

Nikhar Mehta

nikharmehta3@gmail.com | (240)-543-0321

[linkedin.com/in/nikharmehtha-499879109/](https://www.linkedin.com/in/nikharmehtha-499879109/)

EDUCATION

University of Maryland, College Park.

Aug'19 - May'21

Candidate for Master of Cybersecurity, GPA: 3.6/4

CHARUSAT University, Anand, India

Aug '14 - May'18

Bachelor of Technology in Computer Engineering, GPA: 8.71/10

TECHNICAL KNOWLEDGE

Certifications: Pursuing CEH (Certified Ethical Hacking) certification

Security Tools: Burp Suite, Nmap, Nessus, ZAP, Metasploit, Wireshark, Splunk, SQLMap, Dirbuster, Hydra, Owasp ZAP

Languages: Python, JavaScript, SQL, PHP, Java, C, C++, HTML, CSS

Operating Systems: Kali Linux, Ubuntu, Windows

Software: VMWare, MS Office, Git, Jira, Docker

Relevant Coursework: Hacking of C and Unix binaries, Penetration Testing, Cloud Security, Digital Forensics, Cryptography and Network Security, Applied Cryptography, Advanced Computing, Security Tools, Data Communication and Networking.

Area of Expertise:

- Perform comprehensive Web Application Penetration testing using Burp Suite and ZAP, along with triaging and remediating the vulnerabilities including OWASP TOP 10 (Including XSRF, SSRF, XSS, SQLI).
- Experience in VAPT (Vulnerability Assessment & Penetration testing), Security Testing Techniques (SAST, DAST, fuzzing), Threat Modeling.
- Deep understanding of Cloud Security, Code Review, Secure CI/CD pipeline, DevSecOps, Intrusion Detection, MITRE Att&ck Framework, Incident Response.
- Familiar with security and networking protocol such as TCP/IP, UDP, HTTPS, DNSSEC, DHCP, SSH.
- Decent knowledge of Cryptographic algorithms and the attacks.
- Proactive in CTF (Capture The Flag) event participation.

WORK EXPERIENCE

Technical Intern – Security Engineer at Synopsys Inc, US.

May '20 – Present

- Composed security solutions for internal intelligence tool, Stargazer, to get prescription on security scans to be performed and carried out conditional scans (Including SAST, DAST) according to resulted prescription.
- Performed black-box penetration testing on ongoing projects and thoroughly documented the findings including weak authentication, improper encryption, CSRF and collaborated with engineering teams to define remediations.
- Developed a java module to fetch data from Jira about critical and high priority issues to inspect how many open issues are violating the given threshold value and to notify the concerning owners.
- Modernized internal tool, stargazer's GUI to automate the process of security configuration file generation functionality using JavaScript.

Security Intern at Zydus Cadila Pvt. Ltd, India

Nov '18 – July'18

- Performed vulnerability assessment (VAPT), threat modeling of internal employee portal and reviewed the existing code base to find chain of exploits and to improve company's overall security posture.
- Conducted monthly security testing of internal system by scanning and identifying possible security flaws using Internal tools and tools like Nessus, Burp Suite, Wireshark.
- Assisted cross-functional teams in remediating the discovered vulnerabilities to deliver efficient security solutions.

Quality Assurance Intern at Volansys Technologies Pvt. Ltd., India.

Dec '17 – July '18

- Drove testing across "Industrial IoT Enabled with Mobile Application" product suite, analyzed most of the customer use cases and identified potential pitfalls.
- Authored clear, concise testing documentation to facilitate software development across multiple internal teams.

ACADEMIC PROJECTS

Vulnerability Scanner to Detect Known Vulnerabilities

Dec '20

- Developed a Vulnerability Scanner using Python to scan for open ports and to detect & notify users about the exploitable services running on open ports .

Capture the Flag in Windows and Linux Machines

Dec '19

- Hacked into two Windows and Ubuntu Machines using security tools like Metasploit, Hydra, Nmap and successfully captured the flags.

Cloud Migration of Troll World Web Application

Aug '19

- Redesigned and Migrated the Troll World Web Application to AWS Cloud by implementing Patching, Backup, Account Permissions, Load Balancing and DDoS mitigation strategies using AWS cloud services.

Damn Vulnerable Web Application (DVWA)

Apr '19

- Tested, Identified and documented SQL-Injection, Cross-site scripting, Command Injection, and Local file inclusion vulnerabilities in detail on DVWA application as a midterm curriculum project as part of master's program.