FLEXMIND

HOW TO BUILD A CAREER IN CYBERSECURITY

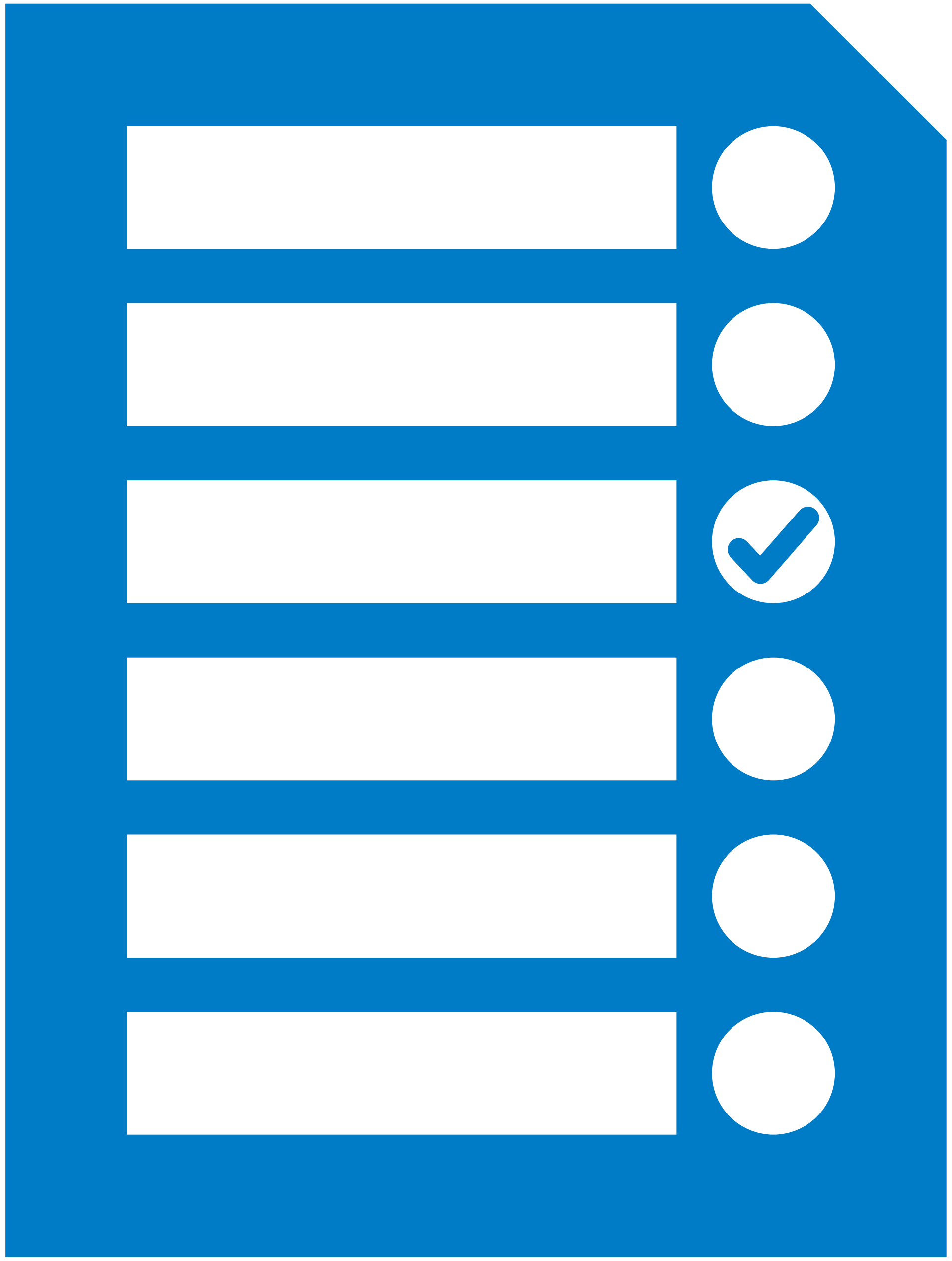
You just need an interest and never give up attitude, rest will fall aside

flexmind.co

Sanjeev Jaiswal (Jassi)

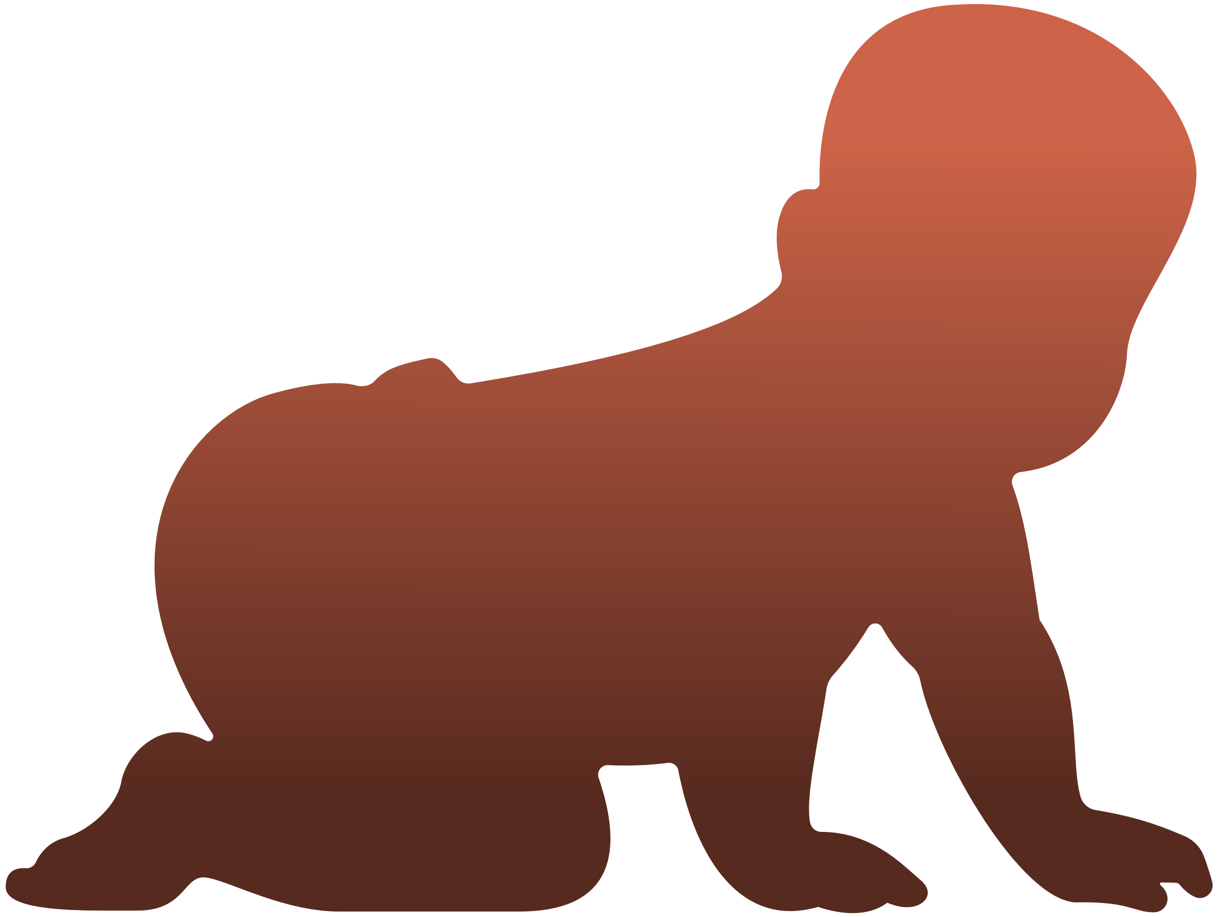
- Working in Epam (Views and data are solely mine)
- Application Security and Cloud Security
- Programming: Perl, Python
- Interested in: DevSecOps and Security Automation
- Twitter: @jassics
- Gmail: jassics[at]gmail
- GitHub: @jassics

What we will cover



- Key Audience
- Job profile categories
- Some known security tools
- Hands-on is the key
- Certifications
- Books
- Online Courses

Key Audience



- College Student/Fresher
- Developer/QA
- DevOps
- System/Network Folks
- Other but interested in Security

Job Profile Categories

- ➤ Web Security
- ➤ Network/Infra Security
- ➤ Application Security
- ➤ Cloud Security
- ➤ DevSecOps
- ➤ Compliance/Audit
- ➤ Mobile App Security
- ➤ Endpoint Security
- ➤ What not?

How to get started (Skills)

- Linux Fundamentals
- Good knowledge of command line tools
- Networking fundamentals (TCP/IP stack)
    - Knowledge of known ports and its applications
- Basics of programming (perl/python/ruby/go)
- Knowledge of Kali tools (Pentest OS based on Linux)
- Keen to explore new technologies …

Web Security

- Understand how different web services work
- Understand request and response (security) headers
- Understand authentication and authorization
- Cookies, tokens, HSTS, httpOnly
- API security
- SOP, CORS, CSP
- OWASP Top 10 (Testing Guide, Code review guide)
- Understand various available encoding i.e. base64
- Comfortable with Burpsuite/OWASP Zap

Network Security

- Secure network architecture
- Firewalls
- Encryption solutions
- Networking commands
- Good with nmap and wireshark tools
- Know IDS/IPS
- DDos prevention
- Aware of CDN implementations

Application Security

- Threat Modeling
- Secure Code design and principles
- Secure Code Review
- Secure-SDL
- Help developers through secure code training
- SAST/DAST
- API security
- git is your friend

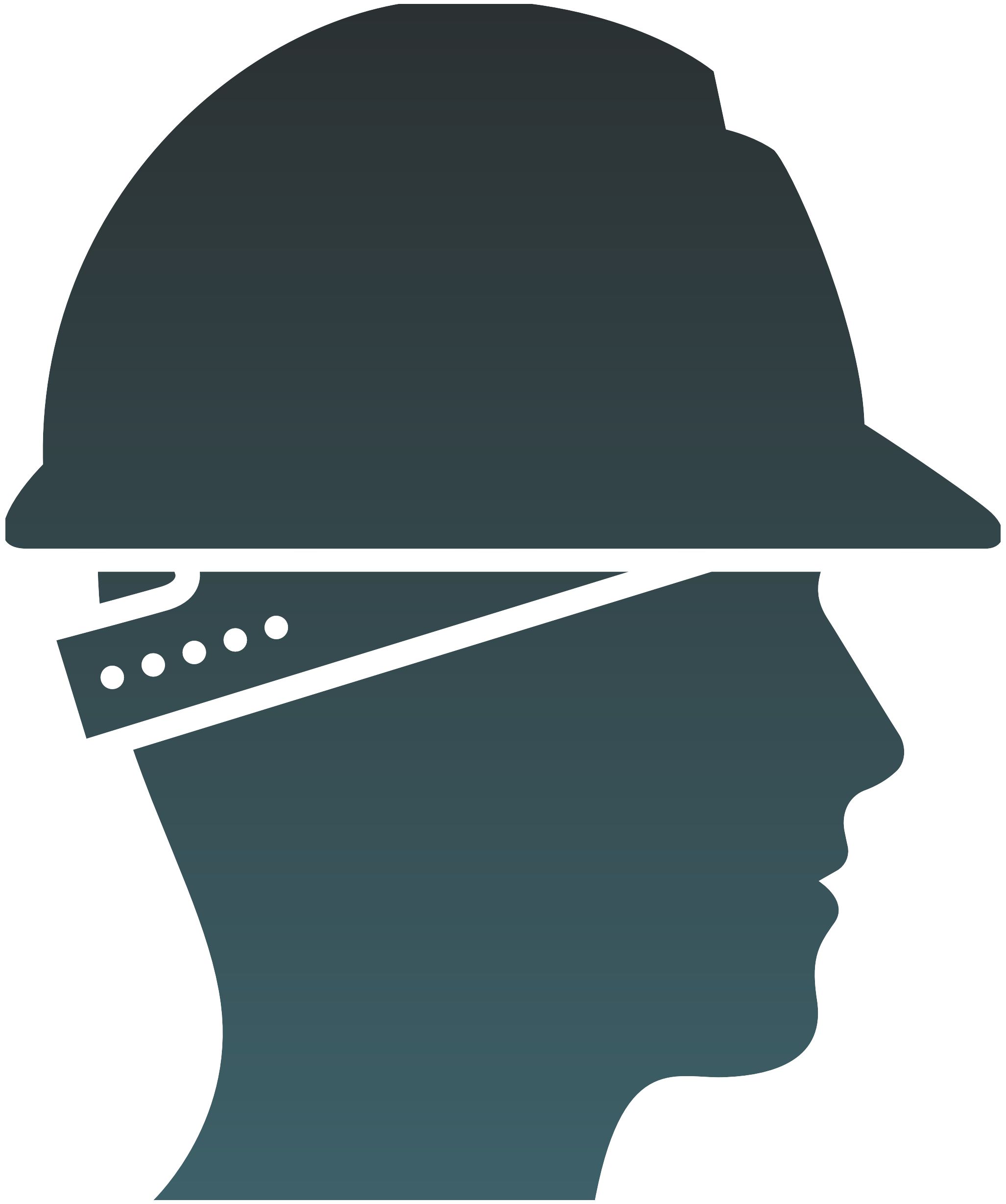
Cloud Security

- Cloud Computing fundamentals
- Security configuration
- Cloud Networking
- Serverless Architecture
- Secure API management
- Data Security
- Encryption at rest, in transit
- Logging and Monitoring

DevSecOps

- Think everything as a Code (Ansible, Terraform)
- You understand DevOps culture
- People, Process and Technology
- Embrace Security Automation
- Comfortable with VCS i.e. git
- Understand CI/CD well
- Well-versed with CI tools i.e. cirlceCI, Travis, Gitlab CI
- Know programming (Python, Ruby, Go)

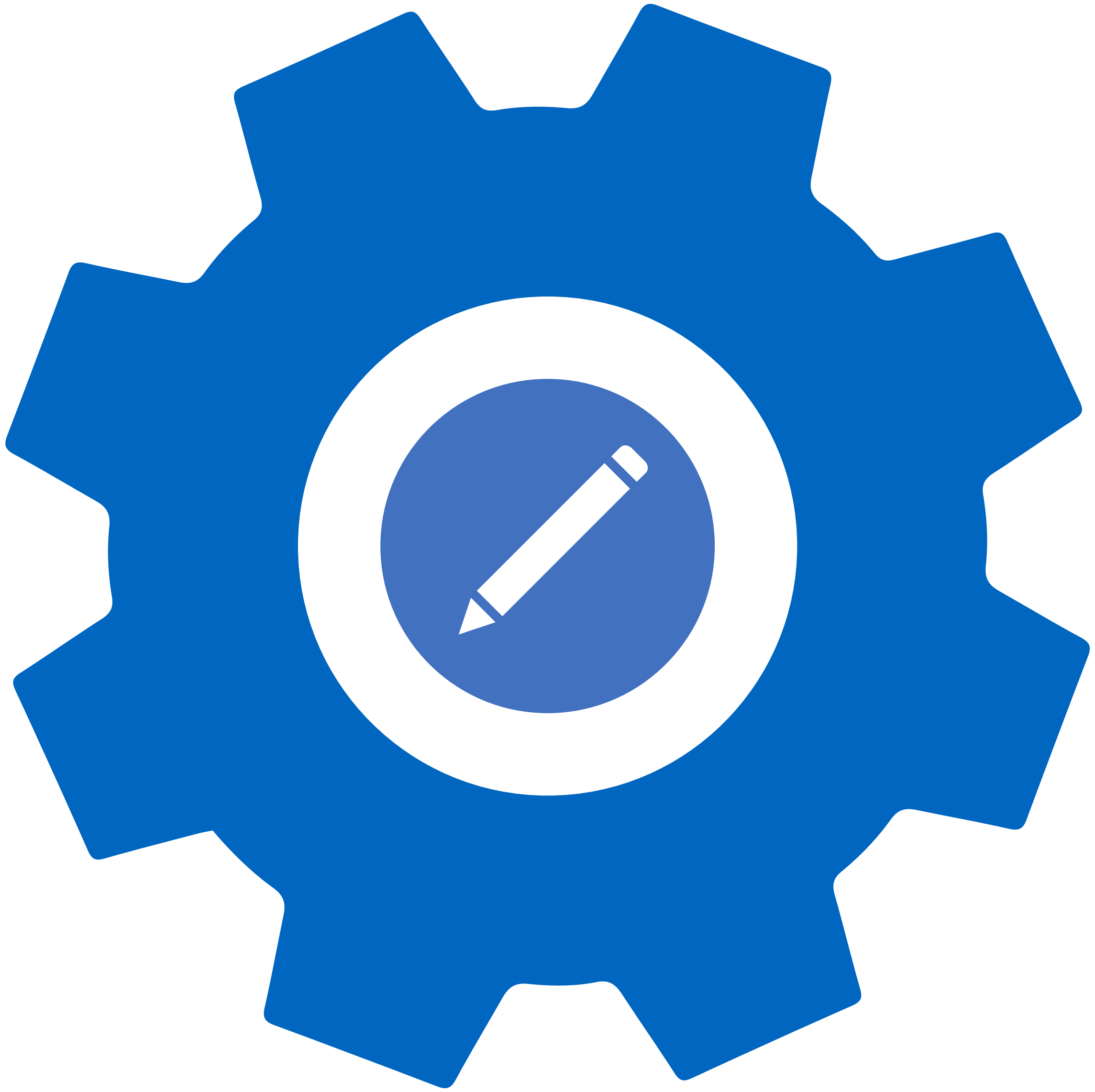
Some known Security Tools



It's just the tip of the iceberg

- Kali Linux
- Burpsuite
- nmap
- metasploit
- aircrack-ng
- nikto
- Hydra
- BeEF
- Frida
- dnsenum
- wireshark
- netcat
- Acunetix
- Qualys
- AppScan
- Contrast
- Nagios
- Cain and abel

Hands-on is the key



- OWASP BWA
- DVWA
- DVNA
- DVIA
- Django.nV
- PentestersLab
- Vulnhub
- Hackthebox

Certifications

- CompTIA
- EC-council
- ISC2
- CSA
- ISACA
- Offensive Security
- Cisco/Checkpoint/Juniper
- Practical-DevSecOps

Books

- ➤ Web Application Hacker’s Handbook (WAHH)
- ➤ *OWASP Guides (Testing, Secure Code review, ASVS)*
- ➤ Writing Secure Code
- ➤ API Security in Action
- ➤ Threat Modeling
- ➤ Violent Python
- ➤ Cryptography & Network Security
- ➤ Mastering AWS Security
- ➤ Securing DevOps

FLEXMIND

CEH Certified Ethical Hacker
CEH Certified Ethical Hacker Practice Exams
CompTIA Security+
CCNA Cisco Certified Network Associate
Todd Lammle
CISSP Official (ISC)² Practice Tests
CISSP Exam Guide
CISSP
Applied Cryptography
Schneier
20th Anniversary Edition
Thinking Security
Bellovin
Modern Authentication with Azure Active Directory for Web Applications
Cryptography Engineering
Ferguson Schneier Kohno
Security What Every Programmer Needs to Know
Dasvani, Kern, Kesavan
Microsoft Azure Security Infrastructure
Cryptography and Network Security
2nd Edition
Forouzan Mukhopadhyay
The Browser Hacker's Handbook
Alcorn Frichot Orrù
The Web Application Hacker's Handbook
Stuttard Pinto
Second Edition
The Mobile Application Hacker's Handbook
Chell Erasmus Colley Whitehouse
threat modeling designing for security
Shostack
Web Application Security A Beginner's Guide
Wireless Network Security A Beginner's Guide
Network Security A Beginner's Guide
Computer Forensics InfoSec Pro Guide
Malware, Rootkits & Botnets A Beginner's Guide
Security Engineering
Anderson
Second Edition
TCP/IP Illustrated, Volume 1
Second Edition
Stevens
Pearson
Perl Best Practices
Mastering Perl
Learning Perl
Intermediate Perl
Programming Perl
Fourth Edition
Christiansen, foy & Wall
Learning Python
Fourth Edition
Lutz
AWS Certified Solutions Architect Official Study Guide
Serverless Architectures on AWS
Design Patterns
Liars & Outliers
Schneier on Security
Secrets & Lies Digital Security in a Networked World
Schneier
Data and Goliath
Bruce Schneier
The Phoenix Project
Gene Kim, Kevin Behr, and George Spafford
Building Microservices
Mastering AWS Security
Pro Git
Chacon
Security Automation with Ansible 2
Modern Python Cookbook
Steven F. Lott
Python for Secret Agents
Python Unlocked
Mastering Data Mining with Python – Find patterns hidden in your data
Cloud Native Python
Manish Sethi
Applied Network Security
Arthur Salmon, Warun Levesque, Michael McLafferty
Building Serverless Applications with Python
Industrial Cybersecurity
Pascal Ackerman
Learning Django Web Development
Sanjeev Jaiswal, Ratan Kumar
Effective DevOps with AWS
Python Penetration Testing Cookbook
WILEY
O'REILLY
PEARSON

Online Courses

- Coursera
- Udacity
- EdX
- Acloud
- Cybrary
- OpensecurityTraining
- Securitytube
- YouTube

Networking is the key

- Null chapter
- OWASP Chapter
- Bsides Chapter
- join mailing list i.e. null google group
- Attend International events i.e. Defcon, Blackhat, Nullcon, Seasides
- jobs.null.co.in for job search
- Meet like minded people i.e. local meetup
- Linkedin contacts, groups
- Follow people in twitter
- Bookmark few security websites

Credits

- Thenoun project
- OWASP projects
- Icons from Apple Keynote
- Quora for analysis

For further queries, please feel free to contact us at ***learning@flexmind.co***