Mazin Ahmed

Cyber Security Engineer (Offensive Security)

Email: mazin@mazinahmed.net **Phone Number:** +971.50.602.1337

Summary

I'm one of those people who turned their hobby into a profession. My expertise is in security engineering, with a focus on web-application security, DevSecOPs, and offensive security.

I enjoy building secure systems and developing security tools to help in automating work and solving problems.

I have worked on a variety of projects and roles within my years of experience, including security research, security engineering, penetration testing, red-teaming, as well as leading major security projects within organizations I have worked for.

I have also built a security start-up, FullHunt.io, a highly-scalable automated assets discovery, monitoring, and scanning platform that helps companies understand their external attack surface and monitor them for security risks.

Furthermore, I have participated in bug bounty programs, where I reported security vulnerabilities to high-profile companies, organizations, and entities around the world, such as the U.S Department of Defense, Facebook, Twitter, Oracle, and LinkedIn to name a few. I have also received security awards in different competitions I have participated in and won.

I present my security research and experiments regularly on security conferences, where I have spoken at Hack-In-The-Box, SwissCyberStorm, OPCDE, and OWASP conferences.

Technical Specialties

- Offensive security experience, running penetration testing and red-teaming engagements.
- Experience with cloud platforms, including Amazon AWS, Google Cloud, and Microsoft Azure.
- Deep knowledge in security automation and developing security automation on scalable levels.
- Extensive knowledge with web-application security.
- Knowledge in mobile-application security.
- Mature abilities in identifying and fixing security holes on applications and systems.

Key Achievements

- Received security acknowledgments and "hall of fame" entries for reporting security vulnerabilities that affected top-profile companies, organizations, and entities, such as the U.S Department of Defense, Facebook, Twitter, Oracle, and LinkedIn.
- Conducted independent security research, named "Evading All Web-Application Firewalls XSS Filters" that received the 4th place at Top Ten Web Hacking Techniques of 2015 award.

- Wrote security tools that are used by thousands of security professionals around the world.
- Host the security podcast, HackBack, where I talk about highlights and insights of security events in multiple languages.
- Actively contribute to Open-Source Software that is related to my work.
- Built successful security programs and led several security projects within my job.
- Holds a number of registered CVEs for reporting security vulnerabilities, such as: CVE-2014-9414, CVE-2017-7320, CVE-2017-7321, CVE-2017-7322, CVE-2017-7323, and CVE-2017-7324.
- Developed reliable public exploit codes and tools for critical security vulnerabilities, such as: CVE-2017-5638, CVE-2017-9805, and CVE-2017-12616.
- Conducted research on the CVE-2014-9414 vulnerability, where it was nominated for the Pwnie Awards of 2015 for the "Best Client-Side bug of 2015".
- Ranked in the top 10 security researchers of Bugcrowd in 2014.
- Have spoken in security conferences, including HITB, OPCDE, and SwissCyberStorm.
- Maintain a blog where my security researches are shared.
- Obtained a full scholarship for studying a bachelor's program in Computer Science based on my work.

Experience

Security Consultant at **Namshi (Emaar-acquired company)**

March 2019 – March 2020

- Developed the company's security program.
- Was responsible for engineering and compliance projects after the Emaar acquisition.
- Worked in establishing DevSecOPs within the company.

Security Consultant at **ProtonMail**

July 2017 – January 2019

- Worked at the ProtonMail security engineering team.
- Conducted frequent security audits on the company's applications.
- Developed security and threat-intelligence projects for ProtonMail.
- Was responsible for managing the ProtonMail bug bounty program.

Founder at FullHunt.io

December 2016 – Present

FullHunt.io is a security startup that I built. FullHunt.io is a highly-scalable automated assets discovery, monitoring, and scanning platform that helps companies understand their external attack surface and monitor them for security risks.

Security Researcher at **Bugcrowd Inc**

December 2013 – March 2017

- Identified security vulnerabilities in different companies, and reported it to vendors responsibly.
- Communicate with developers, and provide solutions for the vulnerabilities.
- Ranked in the top 10 security researchers of Bugcrowd in 2014.

Freelancing Security Researcher at **Bug Bounty Programs**
December 2013 – March 2017

- Participated in numerous bug bounty programs.
- Identified severe security vulnerabilities in major companies, such as: Facebook, Twitter, Oracle, and Linkedin to name a few.
- Wrote articles about some of the findings.

Penetration Tester at **Defensive Security**
April 2014 – October 2014

- Led the penetration testing team of the company to provide better services, covering new web-application testing techniques.
- Performed advanced penetration tests to major companies and organizations.

Volunteer Experience

Security Contributor - Member of ProtonMail's Security Group at **ProtonMail**
July 2014 - July 2017

I was an active contributor to ProtonMail, the world's top end-to-end encrypted email service. I provided security assessments for new builds, helping in providing ideas for future builds, and identifying every single weak aspect before bad people do.

Honors and Awards

U.S Department of Defense – Security Acknowledgment
U.S Department of Defense
Responsibly disclosed several severe vulnerabilities in the U.S Department of Defense systems. vulnerabilities have been acknowledged and patched by the Department of Defense.
https://hackerone.com/reports/195544

Facebook WhiteHat
Facebook
Reported a Cross-Site Scripting vulnerability on one of Facebook's services.
https://www.facebook.com/whitehat/thanks

Twitter Security Acknowledgement
Twitter
Reported multiple critical vulnerabilities responsibly to Twitter Security.
https://hackerone.com/twitter/thanks

Oracle Security Acknowledgement
Oracle
Responsibly disclosed a critical XSS on one of Oracle's services.
http://www.oracle.com/ocom/groups/public/@otn/documents/webcontent/2188432.xml

Hack In The Box 2019 – AI Competition – Finalist
Hack in The Box
Hack in the Box (HITB) AI competition is a 2 months-duration competition where companies and universities compete in building an offensive security project that utilizes Artificial Intelligence in performing target exploitation. Our team reached the finals for our project, Shennina, a fully-automated host exploitation and post-exploitation tool that uses AI for predicting the best exploit against the target.

Pwnie Awards – Best Client-side Bug of 2015 – Nominator
Pwnie Awards
The finding of CVE-2014-9414, W3 Total Cache CSRF that leads to total defacements of websites has been nominated for the best client-side bug of 2015 in Pwnie Awards. The award is given to the person who discovered or exploited the most technically sophisticated and interesting client-side bug.
http://pwnies.com

Top Ten Web Hacking Techniques of 2015 – 4th Place
Top Web Hacking Techniques Award
The research of "Evading All Web-Application Firewalls XSS Filters" has received the fourth place on Top Web Hacking Techniques of 2015 award. The award is given to acknowledge and reward the hard work of the most influential researches done by security researchers.
http://www.darkreading.com/endpoint/top-10-web-hacking-techniques-for-2015-/d/d-id/1325281
https://www.whitehatsec.com/blog/top-10-web-hacking-techniques-of-2015/

ABN AMRO Bank Security Acknowledgement
ABN AMRO Group
Reported multiple critical vulnerabilities on ABN AMRO Bank online services.

Sudanese Higher-Education Championship 2017 - 1st Place
Ministry of Higher-Education – Sudan
Won 1st place on the Sudanese Higher-Education Championship.

LinkedIn Security Acknowledgement
Linkedin
Reported multiple critical security vulnerabilities on LinkedIn services.

Mozilla Hall of Fame - Q4 2014
The Mozilla Foundation
Discovered a critical security vulnerability on Mozilla blog that could allow a full defacement of Mozilla blog via an exploit I previously wrote.
https://www.mozilla.org/en-US/security/bug-bounty/web-hall-of-fame/

ProtonMail's Hackathon 2nd Place
ProtonMailI
I got second place in ProtonMail's first hackathon in August 2014. I have also earned the "Artisan" award for performing the most creative attack resulting in a bug found, and "Shotgun" award for disclosing the most amount of bugs.
https://protonmail.ch/hackathon/

Adobe Security Competition Winner
Adobe
Adobe made a private security competition in May 2015. It was made with the partnership of Bugcrowd platform. I have won 3rd place in the competition.

Ebay Security Acknowledgement
Ebay
Reported various vulnerabilities on Ebay's services and Magneto Web-App.
http://ebay.com/securitycenter/ResearchersAcknowledgement.html

Yandex Security Acknowledgement
Yandex
Acknowledged by Yandex for reporting security issues on their DNS implementations.
https://yandex.com/bugbounty/hall-of-fame/2016/6/

Symantec Wall of Fame
Symantec
Responsibly disclosed a number of security vulnerabilities that affected Symantec web services.
https://www.symantec.com/connect/pages/security-researcher-wall-fame

Sony Hall of Fame
Sony
Reported a security issue that affected one of Sony's services.
https://secure.sony.net/hallofthanks

ESET Security Acknowledgement
ESET
Received an acknowledgment from ESET for reporting security vulnerabilities that affect one of their services.
https://mazinahmed.net/uploads/ESET_Acknowledgement.png

Languages

Arabic	**English**
(Native proficiency)	(Professional working proficiency)

Researches

Practical Approaches for Testing and Breaking JWT Authentication
Research on possible attacks against JWT stateless authentication protocol.
https://mazinahmed.net/blog/breaking-jwt/

Evading All Web-Application Firewalls XSS Filters
A whitepaper that documents shortcomings in various popular web application firewalls (WAFs) and how to trigger cross site scripting attacks regardless of the protections in place. Covered products are F5 Big IP, Imperva Incapsula, AQTRONIX WebKnight, PHP-IDS, Mod-Security, Sucuri, QuickDefense, and Barracuda WAF.
http://blog.mazinahmed.net/2015/09/evading-all-web-application-firewalls.html

Backup-File Artifacts: The Underrated Web-Danger
Research on backup-file artifacts, and how it impacts websites security.
http://blog.mazinahmed.net/2016/08/backup-file-artifacts.html

Summary of HSTS Support in Modern Browsers
Research on implementations of HSTS policy in modern browsers.
https://protonmail.com/blog/summary-of-hsts-support-in-modern-browsers/

Projects

BFAC
BFAC (Backup File Artifacts Checker) is an automated tool that checks for backup artifacts that may disclose the web-application's source code. The artifacts can also lead to leakage of sensitive information, such as passwords, directory structure, etc.
https://github.com/mazen160/bfac

HackBack Podcast
HackBack is an offensive security podcast that discusses security highlights and insights, delivered in English and Arabic. The idea of HackBack is to have a podcast that discusses various security topics while focusing on technical insights.
https://mazinahmed.net/hackback/

Xless
Xless is a serverless Blind XSS (bXSS) application that can be used to identify Blind XSS vulnerabilities.
https://github.com/mazen160/xless

Server-status pwn
A tool that monitors and extracts requested URLs and clients connected to the service by exploiting publicly accessible Apache server-status instances.
https://github.com/mazen160/server-status_pwn

JWT-pwn
Security testing scripts for JWT.
https://github.com/mazen160/jwt-pwn

Firefox Security Toolkit
A tool that transforms Firefox browsers into a penetration testing suite.
https://github.com/mazen160/firefox-security-toolkit

More projects can be found at: https://github.com/mazen160

Education

Future University – Bachelor of Computer Science
2015 – 2019

- Studied a Computer Science bachelor program.
- Represented the university in local technology competitions.
- Obtained a full scholarship based on my work.

SMA Secondary School
2014 – 2015
Obtained a secondary education diploma.

St. Catharine's Collegiate
2013 – 2014

Code Academy
2012 – 2014
Web-Development Languages.

Interests

Mixed Martial Arts, Olympic Wrestling, Soccer, Badminton, Traveling, Trying new things, Reading.

References

Available upon request.