

BAHRUZ JABIYEV

<https://bahruz.me/> | jabiyev.bahruz@gmail.com | github.com/bahruzjabiyev

PROFESSIONAL EXPERIENCE

Dartmouth College

Postdoctoral Fellow

Nov. 2023 – May 2024

Hanover, NH

- Developed a formal verification model for finding new discrepancy-based HTTP attacks
- Contributed to the development of a fuzzing toolset for Electronic Health Record systems

Cold Spring Harbor Laboratory

Computational Postdoctoral Fellow

Apr. 2023 – Nov. 2023

Cold Spring Harbor, NY

- Studied the human immune system to learn new cyber-defense methods
- Studied the methods of viruses to get ideas for new cyber-attack techniques

Northeastern University

Research Assistant, Cybersecurity

Sep. 2017 – Apr. 2023

Boston, MA

- Developed a systematic search technique for HTTP Request Smuggling attack vectors and the [T-Reqs](#) tool, which was adopted by developer teams such as that of Apache Traffic Server
- Discovered a new technique for multi-layer web server fingerprinting and helped the development of the [Untangle](#) tool, which uses parsing discrepancies for fingerprinting
- Developed a systematic search technique for HTTP/2-to-HTTP/1 conversion anomalies and the [Frameshifter](#) tool, which found new attack vectors for popular reverse proxies
- Built a new defense technique against SSRF attacks and a prototype [extension](#) for NGINX, which rewrites all URLs in incoming requests to have them served by a restricted server
- Built a new approach for guiding the input selection in differential fuzzing and the [Gudifu](#) tool, which I developed the initial version of with Envoy Platform Team at Google

Google

Research Intern, Envoy Platform Team

May 2022 – Sep 2022

Cambridge, MA

- Developed a systematic approach for coverage-guided differential fuzzing and a toolset for finding parsing discrepancies between servers in the Google Cloud

Facebook

Security Engineer Intern, Online Safety Team

Jun. 2019 – Aug. 2019

Menlo Park, CA

- Expanded an investigation tool, which was used for only terrorism cases, to be also used for child abuse and human trafficking investigations

Cyberwise

Penetration Tester

Dec. 2014 – Jul. 2017

Istanbul, Turkey

- Reported vulnerabilities in web applications and internal networks of customer companies
- Developed tools for the automation of various security-related tasks such as [watching networks](#) and [parsing scanner results](#), which gave my teammates at least 50x speedup in reporting results
- Designed and delivered an “offensive web and network security” training program

EDUCATION

Northeastern University

PhD in Cybersecurity

Sep. 2017 – Apr. 2023

Boston, MA

- Dissertation: Systematic Search Techniques for HTTP Server Chain Attack Vectors
- Committee: Engin Kirda, Alina Oprea, David Choffnes, David Evans, Zakir Durumeric

Istanbul Sehir University

MSc in Cybersecurity Engineering

Oct. 2014 – Jun. 2016

Istanbul, Turkey

Middle East Technical University

BSc in Computer Engineering

Sep. 2008 – Jun. 2013

Ankara, Turkey

PUBLICATIONS

Gudifu: Guided Differential Fuzzing for HTTP Request Parsing <i>International Symposium on Research in Attacks, Intrusions and Defenses (RAID)</i>	2024
Untangle: Multi-Layer Web Server Fingerprinting <i>Network and Distributed System Security Symposium (NDSS)</i>	2024
Frameshifter: Security Implications of HTTP/2-to-HTTP/1 Conversion Anomalies <i>USENIX Security Symposium</i>	2022
T-Reqs: HTTP Request Smuggling with Differential Fuzzing <i>ACM Conference on Computer and Communications Security (ACM CCS)</i>	2021
Preventing Server-Side Request Forgery Attacks <i>Annual ACM Symposium on Applied Computing (ACM SAC)</i>	2021
Game of FAME: Automatic Detection of Fake Memes <i>Conference for Truth and Trust Online (TTO)</i>	2021
FADE: Detecting Fake News Articles on the Web <i>International Conference on Availability, Reliability and Security (ARES)</i>	2021

PUBLICATIONS IN THE MAKE

Bypassing WAFs using HTTP Content Parsing Discrepancies <i>Work in Progress</i>	2024
---	------

SELECTED ACHIEVEMENTS & AWARDS

PortSwigger Nomination for Top 10 Web Hacking Technique <i>Techniques of T-Reqs and Frameshifter papers in 2021 and 2022 respectively</i>	2021, 2022
NYU CSAW North America Applied Research Competition <i>T-Reqs paper was invited to compete as one of 83 top-quality research papers in cybersecurity</i>	2022
4th Place in Hacking Competition <i>"Cybersecurity Beanpot 2019", an individual hacking competition for students from Boston-area colleges</i>	2019
OSCP (Offensive Security Certified Professional) <i>24 hours long hands-on exam with the goal of compromising at least three out of five systems</i>	2017