

HAIDER MAHMOOD (OSCP)

Mobile # +966535848680

Email: haidermehmoodqureshi@yahoo.com

LinkedIn: <https://www.linkedin.com/in/haider-mahmood-5b755873/>

Summary:

I have 6 years of experience in Penetration Testing working with Multinational clients across countries both in public and private sector specializing in ICT, Telecommunication and Financial Services (List of projects to be provided upon request). I am Offensive Security Certified Professional and did Bachelors in Computer Sciences.

Core Expertise:

- Penetration Testing and Mitigation for OWASP Top 10.
- End to end implementation of Secure SDLC.
- Mobile Application Penetration Testing and Vulnerability Mitigation.
- Security testing and hardening of Linux and Windows operating systems.
- Architecture and Design Review for multi-Tier environments.
- Source Code Review (Manual & Automated).
- Wireless Security Testing.
- Application Threat Modeling.
- Social engineering.
- Programming and Scripting automation (PHP, C#, Python, BASH).

Tools and Standards

Tools: Kali-Linux, Metasploit, Nmap, SQLmap, SET, Wireshark, Burpsuite, Hydra, Aircrack-ng, Nikto, Hashcat, Android simulator, OpenVAS, Nessus, Nexpose, IBM Appscan, Acunetix, Qradar, BigIP-F5, Cloudflare.

Standards: OWASP Top 10 , SANS Top 25, NIST, CIS.

PROFESSIONAL EXPERIENCE

Penetration Tester (Advance Electronics Company – Feb 2016 – Present)

- Participating in Security Architecture for a National level project. The project has a user base of 9 million.
- Continuous Penetration testing for infrastructure, website and mobile applications.
- Introduced Secure Software Development Life Cycle (SSDLC), to have security induced in each phase of Software Development Life Cycle.
- Development of Operational Security Policies/Procedures/Guidelines.
- Introduced customized Application Threat Modeling for better application security visibility.
- Continuous developing of detailed Application security requirements for developers to follow for secure Development.
- Coordination with design & development team for mitigation of security issues identified.



شركة الإلكترونيات المتقدمة
Advanced Electronics Company

Advanced Electronics Company
شركة الإلكترونيات المتقدمة

Information Security Analyst at Trillium Information Security Systems (April 2015 – Nov 2015):

- Penetration Testing Critical Credit card Payment System.
- Web and mobile application and Infrastructure vulnerability assessment and penetration testing for Telecom and Financial Services companies.
- Source code Analysis Manually as well as using automated tools for potential vulnerabilities.
- Documenting vulnerabilities and coordinating with respective teams till fixation.
- Developing detailed Application security requirements for developers to follow for secure Development.



trillium Information Security Systems

شركة إلكترونيات التريليوم

- Setup internal tasks for vulnerability research and learning purposes.

Penetration Tester (Elance Jan 2013 – Aug 2015):

- Web Application Penetration Testing and vulnerability Assessment.
- Incident response, forensics and Malware mitigation.
- Security assessment for endpoints.
- Procurement of offensive surveillance tools for clients.



PROFESSIONAL ACHIEVEMENTS

Rewarded and Acknowledged by Facebook

Reported vulnerability in Facebook Mobile Website under their bug bounty program, got rewarded for responsibly disclosing the issue. Name was mentioned in Facebook Hall of fame for Security Researchers. Link below:-

Reference: <https://www.facebook.com/whitehat/thanks>



Twice Acknowledged by Microsoft

Reported several vulnerabilities to Microsoft in multiple projects. Microsoft mentioned me in Hall of Fame for Security Researchers.

Reference: <http://technet.microsoft.com/en-us/security/cc308589>



Twice Rewarded by Yahoo

Yahoo rewarded me twice for reporting multiple vulnerabilities.

Reference: <https://hackerone.com/haiderm>



Acknowledged by Adobe

Adobe acknowledged me in their Hall of fame for security researchers for reporting vulnerability in their online infrastructure.

Reference: <http://www.adobe.com/support/security/bulletins/securityacknowledgments.html>



1st Position at Capture The Flag Hacking competition at CSP

Got 1st position at Capture The Flag hacking competition organized by Cyber Secure Pakistan (CSP) in Islamabad.

1st Position at Attack-Secure Penetration Testing Competition

Got 1st Position in Capture The Flag Hacking competition organized by Attack-Secure.

CERTIFICATIONS AND TRAININGS

Offensive Security Certified Professional (OSCP)

Offensive-Security



Attack-Secure Penetration Testing Training

Attack-secure.com



EDUCATIONAL QUALIFICATIONS

Bachelors in Computer Science

COMSATS Institute of Information Technology, Islamabad

PROJECTS

Malicious Activity Honeypot Analyzer

Developed a web application honeypot and reporting system in PHP, MYSQL and third party API's. Web application contains several vulnerabilities deliberately left in them having different levels of severity, which allures the attacker to attack them, as they attack the Honeypot their activities are being recorded. Sandboxing is being done mostly on the server side for caging the attacker in a safe environment. Threat Intelligence reports and feeds are then generated from attack logs.

TRAININGS AND CONFERENCES

- Honorable Guest Speaker at National University of Computers and Emerging sciences (FAST-NUCES) on the topic of "Introduction to Application Security testing and Bug Bounties".
- Attended Cyber Secure Pakistan Conferences 13, 14 & 15.
- Attended Pakistan Freelance conference by Elance.
- Attended Software testing and Quality Assurance workshop organized by Bentley Systems.
- Took "Penetration testing with Kali Linux" Training by Offensive security.