

CENTRAL INSTITUTE OF ROAD TRANSPORT
P.B.No.1897, PUNE-NASHIK ROAD, PUNE - 411 026

About us:- Central Institute of Road Transport (CIRT) is approved Testing Agency under Ministry of Road Transport & Highways (MoRTH) under Central Motor Vehicles Rules (CMVR) for certification of vehicles and safety critical Components.

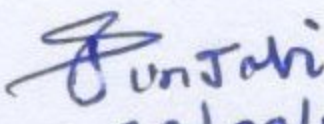
CIRT invites applications for the post of “**Automotive Cybersecurity Research Associate**” & “**Graduate Apprentice – Automotive Cybersecurity Research**” for its Automotive Cybersecurity Penetration Testing Laboratory at CIRT to support security testing of vehicle on-board networks and off-board backend/IT systems. The role is execution-focused and involves working under the guidance of senior testers on real-world automotive cybersecurity projects with OEMs and Tier-1s. The requirements are as mentioned in the table below :

Name of the Post	Automotive Cybersecurity Research Associate (01 Post)	Graduate Apprentice - Automotive Cybersecurity Research (01 Post)
Nature of Appointment	One year with provision of further extension.	Apprentice (One year)
Qualification	B.E./B.Tech in Computer Science/ Cybersecurity/ Electronics & Communication/ Electrical, Automotive, or related disciplines. OR BCA / MCA (or equivalent) with relevant industry-recognized cybersecurity certification(s) and demonstrable hands-on experience in penetration testing, vulnerability assessment (VAPT), or bug bounty.	B.E./B.Tech in Computer Science/ Cybersecurity/ Electronics & Communication/ Electrical, Automotive, or related disciplines. BCA / MCA with Cyber security / bug bounty experience
Experience/ Project Exposure	1-2 years experience in Vehicle network sniffing, replay, or fuzzing on CAN / CAN-FD (lab or project level). Basic UDS testing (session control, DID read/write – lab/project level). Network scanning and service enumeration of backend or on-prem systems. API testing for connected vehicle / telematics services. Academic project, lab, internship, or PoC in automotive or network security. OR Participated in Bug Bounty programs	Fresher having project exposure of IoT device testing at hardware, firmware, or communication level (lab, project, or PoC). Firmware extraction and static analysis using tools like binwalk and strings (basic level). Protocol testing of MQTT, CoAP, HTTP for misconfigurations and basic issues. Network scanning and traffic analysis of IoT devices in a lab setup. Academic project, internship, or PoC focused on IoT security or embedded security.
Required Skills	Understanding of networking fundamentals (TCP/IP, HTTP/HTTPS). Basic Linux usage (shell, basic commands, environment handling). Basic understanding of ECUs and vehicle networks. Strong grasp of cybersecurity fundamentals (vulnerabilities, attack surface, basic OWASP concepts).	Networking fundamentals (TCP/IP, HTTP/HTTPS). Basic Linux usage (shell, networking utilities, file system). Understanding of IoT architectures (device–gateway–cloud). Cybersecurity fundamentals (common vulnerabilities, basic threat models).

Additional Skills	Awareness of ISO/SAE 21434 and UNECE R155 at a high level. Basic scripting skills in Python or Bash (for automation and tooling). Exposure to automotive cybersecurity tools or lab setups (CANoe, CANalyzer, Scapy, etc.)	Exposure to UART/JTAG/SWD interfaces at a basic level. Awareness of OWASP IoT Top 10 and common IoT attack scenarios. Basic scripting in Python or Bash (automation, small utilities, parsing logs).
Key Responsibilities	Assist in testing in-vehicle networks (CAN / CAN-FD, basic UDS). Capture and analyze network traffic using tools like Wireshark and CAN tools. Support backend, API, and network testing using tools such as Nmap and Burp Suite (basic level). Execute predefined penetration test cases and collect technical evidence (logs, traces, screenshots). Document observations and support preparation of penetration test reports and summaries.	Assist in IoT device and firmware security testing. Perform basic network and protocol testing (MQTT, HTTP, CoAP – basic level). Support firmware extraction, basic static analysis, and simple reverse engineering tasks. Test device-to-cloud and API communication for security weaknesses. Document findings, maintain evidence, and support creation of penetration test reports.
Remuneration	Consolidated Pay of Rs. 45,500/- (including HRA) in case the candidate is CSIR-UGC NET or GATE qualified or has proven bug bounty record with vulnerabilities identified. Consolidated Pay of Rs. 36,400/- (including HRA) in case the candidate is not CSIR-UGC NET or GATE qualified.	Presently, it is Rs. 16,000/- per month for Graduate Engineer as per Section 11 of The Apprentices Rules 1992.

Interested candidates are requested to send their resume mentioning name, permanent address, present address, mobile number, Email address, educational qualification beginning with S.S.C.(with self-attested copies of certificates and marksheets) and recent passport size photograph to the Incharge-Administration, Central Institute of Road Transport, P.B.No.1897, Pune-Nashik Road, Bhosari, Pune - 411 026 or e-mail their resume with all relevant documents on pers@cirtindia.com on or before 07/10/2026 at 17.00 hrs.

Date : 22 /09/2026


22/09/26
In-charge-Admin.