










## PERSONAL INFORMATION Muhammed M.Abdelkader

 Stockholm, Sweden  
 +46-(0)723996195  
 muhammed.m.abdelkader@gmail.com  
 <https://www.linkedin.com/in/muhammed-muhammed-bassem-80bb3115/>  
 <http://hackerzoneh.blogspot.com/>  
 <https://github.com/muhammedabdelkader>  
 <https://github.com/muhammedmbassem>  
 <https://github.com/Mr0xr3d>  
 Skype muhammed61107

Sex Male | Date of birth 25/10/1988 | Nationality Egyptian

## WORK EXPERIENCE

27/01/2023–Present

### Application Security Engineer - Senior| Product & Application Security

Schibsted Sverige AB, Stockholm (Sweden)

Manage, triage, and investigate Bug Bounty submissions and external pentest findings.

Developed and maintained secure and scalable web applications using technologies such as Go, Python, Java, Node Js, and PHP.

Implemented and enforced secure coding principles, following industry best practices and OWASP TOP 10 guidelines.

Conducted regular security testing, including SAST, DAST, Threat modeling, and code reviews, to identify and address vulnerabilities in the application code.

Collaborated with cross-functional teams during design and architecture reviews, providing security guidance and recommendations to ensure secure application development.

Actively participated in Agile development processes, including sprint planning, daily stand-ups, and retrospectives, to deliver high-quality software within tight deadlines.

Assisted in the creation and implementation of a secure development lifecycle, integrating security practices at each stage of the software development process.

Worked closely with the DevOps team to secure the CI/CD pipeline, implementing security controls such as code signing, vulnerability scanning, and secure artifact management.

Conducted security reviews and code audits, identifying and proposing remediation strategies for vulnerabilities and weaknesses.

Collaborated with product management and engineering teams to prioritize and address security risks, ensuring the overall risk level was reduced.

Developed and delivered training programs on secure coding practices, security awareness, and emerging threats to promote a culture of security among developers and engineers.

Created and maintained security policies, standards, and guidelines, ensuring compliance with industry regulations and customer requirements.

Responded to customer questionnaires and audits, providing detailed information on security practices, policies, and processes.

07/02/2022–27/01/2023

## Security Operation Engineer - Senior | Security Operations

Tink AB, Stockholm (Sweden)

Proactively monitored, investigated, and mitigated security incidents, ensuring the timely resolution of identified issues.

Managed, triaged, and investigated Bug Bounty submissions and external penetration testing findings, facilitating the identification and remediation of potential vulnerabilities.

Actively participated in Agile development processes, including sprint planning, daily stand-ups, and retrospectives, to deliver high-quality software within tight deadlines, while considering security implications.

Assisted in the creation and implementation of a comprehensive secure development lifecycle, integrating security practices at each stage of the software development process.

Conducted in-depth security reviews and code audits, effectively identifying vulnerabilities and weaknesses, and proposing targeted remediation strategies.

Developed and maintained secure and scalable web applications, utilizing a range of technologies such as Go, Python, Java, Node.js, and PHP.

Implemented and enforced secure coding principles, adhering to industry best practices and aligning with the OWASP TOP 10 guidelines to enhance the overall security posture of the applications.

25/08/2019–07/02/2022

## Offensive Security Engineer - Senior | Product Security

Klarna AB Bank, Stockholm (Sweden)

Collaborated with product management and engineering teams to prioritize and address security risks, ensuring the overall risk level was reduced.

Strategically planned and optimized resource utilization to ensure efficient operations.

Conducted comprehensive white-box and black-box penetration testing on both internal and public-facing applications and assets to identify and mitigate security vulnerabilities.

Managed, triaged, and investigated Bug Bounty submissions and findings from external penetration tests, taking prompt actions to address identified vulnerabilities.

Performed variant analysis on identified security issues across all channels, ensuring a thorough understanding of their impact and potential mitigations.

Regularly conducted security testing, including Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), threat modeling, and code reviews to proactively detect and remediate vulnerabilities in application code.

Collaborated closely with cross-functional teams during design and architecture reviews, providing expert security guidance and recommendations to ensure the development of secure applications.

Actively participated in Agile development processes, engaging in activities such as sprint planning, daily stand-ups, and retrospectives to facilitate the delivery of high-quality software within challenging timeframes.

Assisted in the creation and implementation of a robust secure development lifecycle, integrating security practices at each stage of the software development process.

Worked collaboratively with the DevOps team to bolster the security of the CI/CD pipeline, implementing effective security controls such as code signing, vulnerability scanning, and secure artifact management.

Collaborated with product management and engineering teams to prioritize and address security risks, proactively reducing the overall risk level.

Developed and delivered impactful training programs on secure coding practices, security awareness, and emerging threats, fostering a culture of

security among developers and engineers.

Created and maintained comprehensive security policies, standards, and guidelines, ensuring compliance with industry regulations and meeting customer requirements.

Responded to customer questionnaires and audits, providing detailed information on security practices, policies, and processes, ensuring transparency, and meeting compliance obligations.

27/01/2019–01/08/2019

## Cyber Security Consultant - Lead Engineer | Red Team Services

Secure Misr, Cairo (Egypt)

Perform thorough penetration tests on various systems, networks, and applications to identify vulnerabilities and potential security risks.

Conduct comprehensive vulnerability assessments to identify weaknesses in infrastructure, applications, and other digital assets.

Utilize ethical hacking techniques to exploit vulnerabilities and assess the impact on systems and data integrity.

Prepare detailed reports outlining findings, including vulnerability assessments, exploitation techniques used, and recommended remediation steps.

Stay updated with the latest security trends, emerging threats, and industry best practices to ensure effective penetration testing methodologies and techniques.

Assist in developing strategies and recommendations for mitigating identified risks, including implementing security controls and countermeasures.

Work closely with cross-functional teams, including IT and development teams, to ensure effective coordination and communication of penetration testing results and remediation efforts.

Ensure compliance with relevant industry standards, regulations, and frameworks such as PCI-DSS, ISO27K1, and GDPR.

Provide guidance and training to junior team members on penetration testing techniques, tools, and best practices.

Identify opportunities for process improvement and contribute to the development of new tools, methodologies, and techniques to enhance the effectiveness and efficiency of penetration testing activities.

Responded to customer questionnaires and audits, providing detailed information on security practices, policies, and processes, ensuring transparency, and meeting compliance obligations.

01/01/2018–01/09/2018

## Cyber Security Consultant - Assistant Manager | Cyber Risk Services

Deloitte SBA, Cairo (Egypt)

Assisted in providing strategic guidance and recommendations to clients on cybersecurity initiatives, risk management, and compliance.

Conducted comprehensive security assessments, including vulnerability assessments, penetration testing, and security audits, to identify weaknesses and potential risks.

Assisted in designing and implementing security controls and measures to mitigate identified risks and vulnerabilities.

Conducted security incident response investigations, and provided timely and effective recommendations for incident mitigation and recovery.

Assisted in conducting security awareness training sessions for employees to promote a culture of security within client organizations.

Assisted in the development and maintenance of cybersecurity policies, procedures, and guidelines, ensuring compliance with applicable laws and regulations.

Provided guidance on security best practices and emerging cybersecurity technologies to clients, helping them stay ahead of evolving threats.

Assisted in conducting security risk assessments, analyzing potential risks, and recommending risk mitigation strategies.

Kept abreast of the latest industry trends, emerging threats, and regulatory changes to provide up-to-date cybersecurity guidance to clients.

Assisted in managing client relationships, ensuring client satisfaction, and identifying opportunities for further engagement.

01/07/2015–01/01/2018

### Cyber Security Consultant - Experienced Senior | Cyber Risk Services

Deloitte SBA, Cairo (Egypt)

Perform thorough penetration tests on various systems, networks, and applications to identify vulnerabilities and potential security risks.

Conduct comprehensive vulnerability assessments to identify weaknesses in infrastructure, applications, and other digital assets.

Utilize ethical hacking techniques to exploit vulnerabilities and assess the impact on systems and data integrity.

Prepare detailed reports outlining findings, including vulnerability assessments, exploitation techniques used, and recommended remediation steps.

Stay updated with the latest security trends, emerging threats, and industry best practices to ensure effective penetration testing methodologies and techniques.

Assist in developing strategies and recommendations for mitigating identified risks, including implementing security controls and countermeasures.

Work closely with cross-functional teams, including IT and development teams, to ensure effective coordination and communication of penetration testing results and remediation efforts.

Ensure compliance with relevant industry standards, regulations, and frameworks such as PCI-DSS, ISO27K1, and GDPR.

Provide guidance and training to junior team members on penetration testing techniques, tools, and best practices.

Identify opportunities for process improvement and contribute to the development of new tools, methodologies, and techniques to enhance the effectiveness and efficiency of penetration testing activities.

01/07/2014–01/07/2015

### Senior Information Security Specialist | Professional Services

Raya [DC/IT], Cairo (Egypt)

Perform thorough penetration tests on various systems, networks, and applications to identify vulnerabilities and potential security risks.

Conduct comprehensive vulnerability assessments to identify weaknesses in infrastructure, applications, and other digital assets.

Utilize ethical hacking techniques to exploit vulnerabilities and assess the impact on systems and data integrity.

Reporting and Documentation: Prepare detailed reports outlining findings, including vulnerability assessments, exploitation techniques used, and recommended remediation steps.

Ensure compliance with relevant industry standards, regulations, and frameworks such as PCI-DSS, ISO27K1, and GDPR.

01/01/2012–01/07/2014

## Information Security Engineer | Information Security Department

### National Bank of Egypt (NBE), Cairo (Egypt)

Manage and maintain the bank's security infrastructure, including firewalls, intrusion detection/prevention systems, antivirus systems, and other security tools, ensuring their effectiveness and adherence to industry standards.

Monitor the bank's network and systems for potential security breaches or suspicious activities. Respond promptly to security incidents, investigate root causes, and implement appropriate remediation measures to minimize impact and prevent future occurrences.

Conduct regular vulnerability assessments and penetration tests to identify weaknesses in the bank's systems and applications. Collaborate with relevant stakeholders to prioritize and address identified vulnerabilities, ensuring timely patching and mitigation.

Develop and enforce information security policies and procedures in compliance with regulatory requirements and industry best practices. Conduct regular reviews to ensure policy adherence across the bank and provide necessary training and awareness programs to employees.

Participate in internal and external security audits and assessments, ensuring compliance with applicable regulatory frameworks (e.g., ISO 27001, PCI-DSS, NIST). Coordinate with auditors, provide the necessary documentation, and address any identified gaps or non-compliance issues.

Develop and deliver security awareness programs to educate employees on information security best practices, including data protection, phishing prevention, password management, and social engineering awareness.

Collaborate with the bank's IT and development teams to ensure the incorporation of security controls and practices in the design and implementation of new systems, applications, and infrastructure.

Prepare and submit comprehensive reports on security incidents, vulnerability assessments, and risk assessments to senior management, providing insights, recommendations, and actionable steps for enhancing the bank's security posture.

01/10/2010–01/01/2012

## Technical Support | IT Department

### National Bank of Egypt (NBE), Cairo (Egypt)

Provide technical support and troubleshooting for bank applications, including identifying and resolving software defects, configuration issues, and performance bottlenecks.

Create and maintain scripts in Bash and PowerShell to automate routine tasks, improve efficiency, and streamline processes in the bank's infrastructure and application environments.

Analyze code and system logs to diagnose and resolve complex technical issues related to software functionality, data integrity, and system integration.

Respond to and resolve technical incidents reported by bank users, including triaging, prioritizing, and escalating issues as necessary to minimize downtime and ensure timely resolution.

Create and maintain technical documentation, including troubleshooting guides, standard operating procedures, and knowledge base articles, to facilitate effective issue resolution and knowledge transfer.

Ensure compliance with security policies, standards, and regulatory requirements, such as data protection, access controls, and information security protocols, throughout software development and support activities.

## EDUCATION AND TRAINING

01/01/2006–01/01/2010

BSc in Computer Science

EQF level 5

Faculty of Science - Cairo  
University, Cairo (Egypt)

## PERSONAL SKILLS

Mother tongue(s) Arabic

| Foreign language(s) | UNDERSTANDING |         | SPEAKING           |                   | WRITING |
|---------------------|---------------|---------|--------------------|-------------------|---------|
|                     | Listening     | Reading | Spoken interaction | Spoken production |         |
| English             | B2            | B2      | B1                 | B2                | B2      |

|                                  |   |
|----------------------------------|---|
| Communication skills             | <p>Having the Excellent interpersonal and communication skills to share knowledge and to communicate effectively with different backgrounds.</p> <p>Having strong oral and written communication, organization, and interpersonal skills. Ability to translate complex findings into interpretable and simple output.</p>   |
| Organizational/managerial skills | <p>Strong people management and leadership, Operational Control (operating); Experience leading both a services organization and product development function; Developing Business Strategy and providing Technical Thought leadership; Managing customer engagements escalations to ensure customer satisfaction; Expert understanding of technology and security principles and possessing knowledge of the cyber threat landscape; Expert in leading penetration testing and vulnerability assessment engagements for large enterprise firms.</p>  |
| Job-related skills               | <p>Expert in tailored reconnaissance, exploitation, and lateral movement. Strong knowledge of attack surfaces for common enterprise systems and services.</p> <p>Be able to independently apply testing methods against a wide variety of targets including Web Applications, Mobile Applications, Web APIs, databases, wireless networks, conducting social engineering attacks against customer user base, routing infrastructure, VOIP, and VPN.</p> <p>Perform secure code review. Writing fully functional exploits for common vulnerabilities such as simple stack overflow, cross-site scripting, or SQL injection.</p> <p>Strong knowledge in scripting. Good experience with SIEMs (Splunk)</p> <p>Excellent experience with AWS &amp; GCP. Writing security tools (Golang, Python, Java, and PHP)</p> |

## ADDITIONAL INFORMATION

## Certifications

Offensive Security Certified Expert (OSCE)

Offensive Security Certified Professional (OSCP)

ISO 27001:2013 Lead Auditor Certification (BSI 2013)

GSEC (General Security Essentials Certificate) SANS License 32754

Certified Red Team Professional (CRTP)