# Babak Amin Azad

https://silverf0x00.com

Email : baminazad@cs.stonybrook.edu

Mobile : +1-631-428-4419

## About Me

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. I incorporate static and dynamic analysis techniques to identify unused features in web applications and remove them. In my prior work, I have showed that this method of attack surface reduction is highly effective in removing exploitable vulnerabilities from web applications. I make parsers, code analyzers and symbolic execution engines. 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.

## Education

> **PhD in Computer Science** Stony Brook, NY
> *Stony Brook University*                                   *2017 - 2022 (Expected)*

> **MSc in Computer Science** Stony Brook, NY
> *Stony Brook University*                                   *2017 - 2020*

> **BSc in Software Engineering** Tehran, IR
> *Shahid Beheshti University*                                   *2010-2015*

## Talks & Publications

> **The Droid is in the Details: Environment-aware Evasion of Android Sandboxes**
> *Brian Kondracki, **Babak Amin Azad**, Najmeh Miramirkhani, and Nick Nikiforakis*                                   *NDSS 2022*

> **Catching Transparent Phish: Analyzing and Detecting Two-Factor Authentication Phishing Toolkits**
> *Brian Kondracki, **Babak Amin Azad**, Oleksii Starov, and Nick Nikiforakis*                                   *ACM CCS 2021*

> **Good Bot, Bad Bot: Characterizing Automated Browsing Activity**
> *Xigao Li, **Babak Amin Azad**, Amir Rahmati, and Nick Nikiforakis*                                   *IEEE S&P 2021*

> **Less is More ([Artifacts](#))**
> ***Babak Amin Azad**, and Nick Nikiforakis*                                   *SSSS 2020*

> **Web Runner 2049: Evaluating Third-Party Anti-bot Services ([Video](#))**
> Won the Best Video Presentation Award
> ***Babak Amin Azad**, Oleksii Starov, Pierre Laperdrix, and Nick Nikiforakis*                                   *DIMVA 2020*

> **Taming The Shape Shifter: Detecting Anti-fingerprinting Browsers ([Video](#))**
> ***Babak Amin Azad**, Oleksii Starov, Pierre Laperdrix, and Nick Nikiforakis*                                   *DIMVA 2020*

> **Less is More ([Invited talk](#))** Georgia Tech Cybersecurity Lecture Series
> *Web Application Attack Surface Reduction Through Software Debloating*                                   *April, 2020*

> **Gas What? I can see your GasPots. Studying the fingerprintablity of ICS honeypots in the wild**
> *Mohammad-Reza Zamiri-Gourabi, Ali Razmjoo-Qalaei, and **Babak Amin Azad***                                   *ACSAC ICSS 2019*

> **Less is More: Quantifying the Security Benefits of Debloating Web Applications**
> *OWASP Global AppSec DC*                                   *2019*

> **Less is More: Quantifying the Security Benefits of Debloating Web Applications ([Video](#) - [Artifacts](#))**
> ***Babak Amin Azad**, Pierre Laperdrix, and Nick Nikiforakis*                                   *Usenix 2019*

> **Fingerprinting users on the web.**
> ***Babak Amin Azad***                                   *P0SCON 2018*

> **Penetration Testing Methods for Android Applications.**
> *Babak Amin Azad* *1st OffseConf 2016*

> **Ransomware Threats and Mitigation Techniques.** 5th Annual Conference on EBanking
> and Payment Systems
> *Babak Amin Azad* *January, 2016*

## SERVICES

- Reviewer for Transactions on The Web (TWEB) Journal in 2021
- OWASP Global Appsec San Fransisco 2020 Review Committee Member
- Usenix Security 2020 Artifact Evaluation Committee Member
- IEEE S&P 2020 Poster Review Committee Member
- MADWEB 2020 External Reviewer
- DIMVA 2019 External Reviewer
- IEEE S&P 2020 Shadow PC Member
- IMC 2019 Shadow PC Member
- NECCDC 2020 Proctor

## EXPERIENCE

> **Cloudflare** San Fransisco, CA
> *Software Engineer Intern* *June 2021 - August 2021*

- **HTTP 3 and QUIC Fingerprinting**: I worked with the Bot Management team at Cloudflare as an intern for the summer of 2021. My focus was to build fingerprinting methods for emerging web protocols to detect bot traffic.

> **Cloudflare** San Fransisco, CA
> *Software Engineer Intern* *June 2020 - August 2020*

- **Bots Red Team Automation Platform**: I worked with the Bot Management team at Cloudflare as an intern for the summer of 2020. My focus was on bots that target Cloudflare. I implemented a scalable red teaming platform that automated bot attacks against the Bot Management platform.

> **Stony Brook University** Stony Brook, NY
> *Research Assistant* *2018 - Present*

- **PragSec Lab**: My main focus is on attack surface reduction through software debloating. Orthogonally, I work on the topics of browser fingerprinting, bot detection and other areas of web security.

> **Stony Brook University** Stony Brook, NY
> *Teaching Assistant* *2017 - 2018*

- **Courses**: Undergraduate operating systems and introduction to software security.

> **Kashef Banking Security Governance** Tehran, Iran
> *Incident Responder Engineer* *2014-2016*

- **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.
- **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.

> **Ontech Solutions ltd.** UK (Remote)

*Freelance Web Developer* *2013-2016*

- ○ **Web development**: Our task at Ontech was to upgrade a legacy, desktop-based, sector specific ERP software to a multi user, web based application.