Kareem Ahmed

Penetration Tester

Email : karimahmed011161@gmail.com | GitHub : karim306 | LinkedIn: www.linkedin.com/in/kareemahmed306 | Egypt | phone : +201116176831

OBJECTIVE

I am a penetration tester specializing in web and API security, automation, and network security. I possess hands-on experience with platforms like Hack The Box and TryHackMe, along with active participation in bug bounty programs. I am proficient in programming with Bash and Python, and have published my security research on LinkedIn and Medium

EDUCATION

Bachelor’s Degree in Computer Science

Ain Shams University

SKILLS

Penetration Testing,Security Assessment,Web Applications,APIs,Authentication,OWASP Top 10,SQLi,XSS,CSRF,SSRF, Burp Suite,OWASP ZAP,Nmap,Metasploit,Nikto,Gobuster,Python,Bash,JavaScript Node.js),API Security,JWT, Session Management,Access Control,TCP/IP,Firewalls,Network Security Fundamentals,Vulnerability Research,Exploitation, CTFs,Exploit Development,Security Scripting

Bash,Burp Suite,Cybersecurity,Encryption,GitHub,JavaScript,JWT,MongoDB,Metasploit,Nikto,Nmap,OWASP,Pentesting, Python, SQL, Node.js, Express.js, Gmail, TCP

EXPERIENCE

Backend & Security-Focused Developer

GitHub Contributions & Personal Projects

Focus on Backend & Security-Focused Development

•Developed secure authentication systems in Node.js, implementing best practices for session management and API security
•Built security-focused applications integrating access control, token-based authentication, and encryption

API Security Testing Project

•Performed security assessments on test APIs using **Burp Suite, Postman, and OWASP ZAP**. •Identified vulnerabilities like **Broken Authentication, Excessive Data Exposure, and Insecure Direct Object References IDOR** .

Penetration Tester & Security Researcher

Self-Driven

Published Work on LinkedIn & Medium

•Conducted web and API pentesting, exploiting vulnerabilities and publishing security assessments •Solved numerous Hack The Box, TryHackMe, and PortSwigger challenges, focusing on real-world exploitation

PROJECTS

OWASP Juice Shop Pentesting & Report

A project focused on identifying web vulnerabilities in a known application and sharing the results

•Conducted a comprehensive penetration test on OWASP Juice Shop, identifying and exploiting OWASP Top 10 vulnerabilities such as SQL Injection, XSS, Broken Authentication, and IDOR
•Documented findings in a detailed security report on Medium, including attack techniques, exploitation steps, and remediation strategies

Simple Authentication App

A secure login system designed to enhance security in application authentication

•Developed a secure authentication system using Node.js, Express.js, and JWT
•Implemented role-based access control RBAC , password hashing with bcrypt, and session management, following best security practices for authentication and user authorization

Secure Movie Store

A web application focused on securely handling user data and transactions

•Built a secure movie store application using Node.js and MongoDB, focusing on API security and access control
•Integrated authentication mechanisms, including JWT-based authentication, input validation, and request authorization to prevent common web vulnerabilities