Tarunkant Gupta

Curriculum Vitae

Madhya Pradesh, India
tarunkant05@gmail.com
spyclub.tech

Education

2016–2020 **Bachelor of Technology in Computer Science and Engineering**,
Amrita School of Engineering, Amritapuri, Kerala,
Current CGPA : 8.64/10.

2014–2016 **AISSCE**, *Sarvodaya Sr. Sec. School*, Kota, Rajasthan,
Percentage Obtained : 80%.

Interests

Web security, Penetration testing, Bug hunting, Security Engineering and Automation

Experience

Sept 2021–Present **Security Engineer**, *Disney+ Hotstar*, Bangalore, India.
Working as full time employment.

- Responsible for securing all public facing services in the landscape of Hotstar
- Started and manage the Hotstar Vulnerability Disclosure Program
- Lead the Automation pillar, developing security automation tools for Perimeter Security, significantly enhancing vulnerability detection efficiency.
- Automate real-time security scans via CI/CD (GitHub Actions) and enforce Shift Left Security by integrating security early in development cycle.
- Lead and proactively conduct Red Teaming activities to identify and mitigate security risks across the organization
- Manage security incidents, ensuring quick response and mitigation
- Oversee the security of the Ads component within AppSec, ensuring a strong posture
- Perform penetration testing and develops solutions to mitigate security vulnerabilities
- Conduct security code audits and design reviews to identify vulnerabilities early in the SSDLC and prevent security flaws from reaching production.

July 2020–Sept 2021 **Red Team Security Researcher**, *FireCompass*, Bangalore, India.
Worked as full time employment.

- Performed various security research to find new attack vectors
- Led multiple Red Team activities
- Performed numerous VAPT assessments for a diverse range of clients
- Created multiple offensive security automation tools to add value in the Product

2016–2020 **Member of Team bi0s**, *CTF Team*, Amrita University, Amritapuri.
Team bi0s ranked number-1 CTF team across India for the past 4 years as per ctftime.org.
Main focus on Web Exploitation.

Oct 2018 **InCTF**, *Challenge Developer and Organizer*.
International CTF, conducted along with Team bi0s.
Created the web challenges and was the part of the hosting team.

April 2017 **Smart India Hackathon**, College of Engineering, Pune.
Created a framework as a solution to creating awareness about cybersecurity. The framework was a lightweight, multilingual and cross-platform CTF framework with an interactive game mode. Event was conducted by the Govt of India.

April 2017–2018 **InCTF Junior**, *Challenge Developer and Organizer*.
InCTF Junior is the first school CTF exclusively for Indian school students, conducted along with Team bi0s.
Developed challenges and also worked on infrastructure.

Achievements

Technical

Dec 2022 **Discovered a Security Misconfiguration in Akamai**.
Identified an unusual cache poisoning vulnerability between Akamai and S3, allowing attackers to cache malicious content on S3 buckets onboarded in Akamai due to improper header handling by Akamai when forwarding requests to S3.

Feb 2021 **Found two Security bugs on Dropbox**.
Detected a blind SSRF vulnerability allowing attackers to scan internal infrastructure. Also identified a bug that could lead to user-level DoS.

July 2020 **Found two Security bugs on Spotify**.
Discovered a one-click account takeover vulnerability, enabling full control over victim accounts via API. Also found a flaw allowing attackers to monitor victim activity.

Sept 2019 **Champions of CSAW CTF from India Region**, *as part of team bi0s*.
Conducted as a part of Cyber Security Awareness Week by New York University

July 2019 **Champions of ISITDTU Quals**, *as part of team bi0s*.
Conducted by Duy Tan University, Vietnam

March 2019 **Awardee of Student Excellence Award 2018**, *Amrita University*.
Received for outstanding performance while representing the University in CTFs

Feb 2019 **Found two Security bugs on Quora**, *(Link)*.
Detected Horizontal Privilege Escalation which led an attacker to ask questions or post answers from victim's account. And also was able to ask questions or post answers without having verified email id

Feb 2019 **Second runners up in HackIM CTF**, *as part of team bi0s*.
Conducted by NullCon 2019

Oct 2018 **Champions of the on-site Hack.lu CTF**, *as part of team bi0s*.
Conducted by FluxFingers team as part of HackLu Conference at Luxembourg

March 2018 **Scholarship winner for attending Nullcon**, *Goa*.
Was the recipient of the scholarship of India's largest cybersecurity conference

Non-Technical

July 2018 **Student Social Responsibility**.
Conducted with the aim of educating school students about staying safe in Cyber Space. Students were taught about Phishing/Scamming attacks, cyber bullying and lessons on how to stay safe online

Oct 2013 **Selected for State Level Table-Tennis Selection Meet**.
Event was Conducted by the Ministry of HRD, Dept. of Education and Govt. of India

2013-2014 **Selected for Nationals in 17th Regional Youth Parliament Competition**.
An Autonomous Organization under Ministry of HRD, Dept. of School Education & Literacy and Govt. of India

Projects

Oct 2019 **fuzzphunc**, *(Link)*.
A lazy fuzzer to fuzz all PHP functions and check if they call execve systemcall internally, which can be used to bypass PHP disable_functions via LD_PRELOAD.
Made a tool on top of the same, to let the user know how strong their disable_functions is.

Aug 2019 **Backdrop CMS Testing**.
Tested Backdrop CMS, the forked project of Drupal, with both black and white box testing. Discovered 6 Security issues, in which 4 are fixed and other 2 are acknowledged :

- CVE 2019-14771 : Remote Code Execution using import/export functionality.
- CVE 2019-19902 : Bypassed the patch applied in CVE-2019-14771.
- CVE 2019-14770 : Triggering Stored XSS from search functionality.
- CVE 2019-14769 : Triggering Stored XSS on displaying Block labels.

Aug 2018 **Gopherus**, *(Link)*.
Generate Gopher payload for exploiting SSRF and gain Remote Code Execution on SSRF vulnerable sites having ports open for various servers like MySQL, FastCGI, Zabbix and others. Currently, this tool has 3k+ stars on github.

July 2018 **EndPoint-Finder**, *(Link)*.
A tool for finding the End-points in JavaScript files, which helps in the penetration testing to test all the End-Points of the Application.

May 2018 **Home Appliance Automation**, *(Link)*.
An IoT device which can automate the home appliances as user wants. It was built on the top of Google Assistant for voice interface and ESP8266 for IoT device communication using MQTT protocol.

Computer skills

Languages	Python, PHP, Bash, JavaScript, C, Java
DBMS	MySQL, PostgreSQL, SQLite
Frameworks	Django, Flask, Tornado
Tools	Burp Suite, Wireshark, Docker, VirtualBox
Platforms	GNU/Linux

Online profiles

- GitHub : tarunkant
- LinkedIn : tarunkant-g-215830129
- Twitter : @TarunkantG
- Blog : spyclub.tech
- Wargames Handle : tarunkant, Tarun, SpyD3r