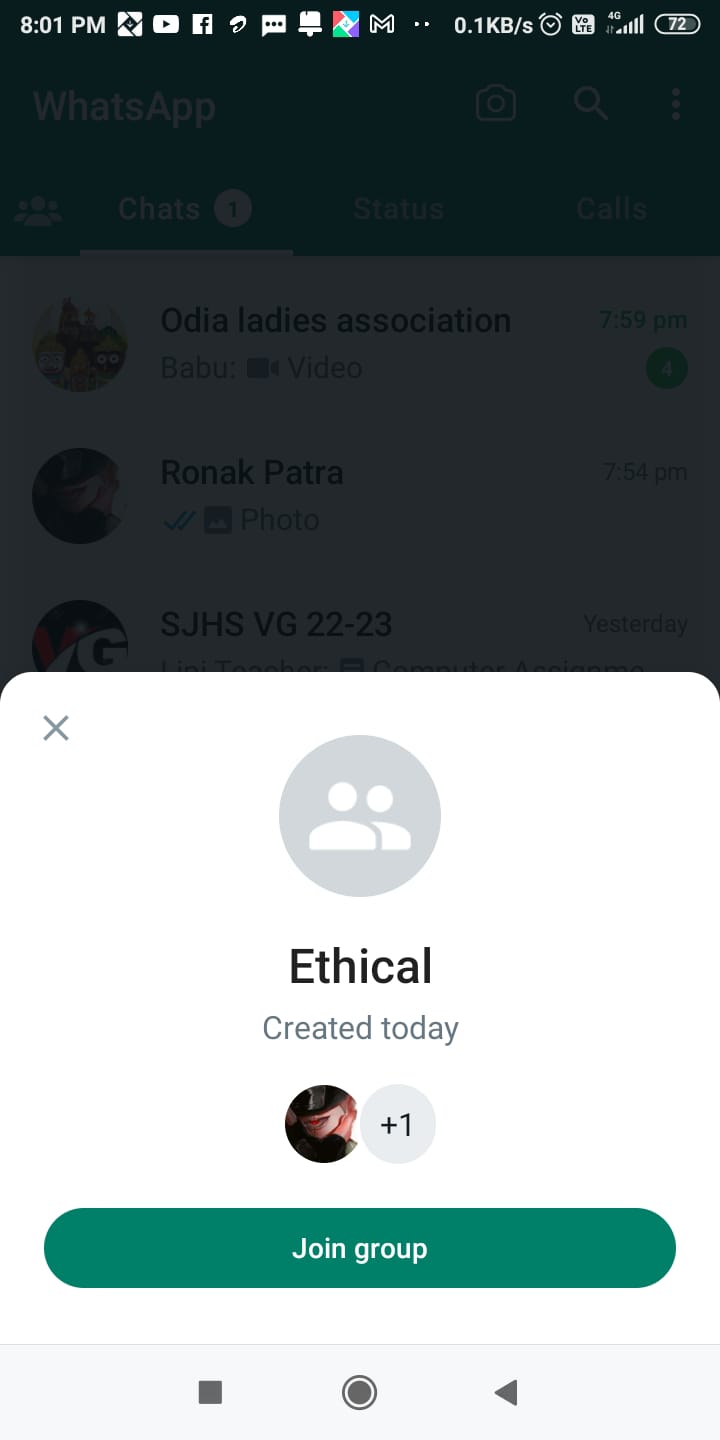
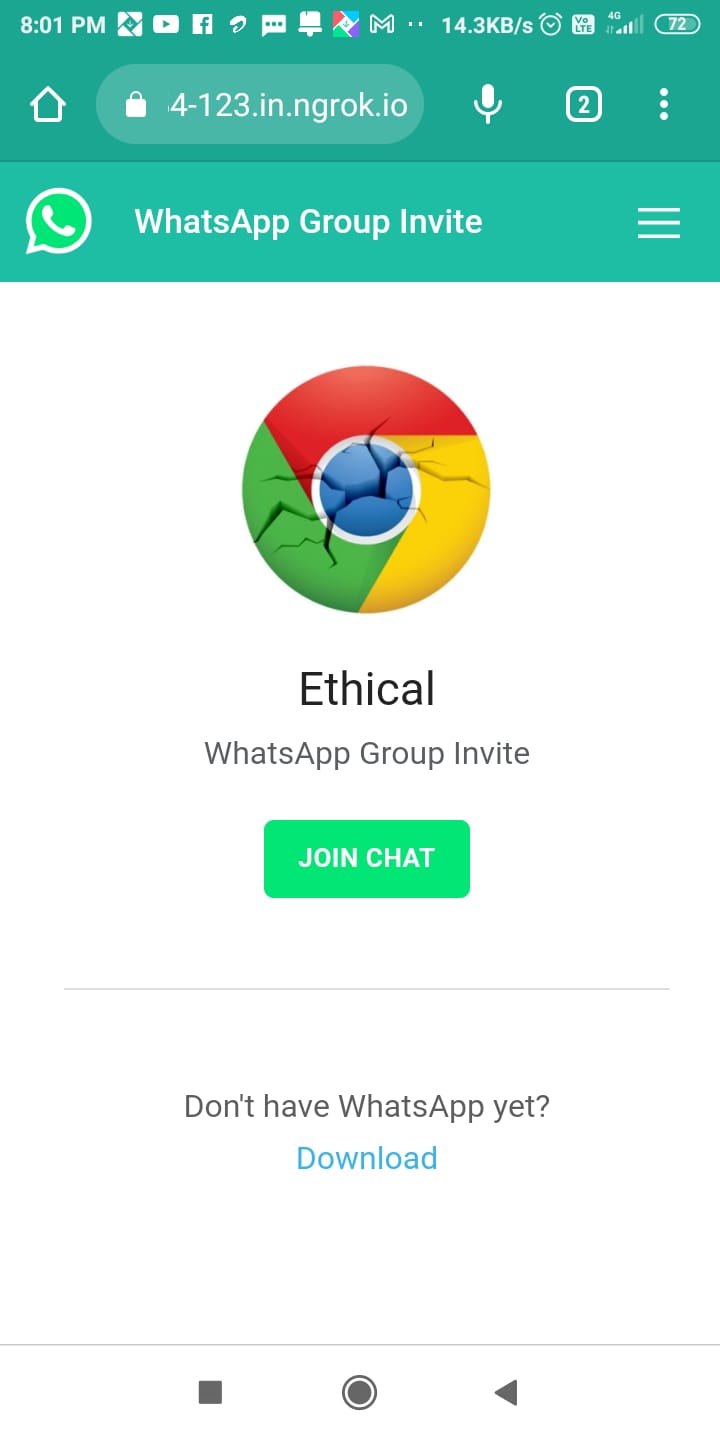
**Whatsapp:**

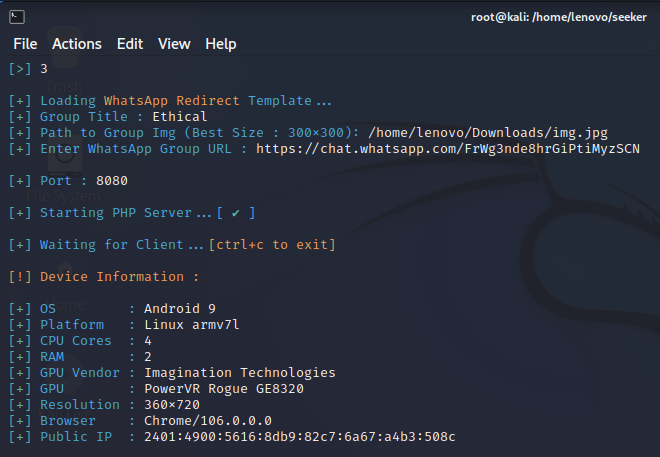
****

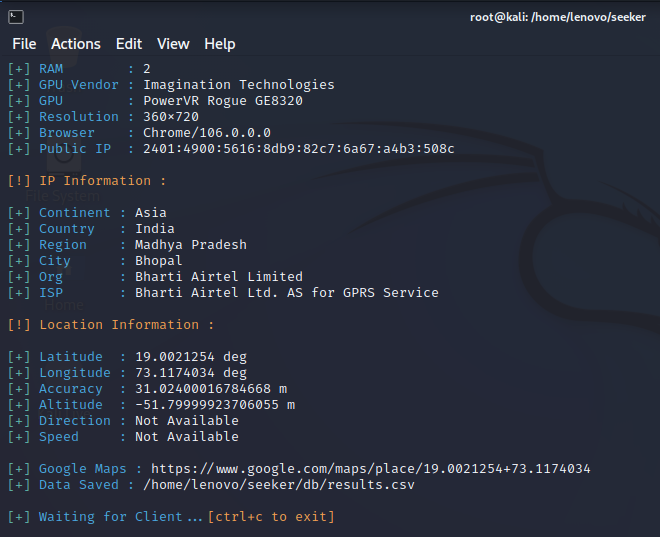
****

****

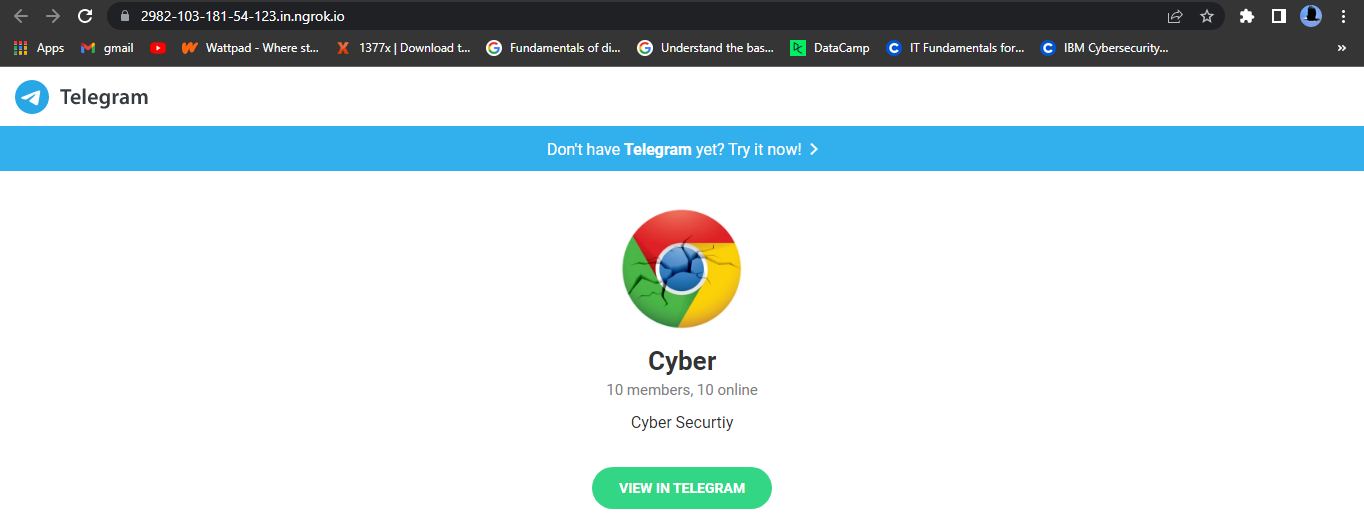
**Whatsapp Redirect:**

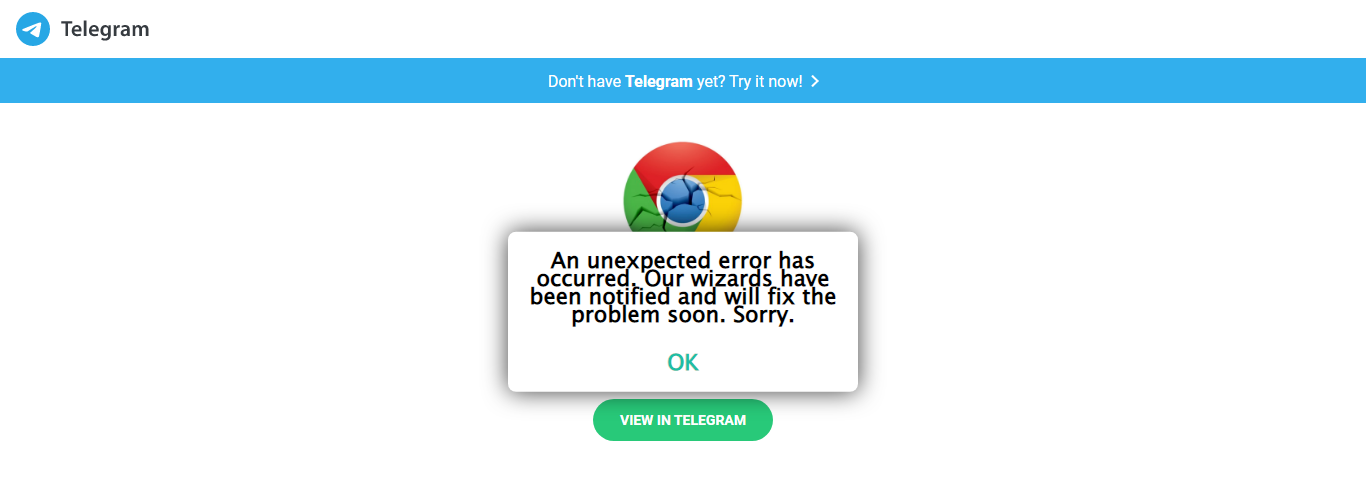
****

****

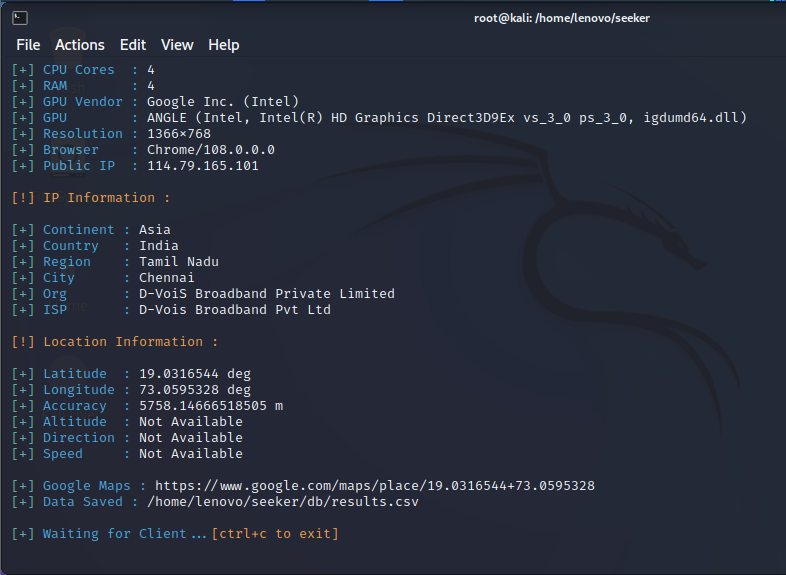
****

**Telegram:**

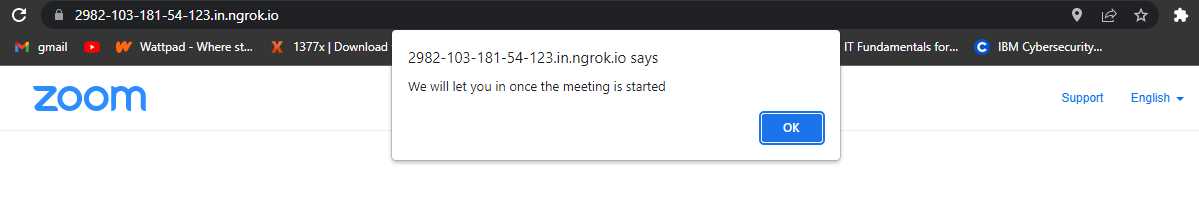
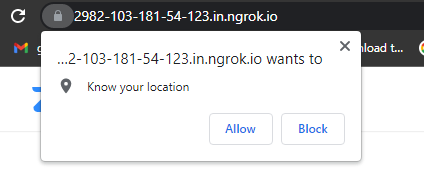
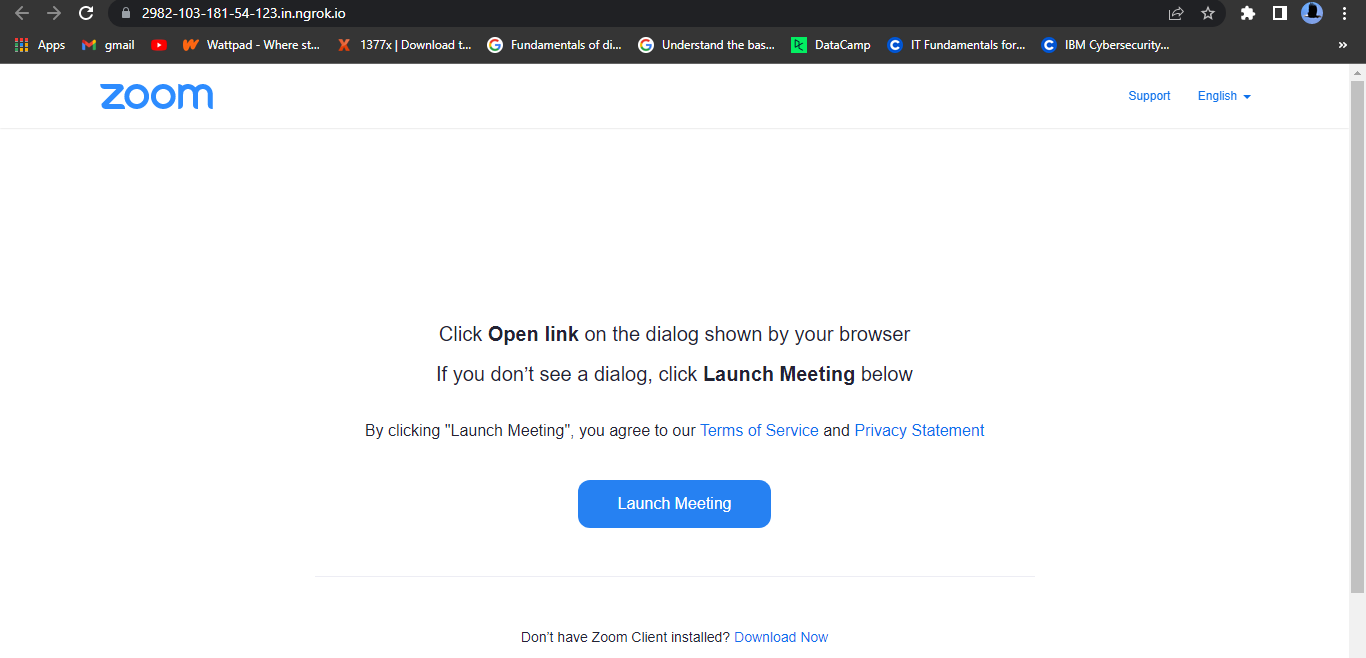
****

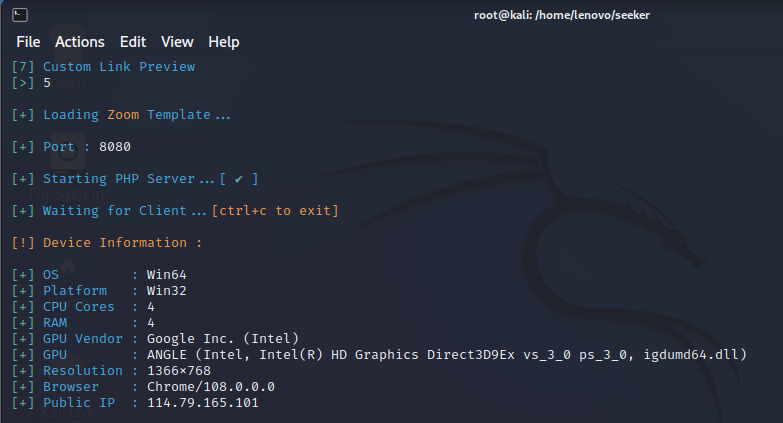
****

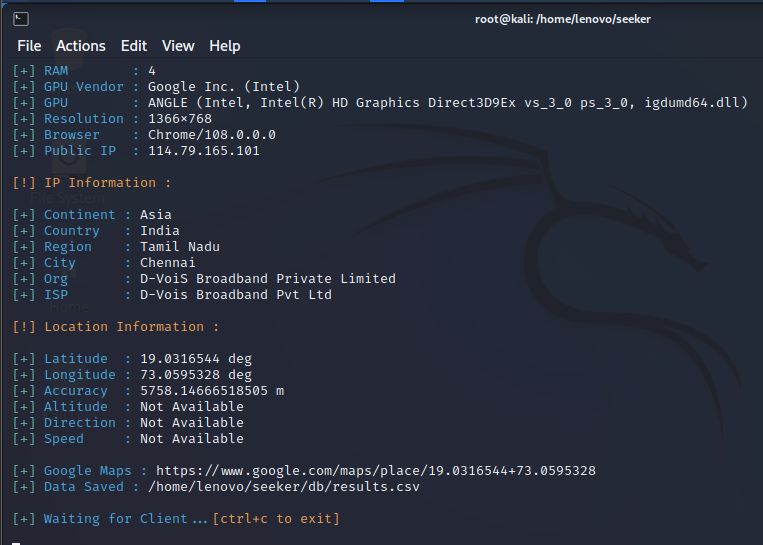
****

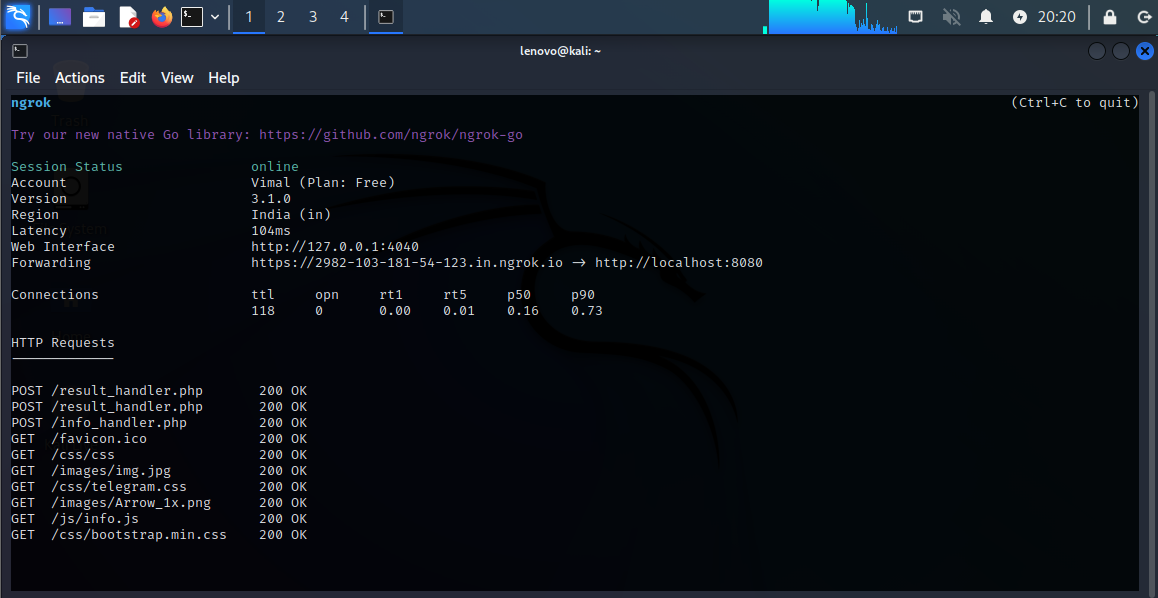
****

**Zoom:**

****

****

****

****