NEERAJ SONANIYA

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

Statement of purpose

With a demonstrated history in Information Security, I hope to work in an environment of active learners, brilliant minds to further groom my skills to a better level and contribute through my experience to enhance the Security of it as well.

Education

Madhav Institute of Technology and 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%**

Awards

Awards & Achievements	• 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, Technologies & Software's	• **Programming** – C, Python • **DBMS** – SQL, ArangoDB • **Softwares** – Pycharm, Burp Suite, Vim. • **Operating Systems** – Windows, Linux • **Cloud** - Amazon Web Services (AWS) • **Others** – Machine Learning, Git, JIRA, Kibana

Developed Projects

redBus

Security Engineer *Sep 2018 - Till Now*

1. KYC Verification Feature for rPool **redBus (Jan'20 - Till Now)**

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) Tech Stack - Python, Arango DB, Elastic Search, Amazon Web Services, Flask.

2. Hierarchical LDA for heterogeneous reviews - A customized version of Guided/Original LDA for Topic Modelling 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) Tech Stack - Python, Topic Modelling, AWS Sagemaker, Flask, Text Analytics.

3. **SubDomainizer - An Open Source intelligence tool (OSINT) for information security**

redBus (Dec'18 - Till Now)

a) Github URL: https://github.com/nsonaniya2010/SubDomainizer

b) Having more than **570 stars and 95 forks** on Github.

c) Given a URL it automatically finds all the JS files (inline & external - in that page) which are prone to contain sensitive information like Secret keys, internal or external subdomains.

d) Based on the regular expression it finds the secrets, domains, firebase URLs, s3 buckets, and other storage services URLs e.g. Azure, RackCDN, Google Cloud services, etc

e) It also does scanning of GitHub that may contain sensitive information, subdomains. Based on the scanning results we can find if any production code is pushed to GitHub.

f) It also does the local folder scanning i.e. given a the root path of the folder, it finds all the files in the folder recursively and reports if any secrets are present in the files.

4. **red:Assassin - A tool to automate API's scanning 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 Stacks - Python, HTML, JavaScript, JIRA.

5. **S3 Bucket scanner - A tool to regularly scan all S3 buckets for mis-configured security policies.**

Other Responsibilities

1. Security fundamentals training to new Joinee's in the organization.
2. Testing new product/features for security vulnerabilities, and help developers in fixing them.
3. Collaboration with developers before starting the project to discuss the security considerations.
4. Taking care of whole information security of the organization.

Internship

Virtual Web Application Security Intern – Crowdin LLC, Ukraine **Dec 2016 - Aug 2017**

The project involved the study of Crowdin website, API & other features and to find security vulnerabilities to secure Crowdin user's data. The results in making user details and data secure by sending detailed reports of the identified vulnerabilities to the developers and they fixed the vulnerabilities in timely manner.

Guide: ***Yuliia Riznyk and Mykhailo Rohalskyy, Customer Success Manger, Crowdin LLC***

Extra-Curricular

- Regularly Participating in Bug Bounty Programs on Hackerone and Bugcrowd.