Francesco Caturano

Tutor: Simon Pietro Romano

XXXIV Cycle - II year presentation

SECSI: SECurity Solutions for Innovation

Context

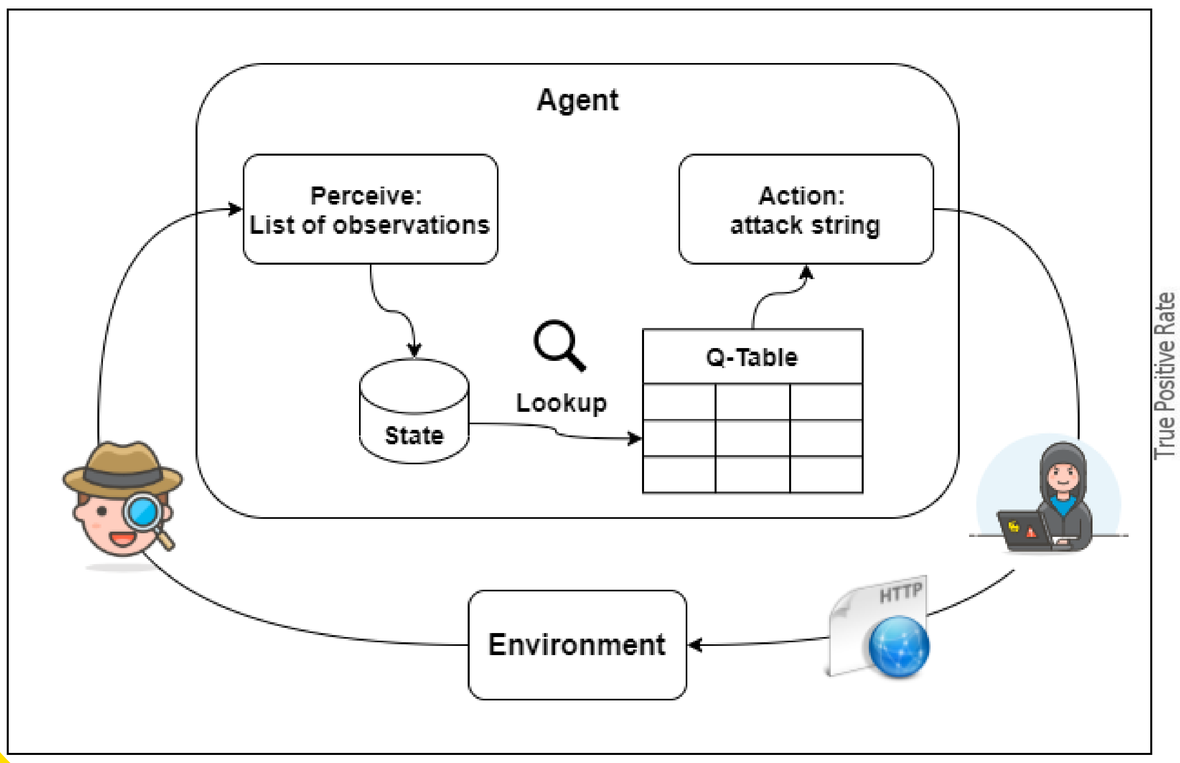
- Intelligent models for Web Applications security testing
  - Reinforcement Learning as a means to learn the behaviour of penetration testers
- Virtualization Technologies for Network Security training
  - Practical solutions to overcome container-based virtualization limits

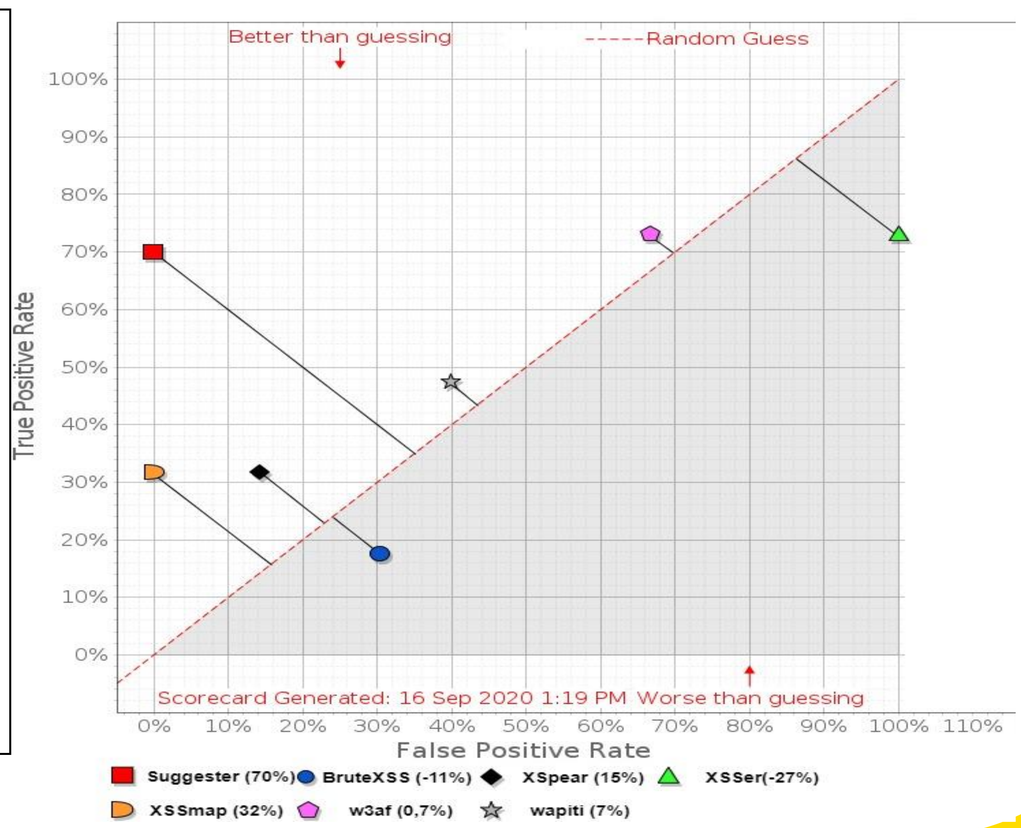
Research activity

Web Application Penetration Testing as a Markov Decision Process

- The penetration tester implements a sequential process:
  - Collects *observations* from a Web Application (Environment & Observations);
  - Improves sequentially the *attack string* (State & Action Space);
  - Provides a *Proof of Concept* of the vulnerability (Epsiodic task feature).

- **First Result**: a semi-automated tool that recommends the best actions to a human tester;
  - Very good accuracy indicators in comparison with state of the art automated scanners.
- **Improvement**: fully automated platform;
  - External module that extract observations and implements the best actions.





Contacts and collaborations:
francesco.caturano@unina.it

- **Future works**:
  - Evaluate the scalability of the proposed approach on other vulnerabilities (SQL Injection)
  - Develop a support decision system for penetration testing based on Knowledge Graphs
  - Design and implement a penetration testing session recorder
    - Create a dataset for expert demonstrations to be used in a Reinforced context