Universidad del Rosario | Escuela de Ingeniería, Ciencia y Tecnología | MACC Matemáticas Aplicadas y Ciencias de la Computación | HINNT Hub de INNovación y Transferencia

Testing tool for weak application inputs

Juan E. Murcia, Rodrigo Castillo and David F. Martínez

MACC
U Rosario

juane.murcia@urosario.edu.co
rodrigo.castillo@urosario.edu.co
davidfel.martinez@urosario.edu.co

@MACC_URosario @MACC.URosario macc_ur

Agenda

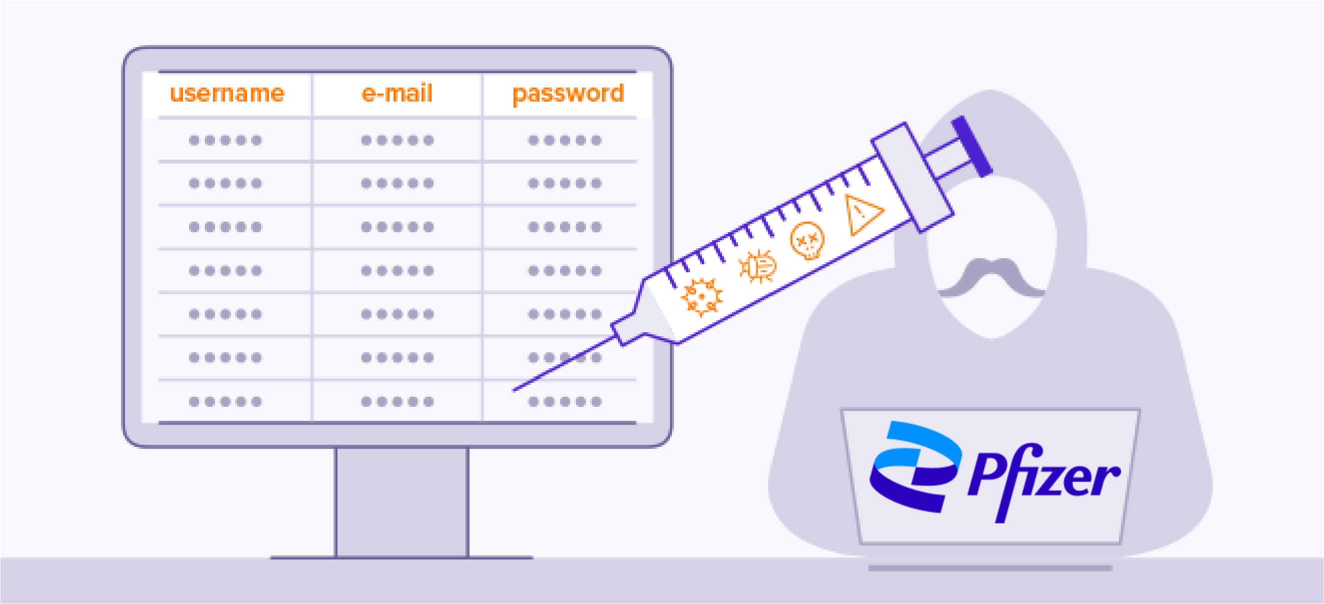
1. Introduction
2. Project explanation

Introduction

Web application's security is a crucial topic nowadays, since having internet access is more and more common around the world. However, several applications deployed still have now or even old vulnerabilities that people can exploit to take advantage from the application. One of the most common vulnerability is injection payloads into the input fields.

Problem Explanation

Due to the existence of such problem, we propose an application that tests several inputs found within a web application recursively, and then starts injecting payloads to check if some work, if it does the program will report which payload worked, and where it was used. We're going to parallelize the application in order to achieve efficiency.

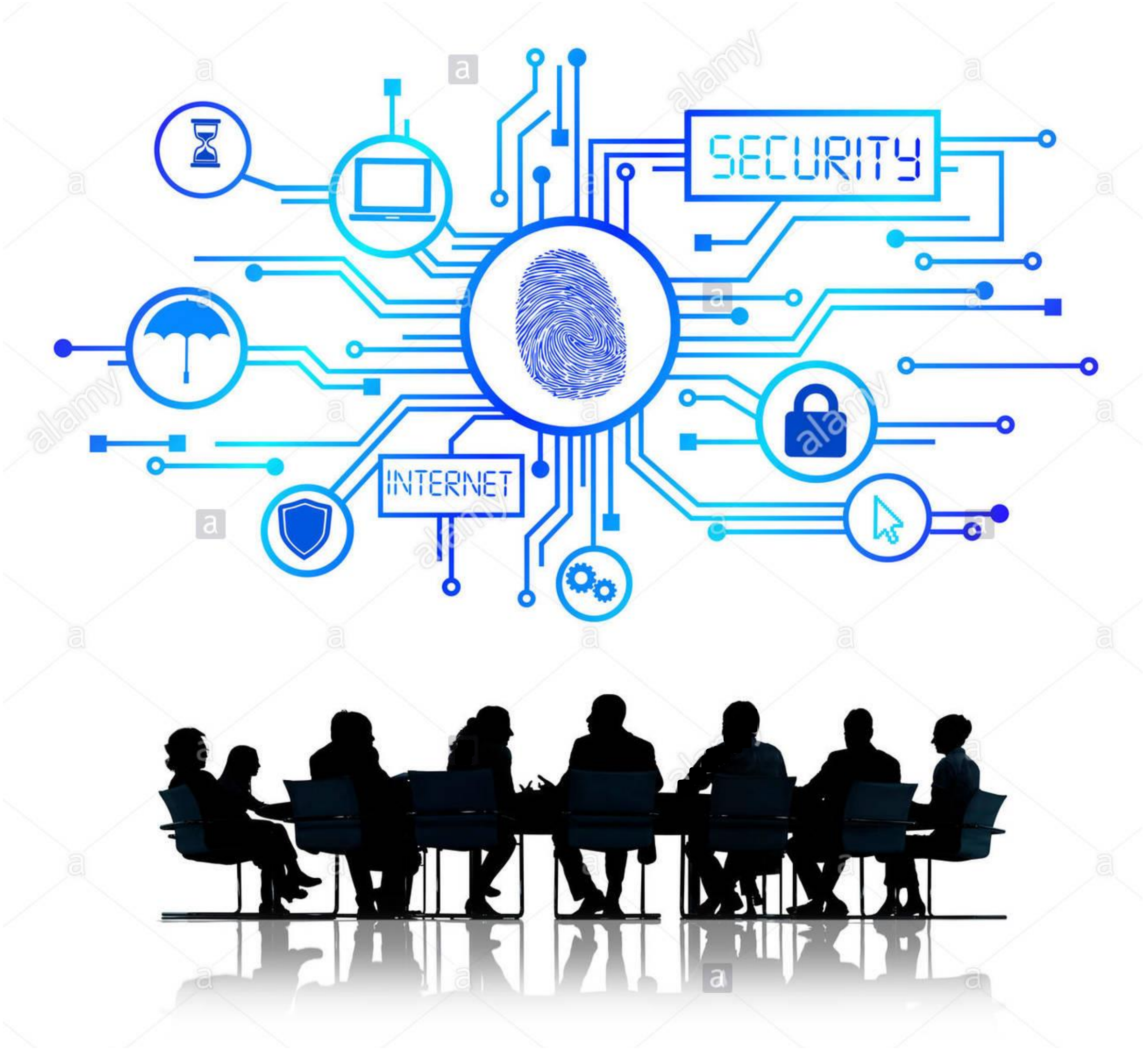


Problem Explanation

Functional Requirements

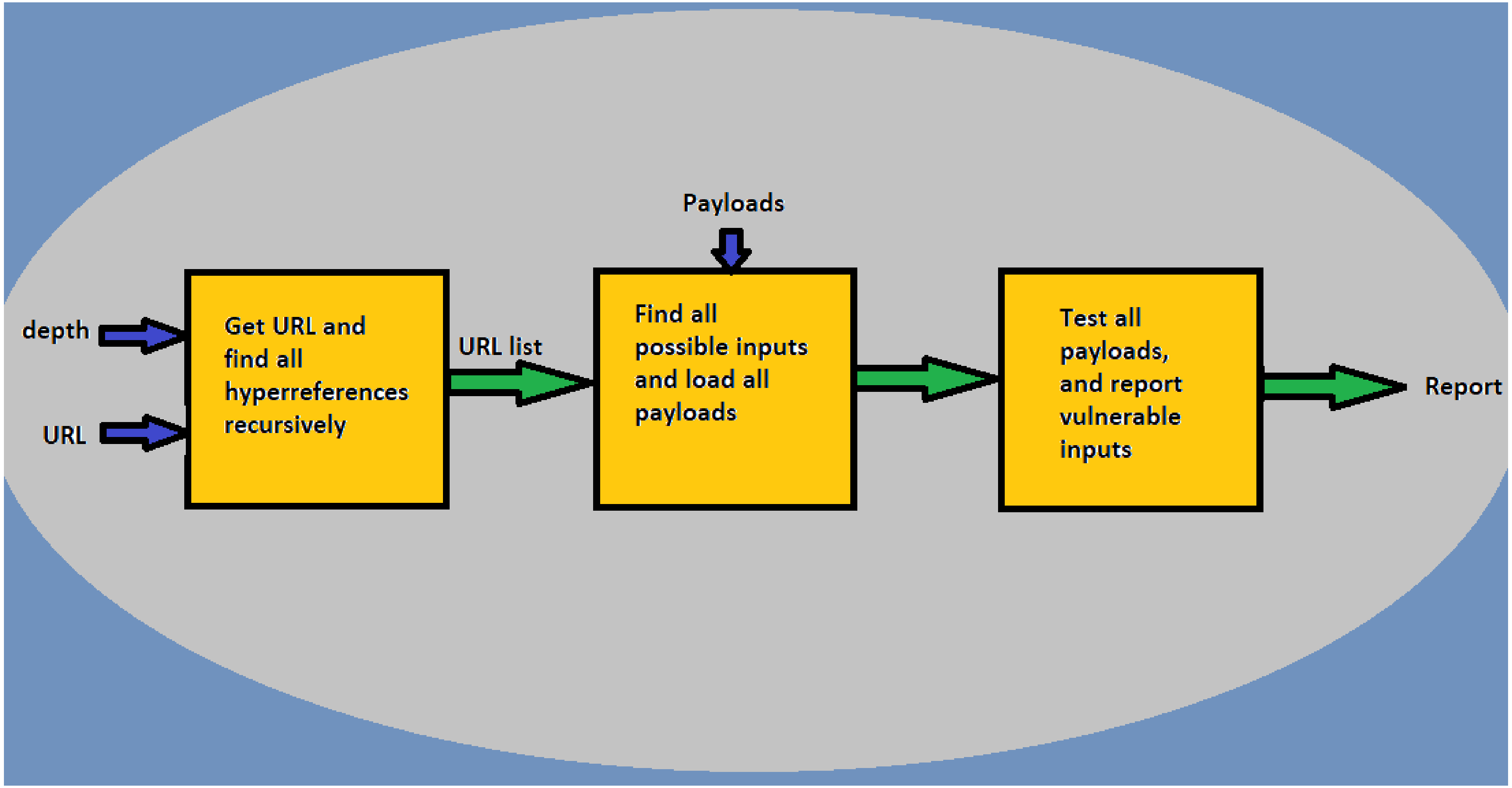
The API should be able to

- Connect to a given URL
- Obtain all hyper references according to recursion level
- Detect and store inputs addresses
- Load a payload database to text
- Try different attack vectors over the detected input fields
- Report successful attacks



Problem Explanation

Projects Architecture


depth
URL
Get URL and find all hyperreferences recursively
URL list
Payloads
Find all possible inputs and load all payloads
Test all payloads, and report vulnerable inputs
Report

Problem Explanation

Sample of attack vectors

XSS

- <script\x20type="text/javascript">javascript:alert(1);</script>
- "`'><script>\x09javascript:alert(1)</script>
- <img src\x09=x onerror="javascript:alert(1)">
- <script /*%00*/>/*%00*/alert(1)/*%00*/</script /*%00*/
- <math><a xlink:href="//jsfiddle.net/t846h/">click

SQL Injection

XXE Injection

THANKS!

Juan E. Murcia,
Rodrigo Castillo and David F. Martínez

MACC
U Rosario

juane.murcia@urosario.edu.co
rodrigo.castillo@urosario.edu.co
davidfel.martinez@urosario.edu.co

@MACC_URosario @MACC.URosario macc_ur