MUHAMMAD HASSAN KHAN

Security Engineer | Penetration Tester | OSCP

923226562081
hassankhan14044@outlook.com
https://hassankhanyusufzai.com
Lahore, Pakistan

EXPERIENCE

Security Engineer

Sendoso

03/2019 - Ongoing Lahore, Pakistan

Sendoso, the leading Sending Platform, helps companies stand out by giving them new ways to engage with customers throughout the buyer's journey.

- Pen-testing Web Application, browser extensions and networks
- Develop various security tools and exploits for penetration testing
- Write automation scripts in bash & python
- Presenting and documenting detailed findings and fixes based on the testing
- Pen-testing and Patching rails specific vulnerabilities
- Deliver security awareness sessions
- Train developers & QA team regarding security.
- Participate in CTFs & bug bounties

Penetration Tester

Independent / Freelancer

2017 - Ongoing

- Almost 4 Year of experience in Web Application Penetration Testing
- Acknowledged by and listed in Researchers' Hall of Fame of many well-reputed companies including Google, Microsoft, Magento, Indeed, Walmart, Netgear, eBay, Sony etc
- Often Participated in CTF's VulnHub, HacktheBox and Hacker101
- Successfully participated and reported vulnerabilities in Private Bug Bounty Programs of 100+ Companies
- Black Box Pen-testing, VAPT, Bug Hunting, Red teaming

Security Researcher

HackerOne / Bugcrowd

2017

https://bugcrowd.com/Splint3r7

- Reported bugs to different companies and received Hall of Fames and monetary payouts
- Ranked Under Top 100 Hackers on Bug-crowd
- Found 200 Bugs in 85 companies & Acknowledged by 60 companies

INTERNATIONAL PROJECTS

Penetration Testing Project

Company / Confidential

07/2018 - 09/2018 Bangkok, Thailand

- 2 months of the project where I learned how to work in Red teaming & attend professional meetings.
- Gained a lot of experience in Penetration Testing as well as personal growth.
- Did Vulnerability Assessment (VAPT) of Web, Android projects and Black Box Pen-testing

SUMMARY

Self learned Security Researcher and Penetration Tester with extensive knowledge of Bug Hunting. Good Understating of Web Applications and Networks. Apart from professional experience, have a deep passion and diligence for hacking, finding new bugs and vulnerabilities.

EDUCATION

BS (Computer Science)

Virtual University of Pakistan

2015 - 2019

GPA **3.4** / 4.0

- Courses of Interest: Programming C & C , Algorithms, Operating system, Web Technologies & languages.

Intermediate (ICS)

Punjab Group of Colleges, Lahore

2013 - 2015

- Courses of Interest: Computer, Physics, mathematics.

ACHIEVEMENTS

MVP Security Researcher

Achieved the title of MVP Hacker on Bugcrowd for identifying 200 valid bug reports.

Acknowledged by 100+ Companies

Acknowledged by 100+ Companies for reporting them severe vulnerabilities that includes Google, Microsoft, FoxyCart, OnePageCRM, GogoAir, Quizlet etc

Won 1st Prize of Hack-fest Competition at GeekWeek'18

Hack-fest was a hacking competition organized by FAST University at GeekWeek'18

LANGUAGES

Urdu
Native

English
Proficient

INTERNATIONAL PROJECTS

Penetration Testing Project

Company/Confidential

08/2018 - 09/2018 Kathmandu, Nepal

- 2 months of projects Where I learned how to collaborate with Hackers/Researcher around the globe for the success of the project, ton of tips and tricks from Security enthusiast geeks
- Handled Web and Android Penetration Testing Projects

CERTIFICATION

Offensive Security Certified Professional (OSCP)

OSCP is by definition capable of identifying existing vulnerabilities and conducting organized attacks writing simple Bash or Python scripts, modifying the existing exploit code to its advantage, performing network pivoting and data ex-filtration & filter bypassing and cracking poorly written applications in rails, PHP, java, .NET

https://www.offensive-security.com/pwk-oscp/

eLearnSecurity Junior Penetration Tester (eJPT)

eJPT by definition is one who can pentest web applications and networks using automated vulnerability scanners as well by manual testing, pivot networks, exploit critical vulnerabilities in the network, holds essential knowledge networking.

https://www.elearnsecurity.com/certification/ejpt/

PUBLICATIONS

Remote File inclusion to local file read

Hassan Khan

http://hassankhanyusufzai.com/RFI_LFI_writeup/

The article explains how attacker can access to local files of the servers if parameter is directly pass in file open functions.

Account Take Over Vulnerability in Google acquisition

Hassan Khan

shorturl.at/uMOT7

CSRF to account take over vulnerability identified in one of the Google's acquisition.

HALL OF FAME

Google	*Indeed*	*Ebay*
Microsoft	*Walmart*	*Ali baba*
Upwork	*Bugcrowd*	*Intel*
Fad at-Media	*Quizlet*	*E-set*

FIND ME ONLINE

LinkedIn
hassankhanyusufzai

Twitter
Splint3r7

TRAINING / COURSES

Pen-tester Academy JavaScript for pen-testers

Pen-tester Academy python for pen-testers

Burp Suite Mastery

SKILLS

Python, Bash Shell Scripting, JavaScript, Rails

Languages

Nmap, Metasploit, BurpSuite, Sqlmap, Wireshark, Nexpose, Nikto, Acunetix

tools

Information Security, Penetration Testing, Vulnerability Assessment, Linux Administration, Security Research

Fields of interest

INDUSTRY EXPERTISE

Web Application Penetration Testing

Network Penetration Testing

Mobile (Android/IOS) Penetration Testing

Development PHP, Ruby on rails

Problem Solving