Asd

Gaurav Narwani

+91 8879499881 | gauravnarwani.com | gauravnarwani97@gmail.com | linkedin.com/in/gauravnarwani97 | github.com/gauravnarwani97

Computer Engineer, looking forward to craft solutions to difficult problems in survivable cyber-physical systems and enterprise information systems. Keen technician and software programmer with extensive experience of online security packages and tools. Seeking a position with more responsibility and room to grow.

Education

University of Mumbai - B.E., Computer Engineering, 7.62 / 10 — July 2015 – Jun 2019

Relevant Coursework: Structural Programming, Database Management and Warehousing, Theoretical Computer Science, Computer Organization & Architecture, Engineering Mathematics, Computer Graphics, Java Programming, Microprocessors, Operating System, Computer Network, Project Management, Web Technology, Mobile Computing, Compiler Construction, Machine Learning

Skills

Language:	Java, C/C++, XML, JavaScript, HTML, CSS, PHP, Python
Operating Systems:	Kali Linux, BackTrack, Windows, Android, iOS, Ubuntu
Tools:	Burp Suite, Nmap, Metasploit, Beef Framework, Ettercap, Hydra, Wireshark, Aircrack-ng, Sqlmap, PuTTy
Software:	Android Studio, Visual Studio, JetBrains, IntelliJ IDEA, Mist, Adobe Suite, Remix, Knoxx, Shodan, Tor

Experience

Cyber Security Engineer– *Société Générale Bangalore* — June 2019 – Present

- Assisted the security team at Société Générale finding vulnerabilities in applications belonging to Société Générale and its acquisitions.
- Participated in weekly vulnerability mitigation meetings, addressing common security threats to the applications of the company and its clients.

Independent Security Researcher - *Synack, Bugcrowd, HackerOne* — March 2018 – Present

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

Cyber Security Intern – *Olcademy* — July 2018 – May 2019

- Assisted the security team at Olcademy as a Penetration Tester to detect vulnerabilities in Web and Mobile Applications.
- Supervised a team of 5 people after being promoted as Cyber Security Lead. Scheduled daily tasks to team members and conducted a small CTF competition in the team. Designed the Road Map of the team to present them to Investors.
- Diagnosed Vulnerabilities such as SQL Injection, Cross Site Scripting, Clickjacking, CSRF, Misconfigured SPF and Information disclosure by using Burp Suite and Nessus.
- Inspected and generated bug reports on the mobile application using Genymotion and Drozer framework.

Security Researcher and Developer Intern - *Security Brigade Mumbai* — June 2018 – July 2018

- Worked as part of the Red Team for hardening the system of companies against real attacks
- Automated the testing of servers for Apache Struts Vulnerability (CVE-2017-5638) using python.
- Incorporated Beautiful Soup Library to scrape the source code and also simultaneously investigate the leakage on GitHub using pygithub3
- Developed a tool to inspect default credentials at specific IP address when connected to MySQL and MsSQL

Projects

Electronic Health Record and Medicine Inventory using Blockchain — Dec 2018

- Developed a storage for Electronic health records on Ethereum network using IPFS. IPFS was linked to content ids' via an Infura node to be stored in the network. Each report accessed via the id created a transaction of few ethers
- Doctors were given permission to view patients reports to whom he was given access

Default Credentials Checker Tool — March 2018

- Tested databases like MySQL/MsSQL for any open ports to extract data by applying default credential checks with the help of a customized tool programmed in python.

System Attack Monitoring and Prediction System @ NSE FutureTech ML Hackathon — Dec 2016 – Jan 2017

- Developed a system to monitor low-priority security alerts to analyze and predict long-term pattern attacks that typically go under the radar. Used K-Means for clustering similar data groups and patterns to identify outliers in the dataset.

Activities & Awards

Delivered a Speech on Owasp Top 10 at TheTestTribe Meetup — Sept 2018

Hall of Fame: Sophos, The Things Network, Ford, Sentiance, TheTestTribe, Under Armour, Inflectra, Roamler, Fitbit, Jet, Western Union, Humble Bundle, Puppet Labs, Overstock VDP — May 2018 – Present

Swag: Octopus, Buddy Works, GeeksforGeeks — May 2018 – Present

Participated in Runs Cyber Security Hackathon ***(Prize Winner)*** — May 2018

Participated in Online Security Testing Hackathon for Junglee Rummy ***(First Place)*** — May 2018

Participated in National Stock Exchange FutureTech 2018 Machine Learning Hackathon — March 2018

Participated in UnScript 2018 Hackathon — March 2018

Participated in Brainwaves Hackathon by Société Générale ***(Fifth Place)*** — Feb 2019

Certifications: Certified Information Security and Ethical Hacking, Pristine Infosolutions — July 2017

Publications

CVE-2019-14546 – *EspoCRM 5.6.8* Aug 2019

An issue was discovered in EspoCRM before 5.6.9. Stored XSS was executed on the Preference page as well as while sending an email when a malicious payload was inserted inside the Email Signature in the Preference page. The attacker could insert malicious JavaScript inside his email signature, which fires when the victim replies or forwards the mail, thus helping him steal victims' cookies (hence compromising their accounts).

CVE-2019-14547 – *EspoCRM 5.6.8* Aug 2019

An issue was discovered in EspoCRM before 5.6.9. Stored XSS was executed when an attacker sends an attachment to admin with malicious JavaScript in the filename. This JavaScript executed when an admin selects the particular file from the list of all attachments. The attacker could inject the JavaScript inside the filename and send it to users, thus helping him steal victims' cookies (hence compromising their accounts).

CVE-2019-14548 – *EspoCRM 5.6.8* Aug 2019

An issue was discovered in EspoCRM before 5.6.9. Stored XSS in the body of an Article was executed when a victim opens articles received through mail. This Article can be formed by an attacker using the Knowledge Base feature in the tab list. The attacker could inject malicious JavaScript inside the body of the article, thus helping him steal victims' cookies (hence compromising their accounts).

CVE-2019-14549 – *EspoCRM 5.6.8* Aug 2019

An issue was discovered in EspoCRM before 5.6.9. Stored XSS was executed inside the title and breadcrumb of a newly formed entity available to all the users. A malicious user can inject JavaScript in these values of an entity, thus stealing user cookies when someone visits the publicly accessible link.

CVE-2019-14550 – *EspoCRM 5.6.8* Aug 2019

An issue was discovered in EspoCRM before 5.6.9. Stored XSS was executed when a victim clicks on the Edit Dashboard feature present on the Homepage. An attacker can load malicious JavaScript inside the add tab list feature, which would fire when a user clicks on the Edit Dashboard button, thus helping him steal victims' cookies (hence compromising their accounts).