# NITHISSH S

**Security Engineer**

No.420, Raja street Kavaraipettai, Gummudipoondi, Chennai, 601206, India

**+91 7010054802** **nithissh@outlook.iin**

Date of birth ..... ***07/08/2000*** Nationality ..... ***Indian***

## LINKS

***Medium, LinkedIn, Github***

## PROFILE

My diverse experience has a security researcher and security engineer has taught me many valuable skills which enables me to be an influential and respected cybersecurity torchbearer. faced with an ever-changing technology landscape , I have the ability to adapt and provide my organization with technology solutions for complex security problems

## EMPLOYMENT HISTORY

### Indepedent Security Researcher, Self-Employed ..... 2018 — 2021

Chennai

- Remote code execution ( Reported and verified by UNESCO, Indian Government and Synack )
- Authenication Bypass ( Reported and verified by ICICI Bank, Accenture, Dutch government )
- Server Side Request Forgery ( Reported and verified by Oneplus and Asus )
- SQL Injection ( Report and verified by Nike , TCL)
- Sensitive/Server Information Disclosure ( Reported and verified by ICICI Bank, Riot Games, TCL )
- Cross-Site Scripting ( Reported and verified by ACT, Shaadi.com, ICIC Bank, Dutch Government, Indian Government, Zoho )
- Business logic errors ( Reported and verified by AEW, TCL, Shopclues, Flipkart )
- XML External Entity ( Reported and verified by Nike, Oneplus )
- Part of Synack Red team ( Security Researcher )
- Host header poising in Engineers Online portal ( CVE-2021-43437 )
- Persistant XSS in iResturant Application ( CVE-2021-43438 )
- Multiple stored XSS in iOrder Application ( CVE-2021-43440 )
- HTML injection in iOrder Application ( CVE-2021-43441 )

### Security Engineer, Tata Elxsi ..... Jul 2021 — Jan 2022

Bengaluru

- Did a source code review for the internal Web framework and fixed few vulnerabilities in the framework
- Performed a Penetration testing on the AWS and found few vulnerabilities and gave the remediation on How to fix it
- As an team we did a research study on the 5G Security and learned alot about 5G Security and Approach methodologies
- Performed a penetration testing on Internal web application and Mobile security testing for OTT Platform
- Working and did a research about the STIG Framework based upon the Firewall, Network, Web servers,etc..

## EDUCATION

### Gurunanak College Velachery ..... Mar 2018 — Present

*B.Sc ( computer science)*

Chennai

### Velammal Matric Hr Sec School Panchetty ..... Apr 2016 — Mar 2017

*HSC*

Chennai

## SKILLS

Penetration Testing

Web Application Security

API Security

Cloud Security

Secure Code review

## COURSES

### CEH v11 — 2021 — 2024

*EC-Council*

### AWS Cloud practitioner — 2021 — 2024

*AWS*

## HOBBIES

***Travelling, Food Explorer***

## LANGUAGES

English — ***Good working knowledge***

Tamil — ***Native speaker***

Telugu — ***Working knowledge***

### Publications

Published some google dorks in Google Hacking Database

- **GHDB-ID: 7725** ( This dork helps in finding the Shodan API Keys around the Pastebin using Google Dorking )
- **GHDB-ID: 7698** ( This dork was once used to find the Java deserialization vulnerabilities in Indian government Web Applications )
- **GHDB-ID: 7699** ( This dork was used to find the Internal source code files of the particular site )
- **GHDB-ID: 7700** ( This dork will expose AWS Access keys through the pastebin which was cached by the particular organization )
- **GHDB-ID: 7719** ( This dork will help us finding the misconfigured nginx leads to disclosure of Internal Source codes and subdirectories )

### Accomplishments

- Certified Ethical Hacker v11 ( By EC-Council )
- AWS Cloud practitioner ( By AWS )
- Braintech Championship ( Hackathon Conducted by Azure Skynet and Got 2nd Position Among the 200 teams participated in the tournament )
- Got Acknowledged by more than 25+ Companies around the world and list includes Government Organization
- Achieved some CVEs for contributing and finding vulnerabilities in the Open source software Application
- **CVE-2021-43437** ( Host header poising in Engineers Online portal )
- **CVE-2021-43438** ( Persistant XSS in iResturant Application )
- **CVE-2021-43439** ( Remote Code Execution in iResturant Application )
- **CVE-2021-43440** ( Multiple stored XSS in iOrder Application )
- **CVE-2021-43441** ( HTML injection in iOrder Application )