



# Sabyasachi Paul

Cybersecurity Engineer

[linkedin.com/in/h0tplug1n](https://www.linkedin.com/in/h0tplug1n)

[sabya.sachi.paul02@gmail.com](mailto:sabya.sachi.paul02@gmail.com)

[github.com/h0tPlug1n](https://github.com/h0tPlug1n)

[h0tplug1n.medium.com](https://h0tplug1n.medium.com)



A dedicated Cybersecurity practitioner and Forensics enthusiast flexible in adapting new technologies. Having a background in Web penetration testing, but also knowledgeable about Android Penetration Testing, Networking, and Robotics. Alongside I am a content creator on Youtube channel regarding information security and programming.

## Experience

**Penetration Testing Intern** Oct'21-Dec'21  
Virtually Testing Foundation

- Learned 10 web vulnerabilities like XSS, SQLi etc.
- Solved multiple challenges based on the bugs

**Cybersecurity Content Creator** May'21-Present  
YouTube

- Creating content on CTF, pentesting & programming
- Android Pentesting Course - 2.6K Views

**Web Developer** Jun'20-Aug'21  
Divaks Total IT Solution

- Developed 10+ websites mostly using WordPress
- Took 5+ Technical Interviews

## Publications

**GHDB-ID: 7802**

Url: <https://www.exploit-db.com/ghdb/7802>

Desc: Useful in getting juicy details about websites and their internal directory structure.

**GHDB-ID: 7799**

Url: <https://www.exploit-db.com/ghdb/7799>

Desc: Useful in fetching some sensitive config files and logs written in PHP. This might also result in SDE (Sensitive Data Exposure). The file might also contain juicy details.

**GHDB-ID: 7693**

Url: <https://www.exploit-db.com/ghdb/7693>

Desc: Useful for listing out login portals in government websites to perform attacks like BruteForce, Account Takeover, No RL, Auth Bypass etc.

**GHDB-ID: 7694**

Url: <https://www.exploit-db.com/ghdb/7694>

Desc: Useful for listing out government website's login portal made with CMS Technology - WordPress. These websites might be vulnerable to : RL Bypass, Open Redirect, BruteForce, Account Takeover etc.

## Education

**B.Tech in Computer Science Engineering**

Adamas University

Aug'20-Present

8.46 SGPA (Sem4)

**AISSCE - CBSE 12th Board**

Asansol North Point School

Apr'18-Mar'20

79%

## Technical Skills

### Software/Tools

Nmap, BurpSuite, Wireshark, Metasploit, Gobuster, Sqlmap, Dirb, Hydra, tcpdump, adb, jadx, Android Studio, Postman, FTK Imager, VMWare, VirtualBox

### Skills

Linux, Networking, Web Pentesting, Android Pentesting, Arduino

### Programming

HTML, CSS, JS, Python, Java, Bash, PHP

## Certifications

- Certified Bug Bounty Hunter
- Certified Cybercrime Intervention Officer

## Achievements

**TryHackMe - [0x9 0MN1] Top 2%**

Url: <https://tryhackme.com/p/sabyasachipaul>

Solved 60+ rooms, having 9 badges

Created 1 room - Status on review

### Acknowledgement from NCIIPC

Secured 5+ Govt. Websites

Found bugs like RXSS, NoRL, IDOR, Broken Auth

## Other Interests

Bug Bounty, CTFs, YouTube Content creation, Drumming, Calisthenics & Hitting Gym