

SSL/TLS Certificate Analyzer Tool

Presented by Mohan Gumgaonkar as part of the Digisuraksha Cyber Security Internship, this project focuses on enhancing web security through an innovative SSL/TLS Certificate Analyzer. The tool aims to simplify the process of analyzing website certificates to ensure secure connections and identify vulnerabilities.



Current System Overview

Manual Command-Line Tools

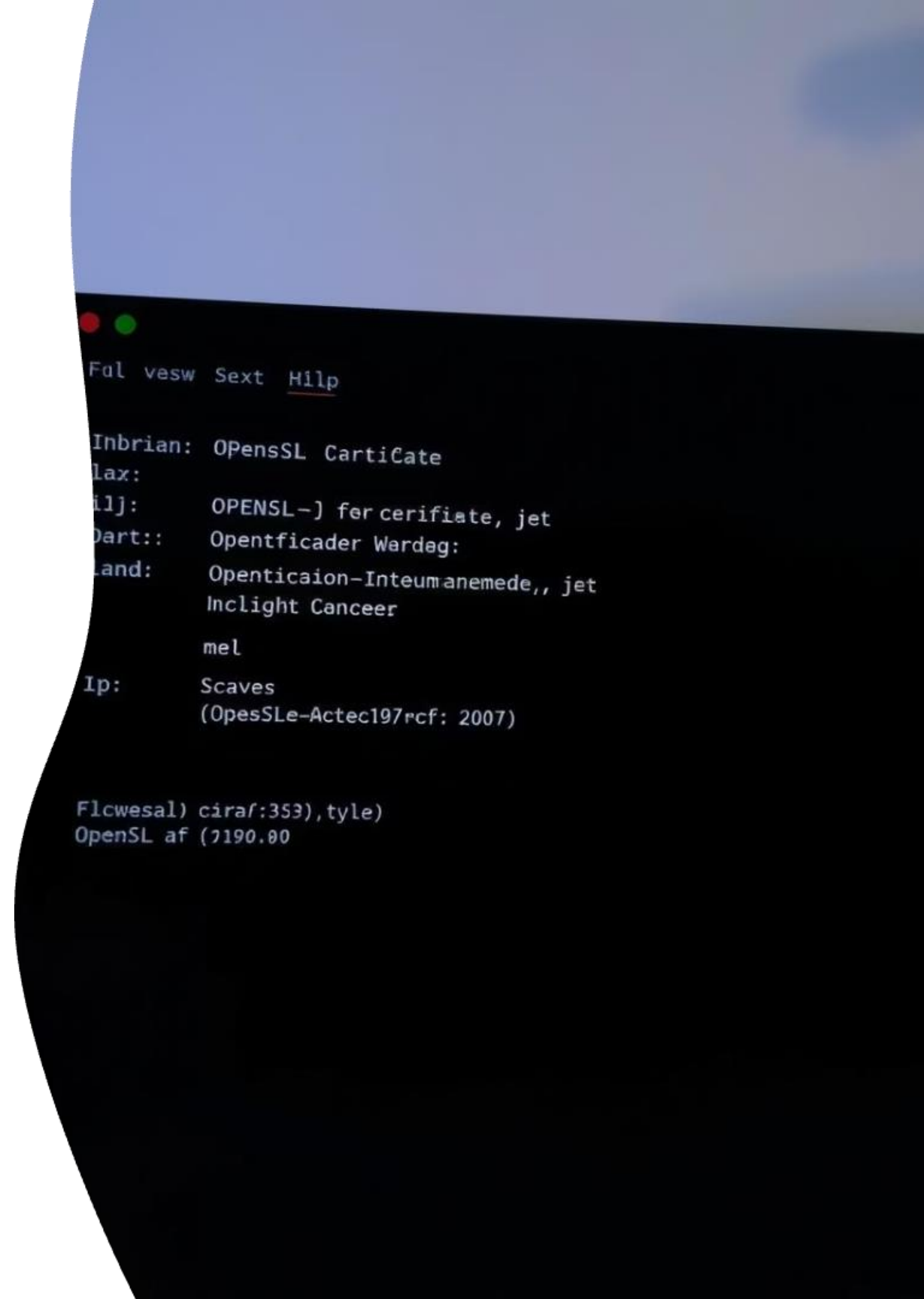
Users rely on OpenSSL and similar tools to fetch certificate details, requiring technical skills and multiple steps.

Browser Warnings

Browsers alert users about expired or insecure certificates but provide limited information.

Basic Online Analyzers

Existing online tools offer limited insights and lack reporting features.



```
Ful vesw Sext Hilp

Inbrian: OPensSL CartiCate
lax:
ilj: OPENSLL-] fer cerifiarte, jet
Dart:: Opentficader Wardag:
land: Openticaion-Inteumanemedee,, jet
Inclight Canceer
mel
Ip: Scaves
(OpesSLe-Actec197rcf: 2007)

Flcwesal) ciraf:353),tyle)
OpenSL af (7190.00
```



Disadvantages of Current Systems

Manual Effort

Technical proficiency needed; multiple steps slow down analysis.

Limited Insights

Fail to detect weak algorithms or self-signed certificates comprehensively.

Lack of Reporting

No options to export detailed analysis reports for documentation.

Inefficiency

No centralized GUI for easy analysis of multiple websites, especially for non-technical users.

Proposed System Features

Intuitive GUI	Certificate Analysis	Weak Algorithm Detection	Expiration Alerts
Easy input of website URLs for quick analysis.	Automatic fetching of issuer, expiration, and signature algorithm details.	Identifies weak algorithms like SHA-1 and self-signed certificates.	Notifies users of expired or soon-to-expire certificates.
Exportable Reports			
Generates detailed reports for documentation and compliance tracking.			

Advantages of the Proposed System

Ease of Use

Simplifies certificate analysis for both technical and non-technical users.

Comprehensive Insights

Detects a wide range of certificate issues to ensure robust security hygiene.

Efficiency

Automates checks and displays results in real time, saving time.

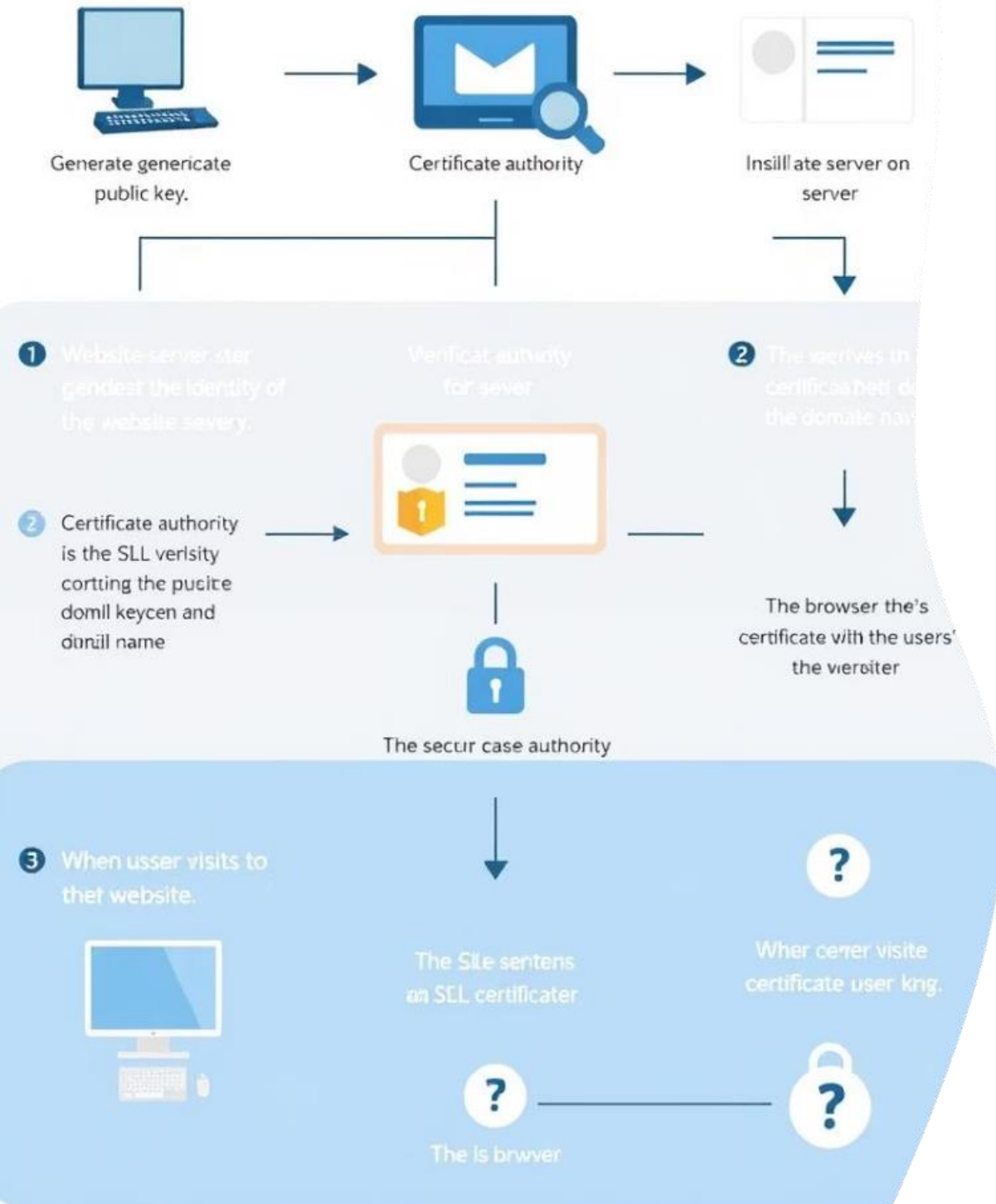
Report Generation

Facilitates documentation and tracking of security compliance.

Improved Security Posture

Helps organizations promptly identify vulnerabilities and maintain trusted connections.

SSL Certificate Analyze



How the Tool Works

1

Input URL

User enters the website address to analyze.

2

Fetch Certificate

Tool retrieves SSL/TLS certificate details automatically.

3

Analyze & Detect

Identifies issues like expiration, weak algorithms, or self-signed certificates.

4

Generate Report

Creates exportable reports for documentation and compliance.

Target Users and Benefits

Web Administrators

Gain quick insights to maintain secure websites and prevent certificate issues.

Security Professionals

Use detailed reports to track compliance and identify vulnerabilities.

Organizations

Improve overall security posture and protect user trust with proactive monitoring.



Conclusion and Next Steps

The SSL/TLS Certificate Analyzer addresses current system limitations by providing a user-friendly, efficient, and comprehensive tool for certificate analysis. It empowers users with actionable insights and report generation to maintain secure web environments.

Next steps include development, testing, and deployment to assist web administrators and security professionals in enhancing web security hygiene effectively.