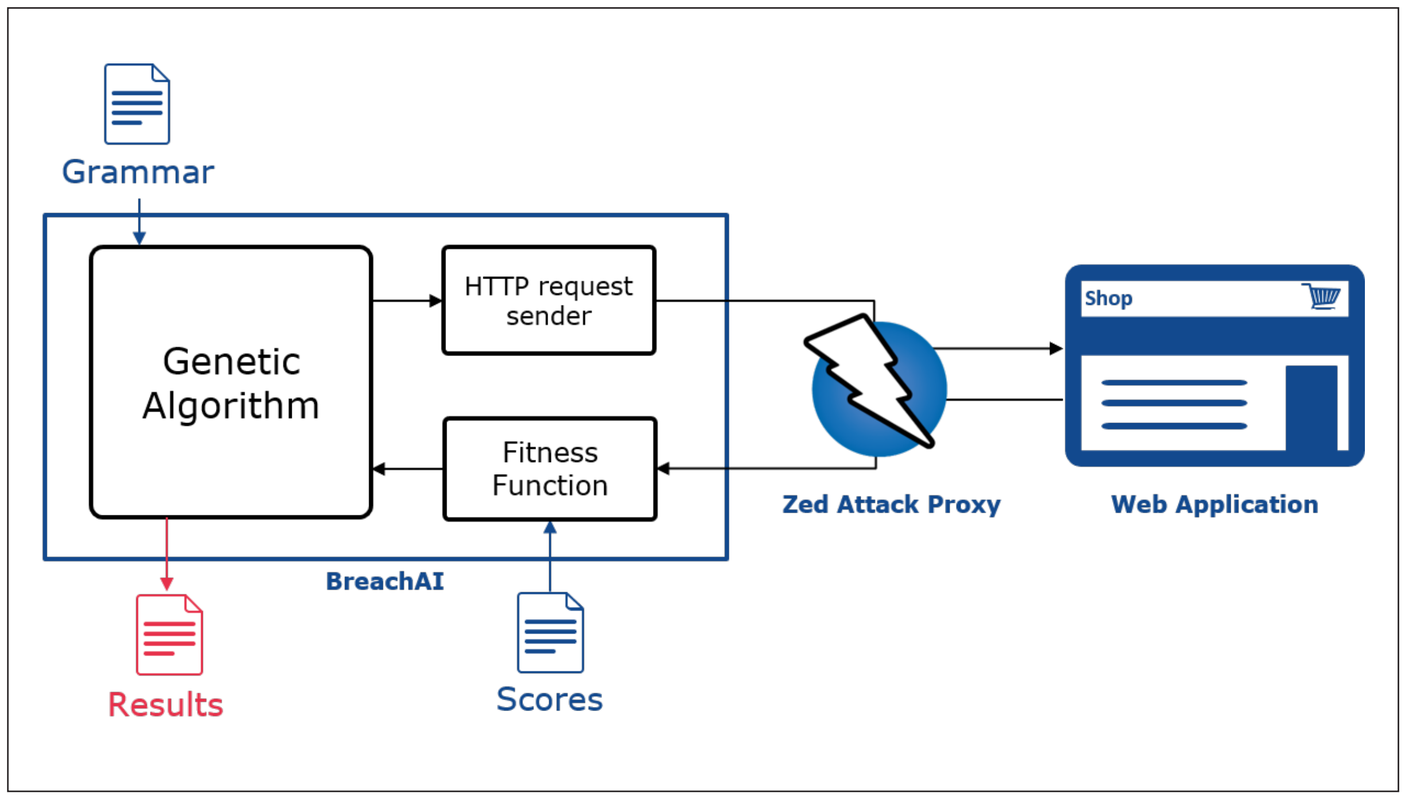
NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

School of Computer Science and Engineering
College of Engineering

BreachAI

An AI-based approach to Web Application Security Testing

Student: Soong Jie Ming
Supervisor: Dr Shar Lwin Khin



BreachAI is a black-box fuzzer that checks for cross-site scripting (XSS) vulnerabilitites. It works seamlessly with Zed Attack Proxy, a web security scanner produced by Open Web Application Security Project (OWASP), to detect XSS vulnerabilitites.

Genetic Algorithm

BreachAI generates its inputs by utilising a search-based algorithm known as the genetic algorithm. The implementation of the Genetic Algorithm can be broken down into five phases:
1. Initialisation, 2. Selection, 3. Crossover, 4. Mutation and 5. **End**

Technologies Applied:

- Genetic Algorithm
- ZAP REST API
- Context Free Grammar
- XSS Validation

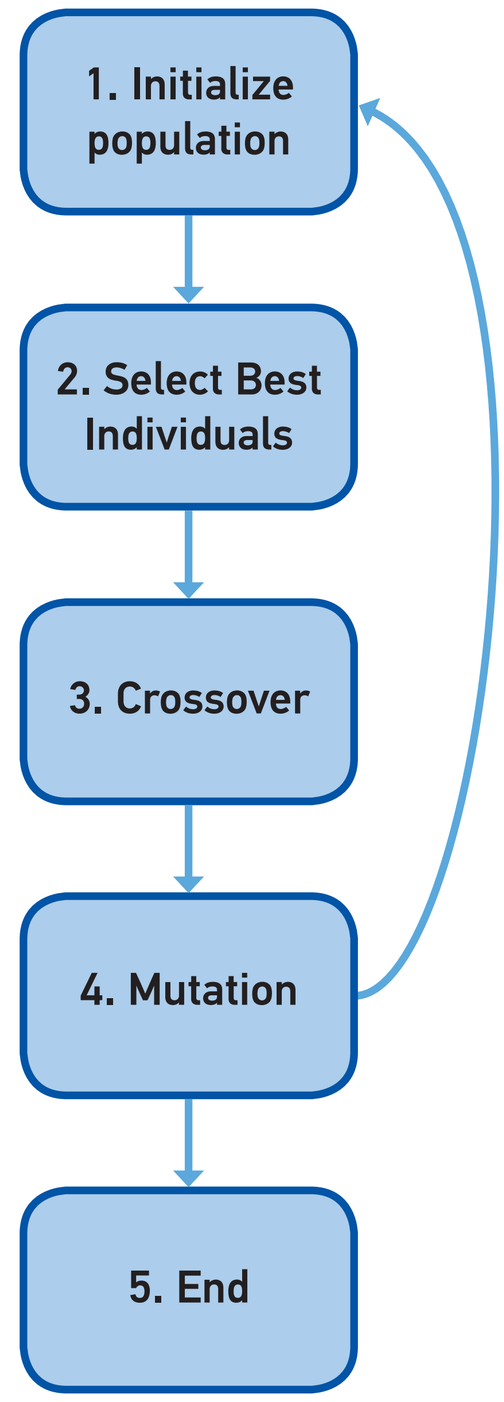
1.Generate population of Strings.

2.Select most promising set of Strings.

3.Mix & match the selected strings to form new Strings.

4.Random chance to mutate Strings. If objective found, head to 5., else repeat 1. to 4.

5.End.



Genetic Algorithm