Abdul Mushtaaq

Cyber Security Senior Analyst | OSCP Certified

Email – abdul.mushtaaq@gmail.com

Cell: 919-307-7218

**EDUCATION PROFILE:**

**Master of Science in Information Systems Technologies - Information Assurance Jan 2014 – Aug 2015** Wilmington University, New Castle, Delaware.

**Coursework:** Web and Data Security, Data Communications and Networking, Data Management, Business Intelligence, IT Policy and Strategy, Analysis Modeling and Design, Project and Change Management.

**Bachelor of Engineering in Electronics and Communications Engineering Sep 2008 – June 2012** Osmania University, Hyderabad, Telangana, INDIA

**WORK EXPERIENCE:**

# Cyber Security Sr Analyst, BB&T now Truist, Raleigh, NC June 2016 – Present

* Identified web application security vulnerabilities (e.g., OWASP Top 10) using Automated tools and manual techniques.
* Managed Manual Testing Process for DAST team - Successfully kept the portfolio of Manual DAST scans in regulatory compliance for the year.
* Performed DAST Testing using tools (Burp Suite, Qualys WAS and Whitehat – Sentinel DAST).
* Manual verification of potential vulnerabilities in the web applications.
* Integrated security touch points into existing SDLC processes.
* Creating Proof of Concepts for Application developers.
* Provided detailed report on issues found and remediation for it.
* Provided review and guidance for application security best practices for the applications.
* Worked directly with internal business units and purple team to communicate risk and help resolve open vulnerabilities.

# Cyber Threat Analyst II, Modis Inc, Raleigh, NC April 2016 – June 2016 Client: BB&T now Truist worked as a contractor

* Identified web application security vulnerabilities (e.g., OWASP Top 10) using Automated tools and manual techniques.
* Configured/Performed DAST testing (Burp Suite, Qualys WAS and IBM AppScan).
* Performed DAST testing on API end points.
* Provided detailed report on issues found and remediation for it.
* Provided review and guidance for application security best practices for applications.
* Worked directly with internal business units to communicate risk and help resolve open vulnerabilities.
* Worked on vulnerabilities found on internally hosted Applications which are high priority and providing remediation.

# MPRSoft Inc Systems Engineer Sept 2015 – Apr 2016

* Identified web application security vulnerabilities (e.g., OWASP Top 10) using Automated tools and manual techniques.
* Integrated security touch points into existing SDLC processes.
* Mapping and Network Scanning using Nessus and OpenVAS.
* Prioritizing Critical Vulnerabilities.
* Performed testing on WSDL/WADL/Swagger or other service provided documentation of functionality.
* Vulnerability fixing/Remediation and Reporting.
* Conducted risk assessments, threat modeling and information security reviews on Morningstar systems, applications and platforms.
* Worked directly with internal business units to communicate risk and help resolve open vulnerabilities.
* Worked on creating information security program goals.
* Assisted in maintaining and updating information security policies and standards.
* Provided security remediation advice and training to technical personnel and security champions.
* Developed and enhanced internal security processes, programs and procedures.

# BLUEWARE TECHNOLOGIES AND SERVICES PRIVATE LIMITED

# Application Security Analyst, INDIA Oct 2012 – Oct 2013

* Conducted internal configuration and vulnerability assessments of information systems using commercial and open source assessment tools.
* Identified web application security vulnerabilities (e.g., OWASP Top 10).
* Re-tested remediation of exploitable vulnerabilities.
* Performed manual testing to validate vulnerabilities.
* Monitored security access.
* Performed application security assessments and code review as part of the software development lifecycle (SDLC).
* Identified information system weaknesses and deficiencies.
* Prioritized risk mitigation decisions and associated risk mitigation activities.
* Confirmed identified weaknesses and deficiencies in the information system have been addressed.
* Created detailed, professional documentation/reports that clearly communicate vulnerabilities, mitigation strategies, and remediation steps.

# TECHNICAL SKILLS

|  |  |
| --- | --- |
| Tools  | BurpSuite, Qualys WAS, Sql map, IBM AppScan Enterprise/Desktop, HP fortify, OWASP ZAP Proxy, Nmap, Wireshark, Nessus, Netsparker, Acunetix  |
| Skills  | Web Application PenTest, Network PenTest, API PenTest, Android Application PenTest, Kali Linux and Vulnerability Assessment.  |
| Scripting  | Basic knowledge of Python, Bash, PowerShell, C & C++   |

# ACHIEVEMENTS

* Offensive Security Certified Professional (OSCP) Certified 2020.
* Certified Ethical Hacker (CEH) 2019.
* SIEM – Splunk Fundamentals.
* Second position in Truist advanced CTF 2020 organized by CCS Lab Day Crew.
* Third position in Triangle InfoSecon CTF 2020 organized by Raleigh ISSA.
* Awarded best performance by Cyber Threat Management group hBB&T for 2017 annual review.
* Active member of OWASP Triangle Chapter group.

# Volunteer Experience

* Worked as a volunteer for a Triangle Infosecon 2018-2020.
* Volunteer with the hBB&T light house project:
	+ In collaboration with the Lost Sheep Ministry organization 2019.
* Worked with hBB&T BRG volunteering team 2018-2019.

**PROJECTS:**

**DRIVE TEST and RADIO NETWORK OPTIMIZATION**

* Performed Drive tests and analyzing RF drive test data to evaluate network performance - track out the TCH blocking and other call related problems.
* Analyzing the Post-Processed drive test data after successful completion of drive test.
* Using the results, analysis of the network performance and provide recommendation to improve the quality of network

# Skill Enhancement Platforms

* PortSwigger – Web Security Academy.
* PentesterLab
* HackTheBox
* TryHackMe
* Completed AWS cloud services training.