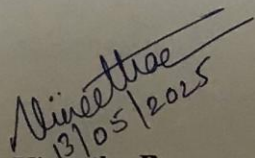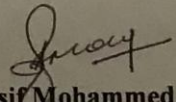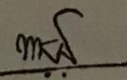# PRESIDENCY UNIVERSITY

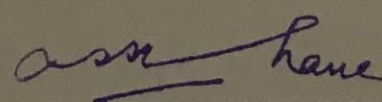# SCHOOL OF COMPUTER SCIENCE ENGINEERING

CERTIFICATE

This is to certify that the Project report **"Creating a Comprehensive Web Application Fuzzer"** being submitted by "Mohan R Shetty, Amulya S Sathish, Suchithra K, Sumanth R" bearing roll number(s) "20211CSE0591, 20211CSE0584, 20211CSE0599, 20211CSE0607" in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering is a bonafide work carried out under my supervision.

Ms. Vineetha B
Assistant Professor
PSCS
Presidency University

Dr. Asif Mohammed H.B
Associate Professor & HOD
PSCS
Presidency University

Dr. MYDHILI NAIR
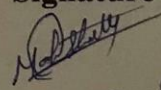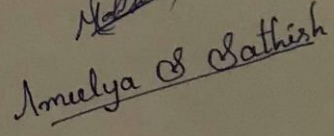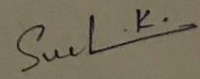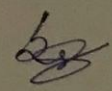Associate Dean
PSCS
Presidency University

Dr. SAMEERUDDIN KHAN
Pro-Vice Chancellor- School of
Engineering
Dean -PSCS / PSIS
Presidency University

PRESIDENCY UNIVERSITY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

DECLARATION

We hereby declare that the work, which is being presented in the project report entitled **Creating a Comprehensive Web Application Fuzzer** in partial fulfillment for the award of Degree of **Bachelor of Technology** in **Computer Science and Engineering**, is a record of our own investigations carried under the guidance of **Ms. Vineetha B, Assistant Professor, School of Computer Science Engineering & Information Science, Presidency University, Bengaluru.**

We have not submitted the matter presented in this report anywhere for the award of any other Degree.

Student Name	Roll Number	Signature
Mohan R Shetty	20211CSE0591	
Amulya S Sathish	20211CSE0584	
Suchithra K	20211CSE0599	
Sumanth R	20211CSE0607	

ABSTRACT

Web applications are increasingly targeted by cyberattacks, making automated security testing essential. This project presents a Web Application Fuzzer, a tool designed to detect vulnerabilities by injecting various malformed, unexpected, or malicious inputs into web applications. The core idea of this model is to detect the vulnerabilities or other errors that is related to security and to analyse them. This project aims to develop an automated fuzzer to identify and test these components for security flaws. The fuzzer will systematically enumerate and test hidden directories, API endpoints, and subdomains while fuzzing URL parameters for injection attacks. The fuzzer identifies critical security flaws, including SQL Injection, Cross-Site Scripting (XSS), Directory Traversal, and Authentication Bypass, helping developers secure their applications proactively.The model integrates automated testing, real-time vulnerability analysis, and risk scoring, improving security assessment efficiency compared to traditional manual testing. Additionally, it can be enhanced with AI-driven fuzzing, cloud-based distributed testing, and DevSecOps integration for continuous security monitoring. The fuzzer generates extensive test cases, ensuring comprehensive security validation across APIs and web endpoints. It can be integrated with CI/CD pipelines, enabling security checks throughout the development lifecycle. A user-friendly web dashboard allows for monitoring vulnerabilities in real time, helping teams take proactive security measures.The implementation of this model reduces security risks, enhances web application resilience, and minimizes the effort required for penetration testing. With further enhancements, such as machine learning-based payload generation and automated patch recommendations, the fuzzer can become a next-generation security testing tool for web applications.

ACKNOWLEDGEMENT