**Work summary sheet for G-46**

**Team Members: i) Aamir Ahmad 18803005**

**ii)Vivek Dwivedi 18803003**

**iii)Dheeraj Kumar 18103099**

**Topic: Web vulnerability scanner system**

**Motivation behind the project**

We have been working in the field of information security since a long time and every team member in our group has reported atleast one vulnerability in some web application. Most of our work revolves around the sphere of govt websites and after getting exposed to the vulnerabilities present, we found out that the state of information security in our country is pathetic. Common and trivial vulnerabilities which can be avoided just by writting safe and secure codes are still present and widespread. Keeping this in mind, we wanted to develop a system/framework which can scan websites for common vulnerabilities listed in OWASP top 10 and thereby do our part in securing the nation’s cyber space. This is a dream project for us which is way beyond the limitations of marks or grades. We will try our nose and toes in making this project succesfull and in dedicating this to the nation.

**Type of project**

This is a ***development cum research project*** as security is a domain which is contantly evolving and is under rigorous research by security researchers.

**Features:**

**i) Implemented-**

* Open port scanner
* XSS scanner

**ii) To be implemented**

* Subdomain enumerator
* IDOR/directory listing finder
* More to come

**Critical Analysis of research paper and references**

**i)** [**OWASP top 10**](https://owasp.org/www-project-top-ten/)

This is published by Open web application security project (OWASP) and it enlists the top 10 most exploited vulnerabilities of a particular year. This gave us a basic roadmap of the top vulnerabilites we should focus during this project.

**ii)** [**Web security testing guide**](https://github.com/OWASP/wstg/tree/master/document/4-Web_Application_Security_Testing)

This is also a repository maintained by OWASP which enlists everything about security from development stage to deployment and post-deployment. This was reallly helpful in finding out patterns about human behavior and common mistakes made by developers.

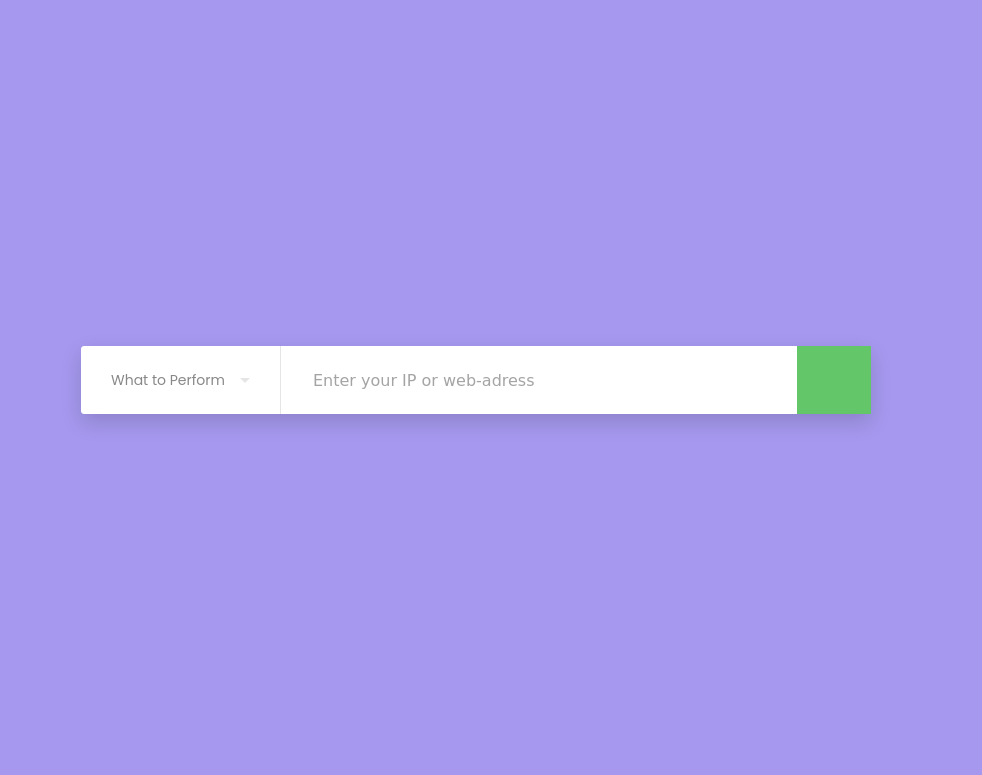
**iii)**[**Portswigger lab research papers**](https://portswigger.net/research/one-xss-cheatsheet-to-rule-them-all)

Portswigger consistently publishes research papers related to web application security advancements and mitigation. The portswigger labs are also a great source of knowledge for security researchers.

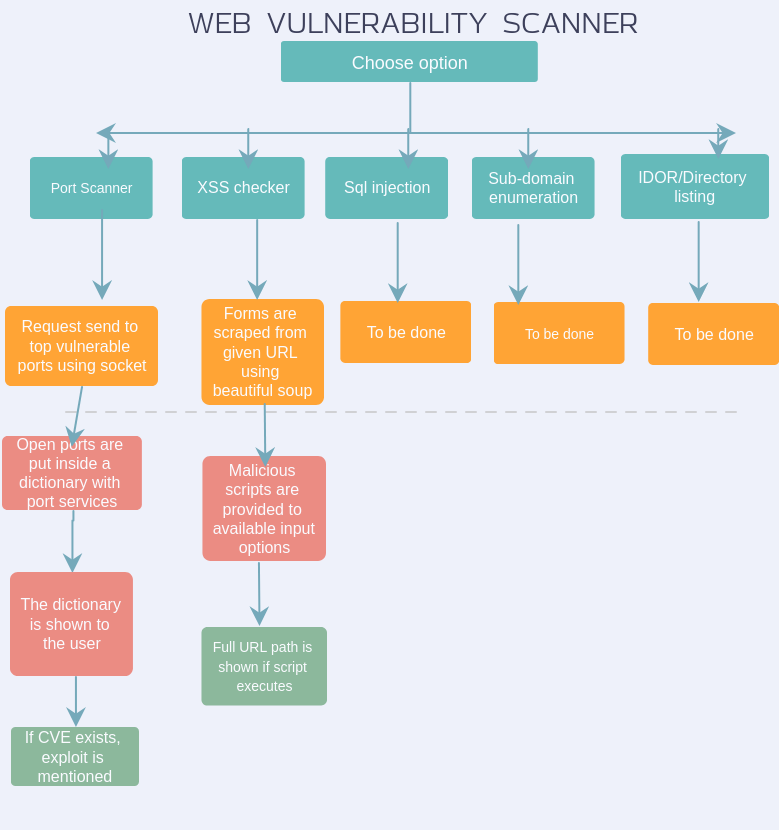
**Languages,frameworks and libraries used so far**

* Python3, Javascript, Html,css.
* Bootstrap, Flask, Python sockets, Beautifulsoup

**Screenshot**

****

**Flowchart:**

****