



Abstract

The issue of security is very paramount in any organization, especially such organization as a bank. Therefore, intended to improve security of the bank was develop a web application that involves the scanning of uniform resource locator, showing the reputation of each uniform resource locator and send notification via email with the result of the scanning. The administrator of the web application will add the different uniform resource locator that the bank wants to scan for reputation status, add the employee email that will be receiving the notification and create the schedule of the scanning. From this project, I hope design an alternative web security system for the bank

Introduction

The goal of this project was to design a web application for daily use on the information security department since web application can be accessed through any web browser, no desktop installation or updates are required the web base project system was developed using technologies like .NET, HTML, MS SQL, Selenium for web automation & virus total API.

Background

The web application will scan different URL store in a database. Using the virus total API it will connect to the databases in the virus total site bringing the reputation of each URL if it has been reported malicious or not after the scan. Another process start to do a search in the McAfee database call trusted source its going to search for the reputation that was reported from the scanned URL. At the end of this process an email is sent to the analyst to review the results and take actions if needed. Virus Total stores all the analyses it performs, this allows users to search for reports given an MD5, SHA1, SHA256 or URL. Search responses return the latest scan performed on the resource of interest. Virus Total also allows you to search through the comments that users post on files and URLs, inspect our passive DNS data and retrieve threat intelligence details regarding domains and IP addresses. Trusted-source other component in the web applications is an Internet reputation system originally developed by Cipher Trust and now owned by Intel Security. It provides reputation scores for Internet identities, such as IP addresses, URLs, domains, and email/web content.

Problem

With the technological advances at the level of web applications the bank lacked an automatic system which could have a list of URL's and scan them quickly in different period of time. to perform this work they had an analyst reviewing each of the URL's one by one in the McAfee Trusted Source database manually. This resulted in a large consumption of time and loss of efficiency.

Methodology

In order to develop this web application a research was made to established the technologies that where going to be use technologies like virus total API , Selenium for process automatization, Bootstrap and jQuery. Tool use to make the application was Visual Studio 2017 and MSSQL.

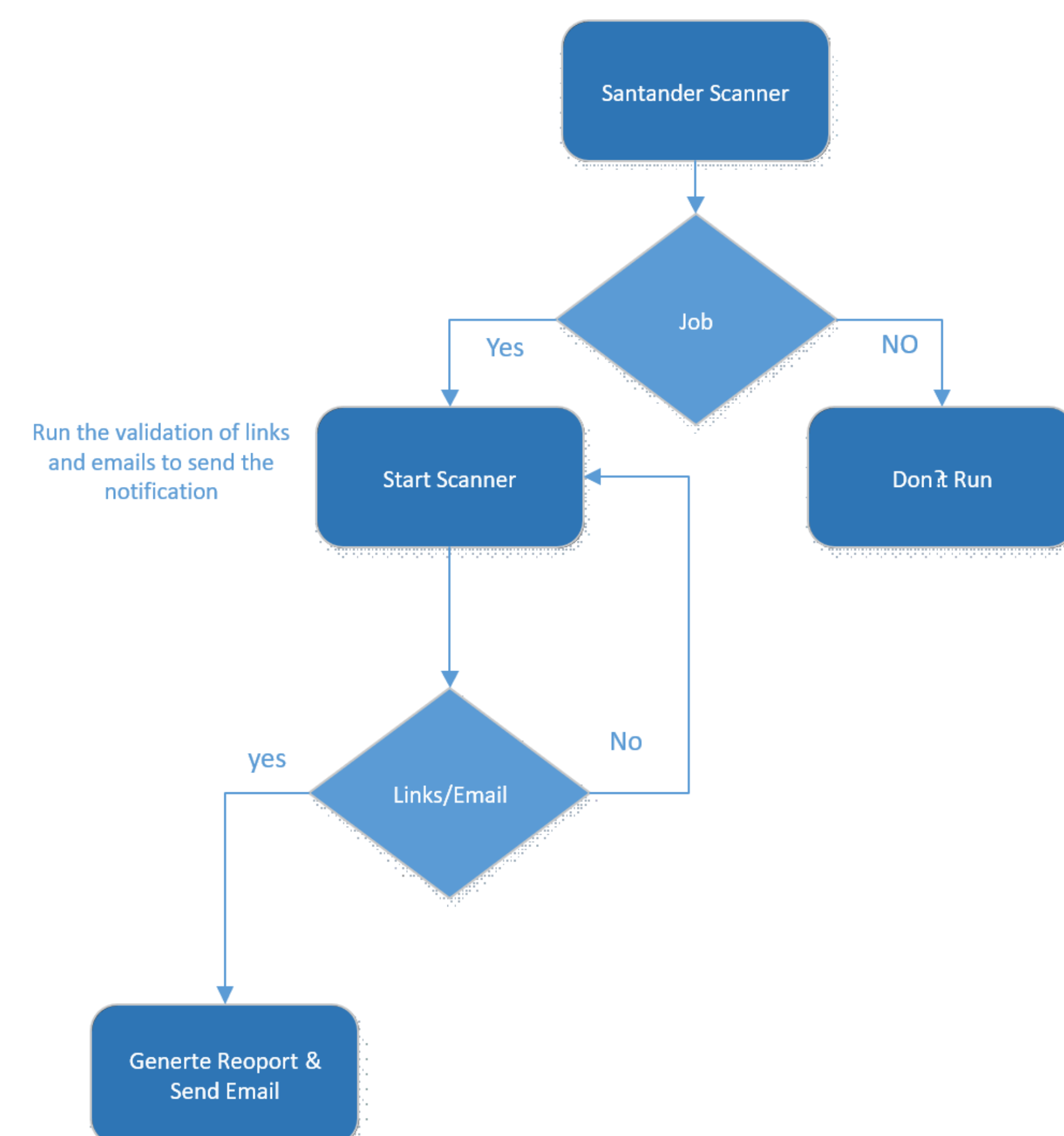


Figure 1 Flow Chart

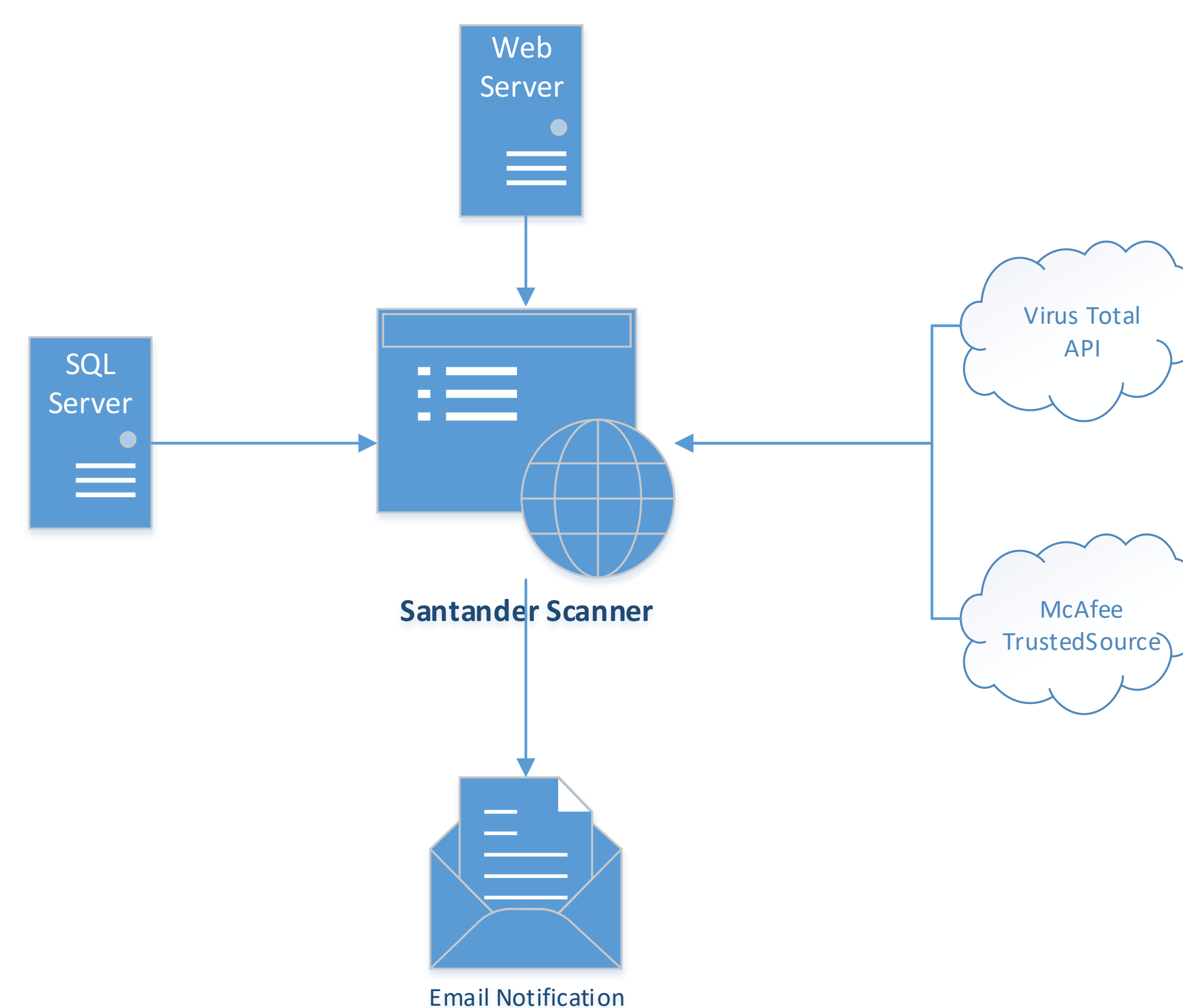


Figure 2 Infrastructure

Results and Discussion

At the end of this project we obtain a fully automated system which has a connection to a database to store the addresses and set the schedules to run the scan. then the web application will send a final report by email to the security analyst to evaluate the results.

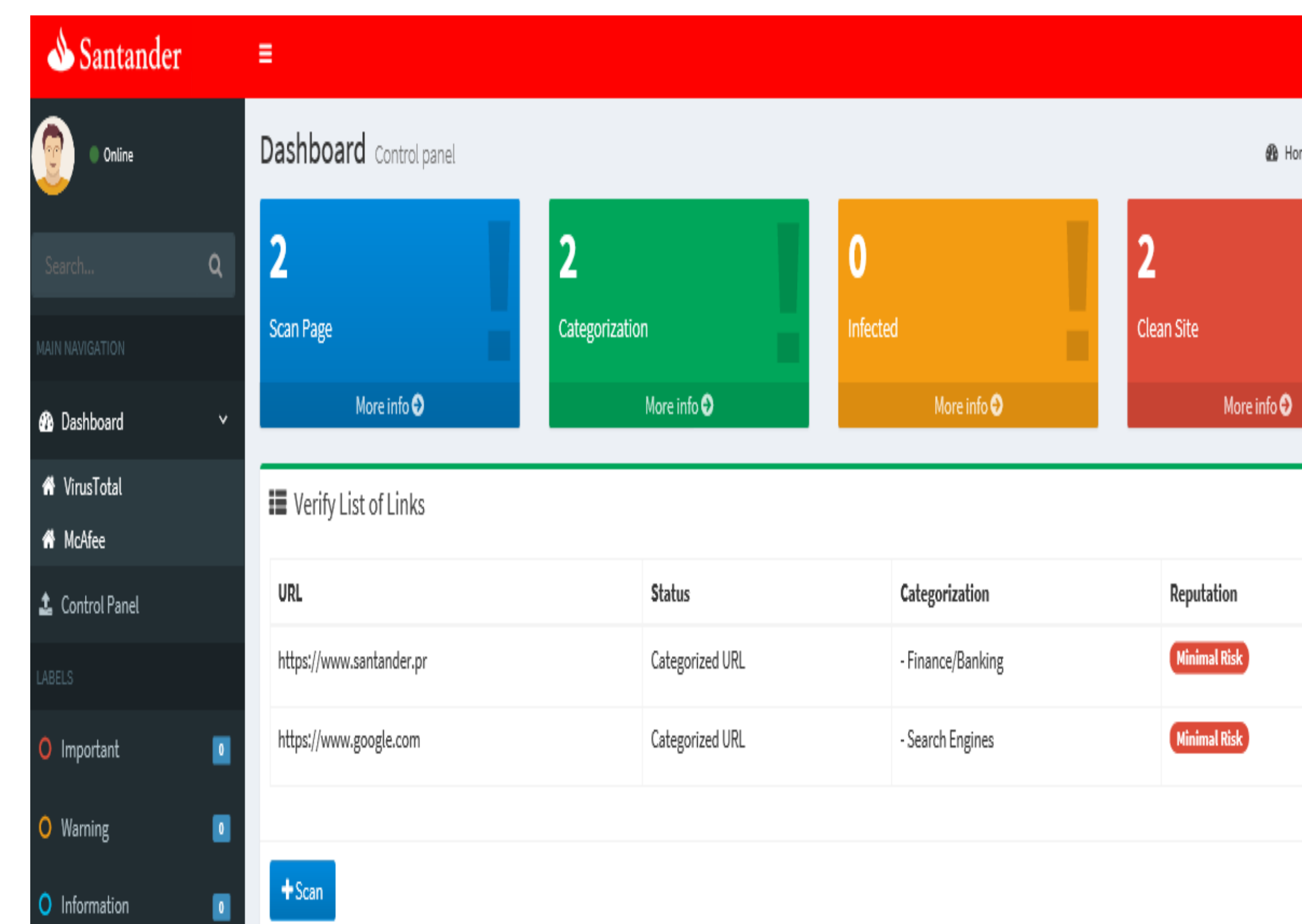


Figure 3 Trusted Source Result

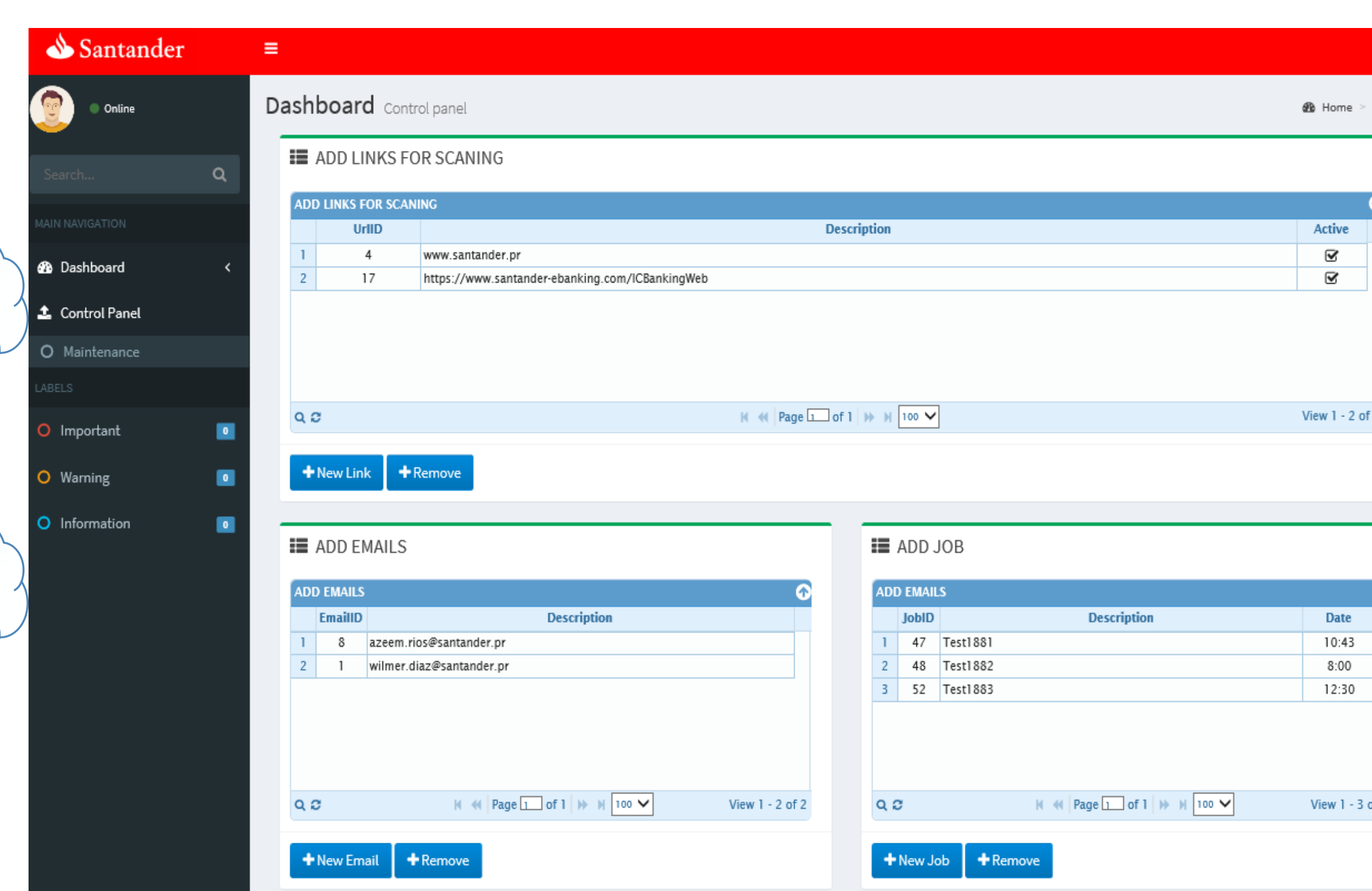


Figure 4 Maintenance Page

Conclusions

In this paper the purpose and objective of the scanner project was achieved. The final product has a GUI interfaces take away all the incidences of errors and labor and give you something manageable. The final objective of this project is to improve the process. we use the right tools; we are assured that our page would be in standard and acceptable to every visitor. This will improve the workflow and other business processes including the productivity of the information security analyst employee.

Future Work

New ideas of what more to improve or how to improve the system and what kind of new features to add, come up through the development of thesis. Another Steps could be implemented an additional module which could add a list of hash to make scan of them obtaining results of malicious categories for each of them. the notification could be implemented via text message in case of finding any malicious result to obtain a faster action of the security analyst if necessary.

Acknowledgements

I thank the operations and information security department for facilitating the execution of this project and my supervisor for continuing to support me to obtain this final product.

References

- [1] S. Project, "Browser Automation," *Selenium Documentation*, 07-May-2019. [Online]. Available: <https://www.seleniumhq.org/docs/>. [Accessed: 10-Jan-2019].
- [2] "Virus Total," *Virus Total*. [Online]. Available: <https://developers.virustotal.com/reference>. [Accessed: 10-Jan-2019].
- [3] "Customer URL Ticketing System," *McAfee*. [Online]. Available: <https://trustedsource.org/>. [Accessed: 10-Jan-2019].