VERNEET SINGH | (+33) 767402211 | verneet.com | verneet115@gmail.com | linkedin.com/in/verneet

EDUCATION

Master of Science	Digital Security	EURECOM, France	–	Sep 2021 – Present
Bachelor of Engineering	Computer Science & Engineering	Oriental Institute Of Science and Technology, India	7.23/10	2015 - 2019

EXPERIENCE

Société Générale, Bangalore — **Cyber Security Analyst** — **June 2019 - Aug 2021**

Responsibilities	▪ **Vulnerability Assessment:** Performed vulnerability assessment on various applications and infrastructures like web applications, cloud, IoT devices and servers. Detected more than 200 critical and high vulnerabilities like Remote code execution, SQL injection, SSRF, XSS, etc. ▪ **Security Awareness:** Hosted cybersecurity sessions on OWASP top 10 in 'Cyber Thursday' to spread awareness on security throughout the organization and actively participated in security events like 'Beat the Bug' and 'Security Hour'. Authored newsletters on importance of secure coding, phishing emails and physical security. ▪ **Purple Teaming:** Performed full-scaled attacking simulations to identify security exposures by challenging the SOC team of the organization and assessing detection techniques.

Bugcrowd & Hackerone & Synack Red Team — **Security Researcher** — **Feb 2018 – Present**

Tasks	Diagnosed vulnerabilities such as Reflected XSS, Stored XSS, Clickjacking, Insecure CORS, Misconfigured SPF record, SSRF, HTML Injection, Host Header Injection, SSTI & SQL Injection. Verified bugs using tools like Burp Suite, Nmap, Niko, Sqlmap, Wireshark, Drozer Framework.

Freelancer.com — **Web Developer** — **Apr 2015 - 2019**

Tasks	Completed over 70 projects with 5 star rating. Designed and developed web-applications, corporate identity on various CMS along with SEO andHelped clients with malware removal and cleanup services.

ACHIEVEMENTS

- Participated in TRACS security and cryptanalysis competition organized by ViaRézo and the DGSE in Paris. 2021
- **Star of the Quarter Q1:** Recognised under 'Curiosity' category for Identifying unique vulnerabilities. 2021
- **Session:** 2020
  - Delivered a session on OWASP Top 10 at Oriental College of Sc. and Tech with more than 400 participants.
  - Delivered a talk on "CVE in 5mins" at Null, Bhopal.
- **Live Hacking Event:** Got selected for International event 'Bounty Bash' in Nepal. 2019
- **Acknowledged**: Vimeo, Preply, SurveyMonkey, Zomato, Redbus, Goibibo, TheVauletapp, Yatra, Ringlead, JotForm, Freelancer, Uber, IRobot, Cloudways, etc. 2020
- Participated in Brainwaves Hackathon by Société Générale **(Fourth Place)**
- **MVP**: Achieved Most Valuable Player of 2019 Q4 by reporting bugs with priority percentile range for P1s, P2s, and P3s above 80%. 2019
- **CTF**: 2nd Runner up at Braindead CTF by Flipkart at Nullcon, Goa. 2018

PROJECTS

Adversarial attack against Healthcare	This project was done in association with iABG. We implemented models to predict the different diseases or benign states of the patient. We explored and implemented methods to attack the models and we focused on PGD, CarliniWagner and Hop skip jump attacks and evaluated a comparison between them.
Lego EV3 Robot (link)	The robot was built using a Lego ev3 Mindstorms set along with various sets of sensors and actuators. The objective of this robot was to race against time and complete the race on track by avoiding the obstacles on the way.
Recon Automation	Developed an automation tool by combining multiple open-source scripts to recon and detect the vulnerabilities in a web application. The tool performs port scanning, directory brute-forcing and detects vulnerabilities like XSS, Open redirect, weak SSL, and many more.

TECHNICAL SKILLS

Language	Python, C/C++, XML, JavaScript, HTML, CSS, PHP	**Tools**	Burp Suite, Nmap, Metasploit, Beef Framework, Hydra, Wireshark, Sqlmap, PuTTy, Nessus
Software	Visual Studio, JetBrains, IntelliJ IDEA, Android Studio	**OS**	Kali Linux, Windows, Android, Ubuntu, IOS

Publications

CVE-2019-16685 CVE-2019-16686 CVE-2019-16687 CVE-2019-16688	An issue was discovered in Dolibarr 9.0.5. It has multiple stored XSS vulnerabilities in 'Job Position', 'User Note', 'Signature', and 'Email Template'. A user with no privilege can inject a script to attack the admin which can result in an account takeover.	2019