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 **Application Security Engineer** with **four*** years of experience.
- Possess practical hands-on experience with penetration testing, secure code review, and secure architecture reviews.
- Experience in defensive side of the application security.
- Admirable familiarity with Mobile Application Security and Cloud Security.
- Experience in automating complex problems (planning, designing, and evaluating) to reduce manual work.
- Effective cross-team communication to get issues resolved in timely manner.
- The "Go to" guy for tough and hard to track problems efficiently.

Awards

Awards & Achievements	• Relentless Leader of 2021 @ Unacademy. • Found a critical vulnerability in State Bank of India – One Time Password (OTP) Bypass at the time of transaction. • Found vulnerability in Facebook and was awarded with bounty – Rate limit problem leads to mobile number removal. • Found a critical vulnerability in Reliance JIO and was awarded with bounty – Hacking all the retailer's accounts leads to disclosure of sensitive information like Aadhar Card Numbers, Address, Email address, Mobile Numbers etc. • Reported valid security vulnerabilities to more than 50 organizations including Google, Facebook, Twitter, Uber and helped them in getting more secure.

Technical Skills

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

Projects

Unacademy

Senior Product Security Engineer (Oct 2020 - Till Now)

1. Static Code Analysis Findings Management System **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.

2. Secrets Life Cycle Management System **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:
    i) Early stage of the SDLC (i.e. in the CI/CD pipeline) - So that secrets can't go into the production code.
    ii) 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) 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.

3. Access Control review for critical AWS Services **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. Hierarchical LDA for heterogeneous reviews - A customized version of Guided(Original) LDA for Topic Modeling of user reviews. **redBus (Apr'19 - Oct'19)**

a) Derived a semi-supervised, DAG (Directed Acyclic Graph) based method to improve the confidence and accuracy of the model.
b) Based on the research, it was found that due to heterogeneous nature of reviews the accuracy/confidence of the model wasn't good.
c) Models from model were created with the help of reviews from each topics we get from original model.
d) Step c is being repeated until the required confidence/accuracy reached.
e) **Tools/Tech Stack** - Python, Topic Modelling, AWS Sagemaker, Python Flask, Text Analytics.

3. 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) **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) Having more than **1320*** stars and **215*** forks on GitHub.
c) Given a URL it finds all the JS files (inline & external to that page) which may contain sensitive information like Secret keys, internal or external subdomains.
d) It can find the Secrets, Sub-domains, S3 buckets, and other storage services URLs. e.g. Azure, RackCDN, Google Cloud services, etc
e) Github Scan - It scans github with given domain(s) and report secrets & subdomains found there.
f) Local scanning - It recursively scans files in the folder and report secrets & subdomains.
g) It can also find Subject Alternative Names (SANs) for the given domains.

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

- Security Research in to find complex problems in bulk.
- Participate in the PODs sprint planning/grooming meetings for Secure SDLC process.
- Help team to improve the productivity.
- Managing the Bug Bounty Program.
- Moderating tech talks internally.

Hobbies

- Watching and Playing Cricket.
- Yoga.
- Meditation.
- Ayurveda.