NEERAJ SONANIYA

Email: nsonaniya2010@gmail.com | **Mobile:** +91-(971)-393-1105 | **Indian** |
Linkedin: linkedin.com/in/neerajsonaniya | **Github:** github.com/nsonaniya2010

Career Snapshot

- An accomplished **Product Security Engineer** with **5+** years of experience.
- Practical hands-on experience with Penetration Testing, Secure Code Review, Threat Modelling (sound knowledge), SAST, Secrets Hunting and Implementing Pre-commit hooks.
- Admirable familiarity with Mobile Application Security, Cloud Security and DevSecOps.
- Streamlining complex challenges via automation to reduce manual workloads for Product Security, SecOps, and Compliance teams.
- Facilitating effective cross-team communication and engaging with managers on a weekly basis to expedite issue resolution and gain insight into new product developments and features for security reviews.
- Familiarity in integrating security measures seamlessly within the Software Development Life Cycle (SDLC).

Awards

Awards & Achievements	• Awarded with **Relentless Leader of 2021 @ Unacademy**. • Uncovered a critical vulnerability in the **State Bank of India** involving an OTP Bypass during transactions. • Discovered a vulnerability in Facebook that earned a bounty, where a rate limit issue resulted in the removal of mobile numbers from Instagram accounts. • Reported valid security vulnerabilities to over **50 organizations**, including tech giants like Google, Facebook, Twitter, and Uber, contributing to their enhanced security measures.

Technical Skills

Programming Languages, Softwares and Technologies	• **Programming** – Python • **DBMS** – MySQL • **Softwares** – Pycharm, Vim, Burp Suite, Nessus • **Operating Systems** – Windows, Linux, MacOS • **Cloud Services** - Amazon Web Services (AWS) • **Others** – Machine Learning, Git, JIRA, Kibana, Linear, Jenkins.

Projects

Unacademy

Senior Product Security Engineer (Oct 2020 - Till Now)

1. **Streamlining Enterprise Security and Compliance through Automation** — **Unacademy (Apr’23 - Now)**
   a. **Automated Detection of Improper Offboarding/Transition:**
      - Automated data collection from Google Sheets (HR-managed), Google Workspace, and Slack, feeding into the database.
      - Creation of a Grafana dashboard for easy data consumption by the enterprise security team and other relevant departments.
      - Streamlined identification of orphan and improperly managed accounts, enhancing security.

   b. **User Compliance Audit Automation:**
      - Implemented an automated system to ensure high-level compliance by swiftly identifying non-compliant users.
      - Integration with multiple applications, including Retool, Atlas, Django Admin, Compass, Linear, Github, and MySQL databases.
      - Drastically reduced manual efforts previously required for collecting compliance data from various systems.

   Tech Stack: Python, MySQL, Grafana

   Impact: Achieved higher user compliance while significantly reducing manual work, resulting in a remarkable **75% improvement** in efficiency for both the user compliance and enterprise security teams across the mentioned tasks.

2. **Automated System for Detection and Management of the SAST Security issues.** — **Unacademy (Mar’22 - Now)**
   a) A baseline based automated system was developed to find potential security issues across all code bases and push them to the DB.(auto detection of the repository programming language(s), and scanning it with supported tools only.)
   b) Logics to de-duplicate and automatically close the issues (if doesn't exist anymore) were created.
   c) Appsmith App was created to review the findings (updating severity and other meta info. into the DB.) and report them to the respective owners.
   d) **Tools/Tech Stack**: Python, Appsmith, Grafana, MySQL, Bandit, Semgrep, GoSec.

3. **Automated System for Hunting and Managing Secrets** — **Unacademy (Nov’20 - Now)**
   a) An automated system was developed to detect and alert secrets across all code repositories to the respective owners.
   b) Detection of secrets was implemented in the:
      - **Pre-commit hooks** were added to devs machines to detect and prevent secrets from getting commited to code itself.
      - Early stage of the SDLC (i.e. in the **CI/CD pipeline**) - So that secrets can't go into the production code.
      - **Recurring weekly scan** (post deployment) - So that, if we miss something in CI/CD, we catch them in weekly scans.

   c) New signatures and detection rules were introduced to improve the overall secrets detection coverage.
   d) **Impact:** Achieved target of 0 secrets within all code bases. (Initial numbers were ~ 2,000.)
   e) **Tools/Tech Stack:** Python, Customized detect-secrets (by Yelp), Grafana, MySQL, Slack.

4. **Critical AWS Services Access Control Audit (Minimizing Attack Surface)** — **Unacademy (Oct’20 - Dec’20)**
   a) Extensive Access Control review was done for AWS services: S3, Redshift, Elastic Search, DynamoDB.
   b) Automation script was written to fetch users IAM data including their access policies for services specified above.
   c) The Principle of Least Privilege (PoLP) was used to remove unnecessary access permissions to the services.
   d) Specifically for S3, buckets were categorised as sensitive & non-sensitive and accordingly action was taken to make changes in bucket and user's IAM permissions.

redBus

Security Engineer (Sep 2018 - Oct 2020)

1. **KYC Verification Feature for rPool** **redBus (Jan’20 - Apr’20)**
   a) Integration of KYC verification feature with 3rd party to verify user while on-boarding to rPool.
   b) Automatic verification of multiple Govt Identity cards including Indian PAN Card, Driving License etc.
   c) Developed with considering security risks in mind like limiting number of verification attempts in a time frame, user registration check before initiating verification, image tampering etc.
   d) **Tools/Tech Stack** - Python, Arango DB, Elastic Search, Amazon Web Services, Python Flask.

2. **red:Assassin- A tool to scan API’s for security vulnerabilities** **redBus (Nov’18 - March’19)**
   a) Created a tool to automate API scanning for security risks not limited to only OWASP Top 10 (2017).
   b) Given a URL of either Postman collection or Swagger JSON data, it will automatically detect type of collection (Postman or Swagger) and start scanning for security vulnerabilities.
   c) After completion of scanning, all identified security vulnerabilities are displayed on UI, with HTTP request, payload (if available), severity, definition of vulnerability, remediation, and other resources.
   d) It also creates an issue with identified severity on JIRA Dashboard with detection of duplicate reports (this is limited to the reported created by red:Assassin only).
   e) It also create a message on Slack to notify other persons.
   f) **Tools/Tech Stack** - Python, HTML, JavaScript, JIRA.

Open Source Contribution

SubDomainizer - An Open Source intelligence tool (OSINT) for information security professionals. **Self (Dec’18 - Till Now)**

a) Github URL: **https://github.com/nsonaniya2010/SubDomainizer**
b) **Impressive GitHub Stats:** Garnering over **1593*** stars and **241*** forks on GitHub.
c) **Comprehensive URL Analysis:** Proficiently identifies all JavaScript files (both inline and external) associated with a given URL, potentially revealing sensitive information such as secret keys and internal/external subdomains.
d) **Multi-Service Detection:** Capable of detecting not only secrets and subdomains but also various storage service URLs like Azure, RackCDN, Google Cloud services, and S3 buckets.
e) **GitHub Scan:** Offers a convenient GitHub scanning feature where it scrutinizes specified domains on GitHub and generates reports detailing the discovered secrets and subdomains.
f) **Local Scanning:** Provides the ability to perform local scans by recursively examining files within a designated folder, uncovering secrets and subdomains present.
g) **SAN Discovery:** Equipped to find Subject Alternative Names (SANs) associated with the given domains, enhancing its utility in certificate and domain analysis.

Education

Madhav Institute of Technology & Science	**Bachelor of Engineering, Computer Science and Engineering, 2014-2018** Cumulative Grade Point Average (CGPA): **7.20**
Lady Anusuya Singhania Educational Academy	**Higher Secondary Education** Central Board of Secondary Education (CBSE) Aggregate: **82.00%**, Mathematics: **95%**

Other Responsibilities

- Conducting Security Research to Identify Complex Issues at Scale.
- Active Involvement in PODs Sprint Planning/Grooming Meetings to Enhance the Secure SDLC Process.
- Collaborating with the Team to Boost Productivity.
- Overseeing and Managing the Bug Bounty Program.

Hobbies

- Enthusiastic Cricket Enthusiast and Player.
- Embracing Yoga and Meditation for Mind-Body Wellness.
- Exploring the Benefits of Ayurveda for Holistic Health.