# Abstract

Web applications security is playing crucial role in this world by securing businesses and their data. By using the web applications and sites, businesses can easily achieve its objective much faster. Web system are accessible anytime, anywhere via any pc with an internet connection. As technology changes, it becomes increasingly challenging for businesses of all types to keep their personal and customer's information on the web secure. If web applications/sites are not safe and secure, those critical business relationships cannot be compromised. A single security breach could be a death-knell for small business. Before publishing the sites and applications we need to check secureness of the web sites/apps. But it is very expensive to learn it with using professional tools, same as with community version tools  it's unable to access the wanted information from the community version.

In this research project, I am making web vulnerable scanning scanner using Python programming language. In this project we use object oriented programming language. This project depends on Python and Python's libraries such as beautiful-soup, regular expression and Damn vulnerable web application which including all html resources and its back-end. In this project we scarp data, extract form, scanning link, send payloads  to specific form and link to find vulnerability. cross site script is used to inject web application because the payloads is not visible for the browser's XSS filter. User accidentally trigger the payload if they visit the affected page. we can inject manually but it is not convenient due to lots of pages. Our scanner scan automatically in whole web app within limited time. Which helps to a fresh web security learner and motivate them to start web security.

KEYWORDS: Python, Beautiful-soup, data scrapping and web vulnerability.