Mazin Ahmed

Information Security Specialist / Penetration Tester

Email: mazin@mazinahmed.net **Phone Number:** +971506021337

Summary

Mazin is one of those people who turned their hobby into a profession. His expertise is on Information Security in general, and Web-Application Security in specific.

Mazin is self-motivated, adaptable to new situations and responsibilities, and able to work in fast-paced environments. He works effectively both as a team member and independently. He always has positive and professional attitude, and committed to excellence in his tasks.

In his spare time, Mazin participates in security competitions and bug bounty programs to help projects and companies to enhance their security, and to help building secure applications. Also, he likes to read books that are related to computer-security and software-development.

Being a penetration tester for a long time has gained him skills that make him one of the top security professionals in the field. Mazin has been listed in numerous Hall of Fames on top-profile companies, such as Facebook, Twitter, Linkedin, and Oracle to name a few. You can check the "Honors & Awards" section for detailed information about some of the acknowledgments that he has received.

Technical Specialties:

- Extensive experience with Web Application Security.
- Deep knowledge in Network and Network Security.
- Mature abilities in identifying and closing security holes.
- Familiar with web-developing languages.
- Deep knowledge in Server Security.

Key Achievements:

- Received security acknowledgements 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 an 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.
- Ranked in the top 100 security researchers around the world at Bugcrowd.
- Conducted a 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".

- Wrote security tools that are used by thousands of security professionals around the world.
- 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.
- Maintains a blog where security-related resources are shared.
- Obtained a full scholarship for studying a bachelor program of Computer Science based on his work.

Experience

Security Consultant at **Namshi (Emaar-acquired company)**
March 2019 – Present

- 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.

Security Researcher at **Bugcrowd Inc**
December 2013 – Present

- Identifies security vulnerabilities on different companies, and reports it to vendors responsibly.
- Communicates with developers, and providing solutions for the vulnerabilities.
- Ranks in the top 200 out of 100,000+ security researchers around the world.

Freelancing Security Researcher at **Bug Bounty Programs**
December 2013 – Present

- Participates on numerous number of bug bounty programs.
- Identifies critical vulnerabilities in major companies, such as: Facebook, Twitter, Oracle, and Linkedin to name a few.
- Writes articles about some of the findings.

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

Security Tester at **ICE Coder**
March 2014 – May 2014
Volunteered in helping the developers of ICE Coder project to build a secure application.
Project's website: https://icecoder.net

Honors and Awards

U.S Department of Defense – Security Acknowledgment
US. Department of Defense
Responsibly disclosed a number of severe vulnerabilities on US. 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 into building 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
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
I won the 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 have got the 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 has made a private a security competition on May, 2015. It has made with partnership of Bugcrowd platform. I have won the 3rd place on 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 acknowledgement from ESET for reporting security vulnerabilities that affects 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
A 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
A 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
A 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…
Project's Homepage: https://github.com/mazen160/bfac

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.
Project's Homepage: https://github.com/mazen160/server-status_PWN

JWT-pwn
Security testing scripts for JWT.
Project's Homepage: https://github.com/mazen160/jwt-pwn

Firefox Security Toolkit
A tool that transforms Firefox browsers into a penetration testing suite.
Project's Homepage: 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

- Studying a Computer Science bachelor program.
- Obtained a full scholarship based on my work.

SMA Secondary School
2014-2015
Obtained secondary education diploma.

St. Catharine's Collegiate
2013 - 2014

Code Academy
2012 - 2014
Web-Development Languages

Interests

Web-Application Security, Network Security, Security Competitions, Bug Bounty, Programs, Olympic Wrestling, Soccer, Badminton, Traveling, Trying new things, Reading.

References

Available upon request.