Saksham Chawla

Application Security

chawla.saksham08@gmail.com

+91-8527889389

linkedin.com/in/saksham-chawla-379218126

medium.com/@chawla.saksham08

I am an experienced **Offensive Pentester** with expertise in Web and API VAPT, Secure Code Reviews, and Secure Design Reviews. Current recipient of the Youth Mobility Scheme Visa, a **UK government-approved and sponsored work permit**.

WORK EXPERIENCE

Security Services Senior Associate Consultant
Synopsys Inc

02/2023 - Present   *Bangalore, India*

Achievements/Tasks

- Co-led in managing and facilitating reviewing of team-wide assessments for a **leading global financial and banking institution** as the **Assistant Team Lead.**
- **Designed and created documentation for training, lookup, and feedback** to help narrow down the understanding of niche client practices and reduce dependencies.

Security Services Associate Consultant
Synopsys Inc

06/2021 - 01/2023   *Bangalore, India*

Achievements/Tasks

- Exploited various instances of missing authentication and authorization, found **race conditions in CAPTCHA validation** leading to mass registration, and discovered **RCE** exploits on default php pages. **Source code disclosure via LFI.**
- Completed **critical time-boxed assessments** to meet last-minute client-escalated expectations for a leading global financial and banking institute. Performed **chained attacks**, **web cache deception** attacks, **abusing SSO** logins and **race conditions** to exploit business logic workflows.
- Worked with various assessors across their engagements to come up with **business impact-oriented CVSS vectors**. Identified client-specific requirements for assessing impact by framing attack scenarios based on **PCI-DSS** compliance, including impact analysis of breach of **MNPI** data confidentiality.
- Analyzed scan logs, proxy history, and attack surfaces to identify potential attack scenarios within **expedited SLA timeframes**. Discovered exploitative scenarios in access-restricted environments. Bypassed WordPress-PHP restrictions on system-execute functions to induce **RCE via RFI** and **self-SSRF**.
- Exploited **SSRF** to build a working POC of a private network port scanner, leading to **AWS S3 instance exposure**.

Senior Associate
Lucideus Technologies

06/2018 - 07/2019   *New Delhi, India*
aka Safe Security

Achievements/Tasks

- Worked with India's top Banks, Aviation, and Insurance companies. Performed application security assessment of **Web**, **Network**, and **Thick client** applications.
- Categorized identified vulnerabilities as per **OWASP Top 10** and **CVSS** standards to define severity. Communicated risks to management and developers.
- Provided code-level fixes and vendor-released patches to mitigate vulnerabilities. Worked with developers to validate and understand the root cause.
- **Conducted workshops** illustrating various exploitation techniques, audit tools, and assessment strategies for developers and client-side teams.

Intern
Lucideus Technologies

04/2018 - 06/2018   *New Delhi, India*
aka Safe Security

Achievements/Tasks

- Built a foundation of the **Owasp Top 10** security risks and penetration testing methodologies.

Intern
Josh Talks

2016 - 2017   *Gurgaon, India*

Achievements/Tasks

- Developed websites and backend using socket.io, MEAN and LAMP stacks.

SKILLS

OWASP Top-10   Whitebox Testing

Blackbox Testing   Secure Code Review

Secure Design Review

Chained web attacks   Race conditions

Abusing SSO   SSRF attacks

Web Cache Deception   RCE via RFI

Sqli and XSS

AWARDS

ACE - Customer Focus Award (11/2022)
Synopsys Inc

- Received **Synopsys "Customer Focus" Award**.

ACHIEVEMENTS

Client Appreciation (03/2023)
*Received client-initiated appreciation spot bonus for **continued effort and support** across their engagements.*

Cert-in Compliance (02/2023)
*Part of the team that **successfully completed "Cert-IN" compliance certification** allowing Synopsys to renew its status as a cyber-security auditor in India.*

CERTIFICATES

Participated in Ethical Hacking Workshop (2014)
*Acquired hands-on experience with **Kali Linux** aka Backtrack.*

PERSONAL PROJECTS

Technical Blog (2019 - Present)
- Published blogs on Thick-Client security.

Malware Detection Tool (2015)
- Heuristic and checksum techniques implemented in Python to **detect a file's degree of deviation** from its ideal behavior.

EDUCATION

Computer Engineering
Master at University of Texas at Arlington

2019 - 2020
(DROPPED)*

Computer Science Engineering
Bachelor in Technology at Jaypee Institute of Information Technology

08/2013 - 06/2017