

Project Title: SAMPARK

Team name: The Architect

Team leader name: Saket Upadhyay

College name: VIT Bhopal

**Theme: Internet Security**

**Problem Statement:** Recently, online operations aiming at end-customers are relying more on web-based services. Many fake e-commerce websites might claim to sell the products which are currently unavailable elsewhere. Considering the overall growing amounts of unaware end-users, we can see more security holes and easy opportunities for cybercriminals. For example: as people can't go out to buy daily necessities they rely on e-commerce websites which may lead them to use unknown/less trustworthy sources which can force them to make the financial processes online. This will help **criminals to steal your credit card number, PIN, and security code to make unauthorized transactions**, without needing your physical credit card. Make software that helps prevent these credit card frauds and warns the user before they make transactions online

# Idea / Approach

Describe your idea/approach

- **SAMPARK is a user friendly** platform that allows you to scan for multiple threats present in a website on a single platform.
- The user needs to only provide the URL and SAMPARK will determine the safety of the website making it very **convenient for a non- technical person** to use
- In this PROTOTYPE (v2) it scans the website for Malware, presence of HTTPS and proper SSL certification and covert redirection scripts.
- Technically SAMPARK is more than 'just a software', **it's a framework**. We wanted SAMPARK to be able to easily integrate with other tools and technologies easily, hence it follows 'Modular' Design from the scratch.
- The **main goal** is to perform **complex scanning tasks in background with diverse tactics** and **give user simplest possible answers** in YES/NO or similar forms, **so that everyone can understand it**, from common office going person to computer security researcher.

# Technology Stack and Use Cases

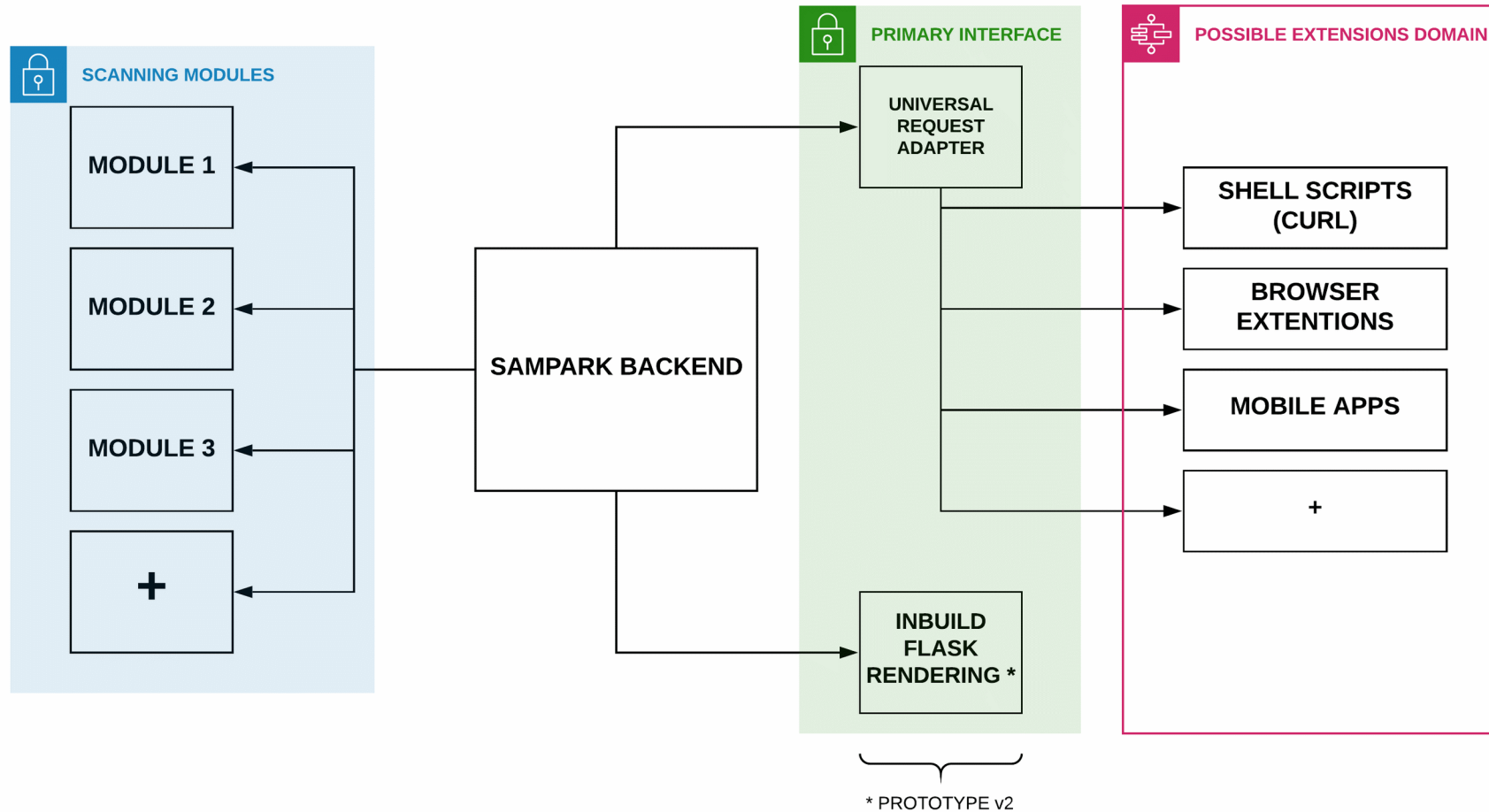
## Technology Stack

- Python3
- Flask
- OpenSSL
- CSS
- HTML
- JS
- VT API

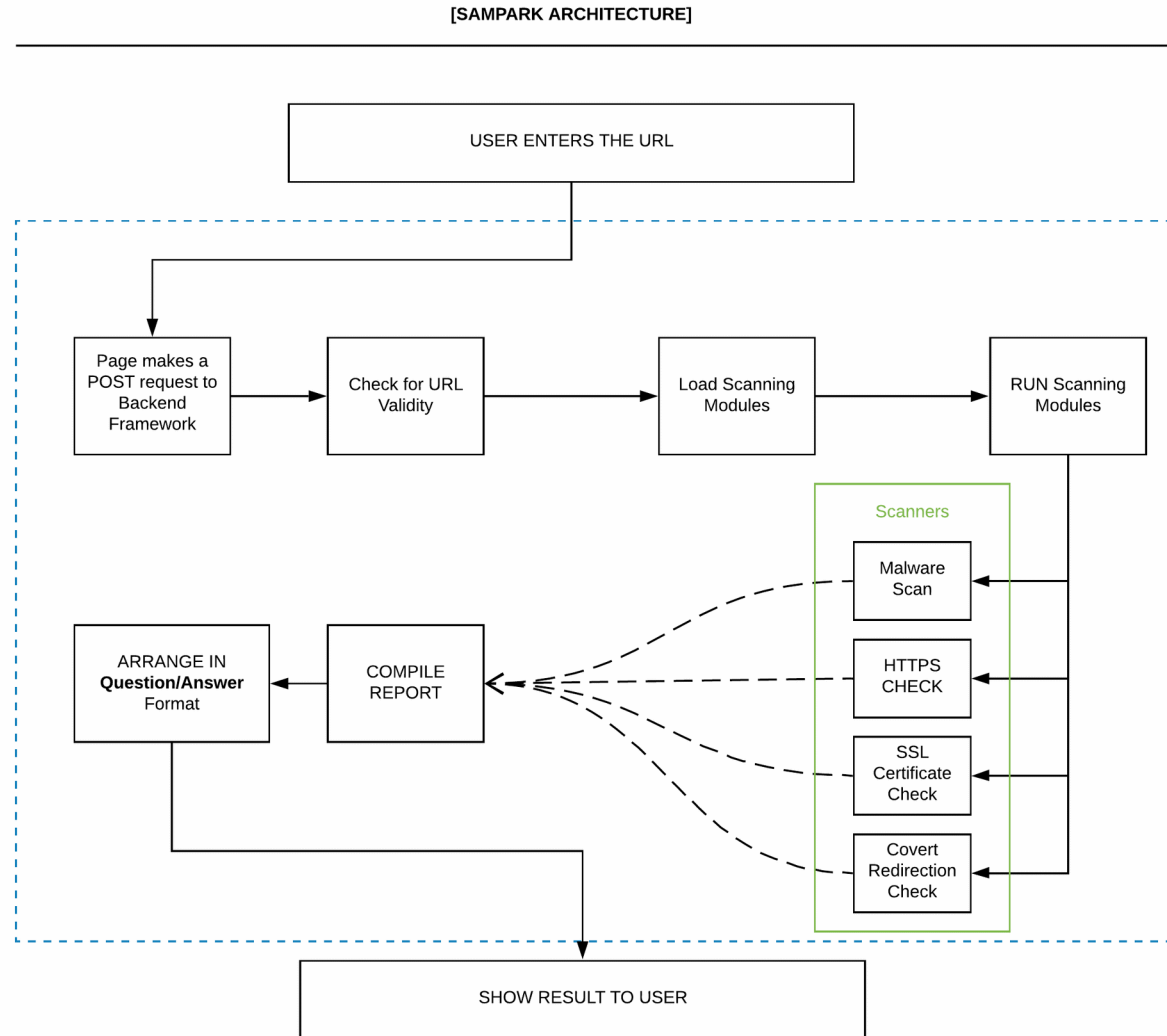
## Use Cases

- To check if a website or web portal is safe for sensitive information transaction.
- To check the validity of e-commerce website
- To check fundamental security status of any payment portal
- To build complex detection tools around the SAMPARK framework
- Check for hidden malicious scripts and redirection codes.

# Block Diagram / Architectural Diagram



# Block Diagram / Architectural Diagram



\* THE SCANNERS SECTION SHOW MODULES USED IN PROTOTYPE v2, SAMPARK IS DYNAMIC FRAMEWORK WE CAN ADD MORE MODULES EASILY

# Dependencies

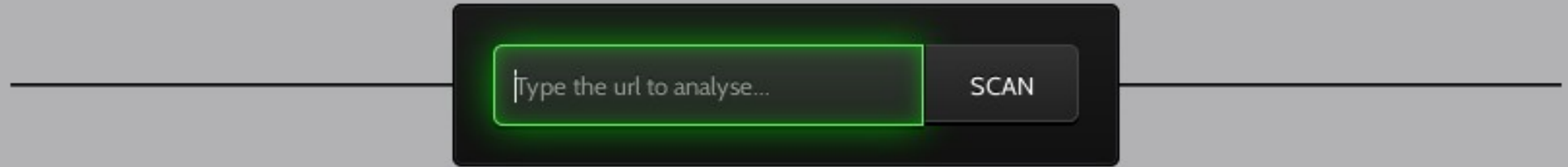
## Dependencies

- Virus Total API
- Open source HTML templates for flask interface from [codepen.io](https://codepen.io)

# Social Impact Analysis with COVID19

COVID19 has changed our lifestyle drastically. Ever since WHO announced COVID19 as a global pandemic e-commerce has become increasingly popular. During lockdown many essentials that were earlier purchased in physical markets are now being purchased online from the safety of homes. Even the post lockdown period will see an increase in e-commerce due to continued social distancing. In a period where all other businesses are at a standstill e-commerce websites are lucrative targets for cybercriminals. Fake e-commerce websites claiming to provide essentials are popping up. This is very harmful to economies all over the world that are already crashing in the wake of the pandemic. SAMPARK aims to prevent these cyber crimes by providing a platform for the non technical end user to check whether the e-commerce website he is using is safe or not. For a non technical end user SAMPARK will simplify the entire complicated process of scanning for different vulnerabilities on one platform. This will ensure that the common man need not be concerned about complicated technicalities of cybersecurity but still be safe from fraudulent e-commerce practices and attacks from cyber criminals. The only thing the user needs to provide is the URL of the website he wants to test for security. Even in a post COVID19 world SAMPARK will be beneficial for the society as increased e-commerce is predicted. Prevention of these cyber crimes using SAMPARK will allow e-commerce to flourish which in turn will be beneficial for our crashing economies.

# Implementation [Main Page]



The image shows a dark-themed user interface for a web application. At the top, there is a horizontal line. Below this line is a dark rectangular box containing a text input field and a button. The text input field has a green border and contains the placeholder text "Type the url to analyse...". To the right of the input field is a button labeled "SCAN".

SAMPARK

Prototype v2

NOTE : Remove "http(s)://" part from url



# Implementation [SAFE]

Question	Answer
Is this website safe for transaction?	YES
Website under scan	www.onlinesbi.com
Malware Scan Result	SAFE
Is website using HTTPS?	YES
What is the redirection scheme for HTTPS?	NO REDIRECT
SSL Host Name	www.onlinesbi.com
SSL Peer Name	('103.68.221.190', 443)
SSL Common Name	www.onlinesbi.com
SSL Alternate Name	['onlinesbi.com', 'www.onlinesbi.com']
SSL Certificate Issuer	DigiCert Global CA G2
SSL Certificate Issuer in Trusted List	YES
SSL Not valid Before	2020-01-20 00:00:00
SSL Not valid Before	2022-01-24 12:00:00
Do website perform Covert Redirection?	NO

# Implementation [MALICIOUS]

Question	Answer
Is this website safe for transaction?	<b>NO</b>
Website under scan	vitaly.agricolacolhue.cl
Malware Scan Result	<b>UNSAFE</b>
Malware Scan Triggers	['Kaspersky', 'Trustwave']
Malware Scan Categories	['phishing site', 'malicious site']
Is website using HTTPS?	<b>NO</b>
Do website perform Covert Redirection?	<b>NO</b>

# Link to the project

GitHub link: <https://github.com/Saket-Upadhyay/sampark>

Google Drive link:

<https://drive.google.com/open?id=1csy31knkkmfD8h5uuHuO1Fy3o7XxnkfU>