# Neelkumar Patel

Graduate Research Assistant
WiSSR Lab, University of Maryland, College Park

Email: nnpatel@umd.edu
Address: Hyattsville, College Park, MD
GitHub: github.com/neelpatel05

## Education

- **University of Maryland** — College Park, MD
  *Masters of Engineering, Cybersecurity; GPA: 4.00* — *Anticipated May 2021*
- **Gujarat Technological University** — Anand, India
  *Bachelors of Technology, Information Technology; GPA: 3.85* — *Aug 2015 - May 2019*

## Experience

- **Department of Computer Science, University of Maryland** — College Park, MD
  *Graduate Research Assistant* — *Jan 2020 - Present*
  - **Research field**: Currently, working at WiSSR Lab advised by Prof (Dr.) Nirupam Roy. My research is focused on Embedded System Security and Intelligent Honeypots for IoT/Hardware devices.
- **OpenEyes Technologies** — Vadodara, India
  *Intern - Product and Project* — *Jan 2019 - Apr 2019*
  - **Convolution Neural Network Developer**: Researched latest technologies to construct a Convolution Neural Network (CNN) platform "Anti-Smokify" achieving 92% accuracy.
  - **Amazon Web Services**: Performed Identity Access Management (IAM) for development of platform utilizing Amazon Web Services (AWS). Utilized DynamoDB for backend development.
  - **Security**: Inspected and resolved API request and response errors employing Wireshark sniffing tool to capture and rectify faults. Diagnosed and exposed critical software vulnerabilities to propose solutions to augment software security.

## Skills Summary

- **Languages & Databases**: Python, C, C++, Java, Go, Unix scripting, Javascript, SQL, NoSQL, MongoDB
- **Assembly Languages**: x86 IA-32, IA-64 (Familiar)
- **Hacking Tools**: Wireshark, NMAP, Burpsuite, Metasploit, Dig, Hashcat, John the ripper
- **Operation Systems & Tools**: Linux, macOS, Windows, Riverbed Modeler, Docker, GIT, Android Studio, Xcode
- **Other**: Rest APIs, Flask, Machine Learning, Deep Learning, Keras, Tensorflow

## Projects

- **Exploiting Buffer Overflow in Cherokee Webserver - C, IA-32, Python, GNU Debugger**: Developed exploit in python to buffer overflow the cherokee webserver which leads to crashing. Overwriting argv[0] to insane length causes the webserver as well as admin panel to carsh and fails to bind the port (Dec '19)
- **Brute force SSH - Go, Python, Wireshark**: Designed and created a brute force attacking software to gain remote access of machines through Secure Shell (SSH) protocol. Integrated project with crunch penetration testing tool to generate word-list according to specifications of attacker (Aug '19)
- **Brute force ZIP - Go, Python**: Implemented a terminal program to perform a brute force attack on password-protected zip files on a local computer or remote machines. Scripted Python code generates word list and Golang script performs brute force attack with each password in generated word list (July '19)
- **JSON Web Tokens, JWT - Go, Python, Postman, REST API**: Built a secure REST API implementing JSON web tokens to assert claims between two parties or endpoints complying with RFC 7519 industry standard. Utilized REST API project to ensure secure authentication and integrity of information in various types of projects and software (Mar '19)
- **Cryptographic Algorithm - Python**: Devised a novel encryption and decryption cryptographic algorithm operating with metadata of input information for safe transmission of data over physical transmission media preventing from active and passive attack. Formulated algorithm randomly generates key from input data of different length and embeds key into transmitted information (Mar '18)

## Honors and Awards

- Ranked Third among batch of 72 students in my Information Technology Engineering Department.
- Received Excellency Award by "NASSCOM" for best project in Information Technology Department
- Acquired government funding for a national level project from Student Start-Up & Innovation Policy (SSIP)