Babak Amin Azad

baminazad@cs.stonybrook.edu
https://www.silverf0x00.com
https://www.linkedin.com/in/babakaminazad

INTRO

I'm currently a PhD student in PragSec Lab at Stony Brook University. I work under the supervision of Professor Nikiforakis, aiming uncover vulnerabilities and practices, that make the web insecure. More specifically, my research goal is to make web applications safer, by reducing their attack surface through software debloating. In my latest work (published at USENIX security 2019) I showed that we can remove up to 60% of historical CVEs and reduce the size of a web application by 65% while maintaining the most popular functionality of the evaluated web applications. This work requires the dynamic analysis of web applications written in PHP and rewriting parts of their code. Orthogonally to my work on attack surface reduction, I study malicious bots on the internet devising ways to protect websites against them by differentiating their traffic from regular user traffic.

TECHNICAL SKILLS

While I believe as a pentester and researcher in InfoSec community, it is less important what programming languages I know, I do have a software development background as a web developer and these days in my daily job I use the following technologies:
Operating Systems: Linux, MacOS, Windows.
Database Systems: MySQL, MSSQL.
Web Servers: Apache, IIS.
Programming Languages: Python, JavaScript, PHP, C#.
Other: Cloud Environments (AWS), Virtualization and Docker.
Skills and Coursework: Network Security, Cryptography, DataScience and Machine Learning, PKI (SSL/TLS), Web and Mobile Penetration Testing.

EXPERIENCE

Research Assistant (3rd Year PhD Student) August 2017 - Present
State University of New York at Stony Brook, NY
GPA: 3.9/4.0

Cyber Security Analyst, Incident Response Team August 2014 - 2016
Kashef Banking Security Governance, Tehran, Iran

- **Website Monitoring and Deface Detection Service:** In this project an application was developed to monitor national banks' websites and alert the CSIRT team if a downtime or a deface takes place. Important features of this application includes:
  - Monitoring Script addition to the page
  - Monitoring redirection to another domain
  - Checking for addition of specific words to pages
  - Checking for change in the HTML source of website greater than a predefined threshold
  - Monitoring DNS records status
  - Monitoring WHOIS entry changes and expiration
  - Integration with Qualys SSL Labs to produce reports about SSL configuration.

- **Banking Websites' SSL Configuration Report and Hardening Guide:** This project spanned over 35 national banks' internet banking websites, SSL protocol configuration of these sites was studied, factors like security against SSL vulnerabilities (Heartbleed, POODLE, FREAK, LogJam etc.), certificate signature algorithm and cipher suites negotiated with clients were taken into consideration and a hardening report was delivered to their admins to address the issues.
- **Mobile Banking Software Security Report and Secure Android Development Guide:** The android version of mobile banking applications of 35 national banks was studied, features like secure software distribution, frequent updates, tamper detection and integrity verification, secure communication channel to the server, cryptographic protocols, insecure data storage and presence of source code protection was tested, during this study several high impact vulnerabilities were found and reported. Lastly, a secure android development guide was produced to address common pitfalls in applications tested during this study.

Freelance Web Developer 2013 - 2016
Ontech Solutions ltd., United Kingdom (Remote)

Our task at Ontech was to upgrade a legacy, windows based sector specific ERP software to a multi user, web based application, this was a web development project but due to abundance of features it had, the design and implementation of it was quite a challenge.

TALKS & PUBLICATIONS

Less is More: Quantifying the Security Benefits of Debloating Web Applications September 2019
OWASP Global AppSec 2019, Washington, D.C, USA

Less is More: Quantifying the Security Benefits of Debloating Web Applications August 2019
USENIX Security '19, Santa Clara, CA, USA
`https://debloating.com`

Fingerprinting users on the web. The good, the bad and the ugly. August 2018
P0SCON 2018 Conference, Urmia University of Technology

Penetration Testing Methods for Android Applications November 2016
1st Offseconf Conference, Khaje Nasir Toosi University

Ransomware Threats and Mitigation Techniques January 2016
5th Annual Conference on E-Banking and Payment Systems

PUBLIC SERVICE

External Reviewer for DIMVA 2019 Conference March 2019