AUTONOMOUS VULNERABILITY SCANNER FOR NETWORK SECURITY

Dr.S.Balaji, Mukunth Venkatesh N G, Matheswaran K K, SanthoshKumar A

Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, Tamilnadu, India

# ABSTRACT

With the advancement of technology and the pressing need for network security, vulnerability scanners have received special attention, and they are now considered a critical component for network security assurance. Various scanners have been created with the goal of detecting potential vulnerabilities in advance of harmful attacks. However, the majority of them concentrate on a single goal. In this study, an effective network vulnerability scanner is developed that combines information collecting with vulnerability detection to determine whether or not IP addresses that are available internationally are vulnerable. The experimental findings show that our tool achieves remarkable web vulnerability detection capacity with a vast scanning scope by steering the detection process with the useful acquired information.

# INTRODUCTION

User’s security has been a more worried factor since the advent of information technology. Because most software developers are unaware of the various security measures that should be implemented because their primary goal is to make the software application run in the desired state without considering the flaws that the programming language may have introduced into the system, it becomes increasingly important to devise new strategies and methodologies that will protect users from being attacked by any unauthorised access.

# EXISTING SYSTEM

The existing system uses the synchronous approach and they use the simple scanning method to ping an IP address. When a synchronous method is called, it returns a value.Before returning to the caller, it finishes executing. A synchronous programme is carried out in steps. Even with conditional branching, loops, and function calls, you may think of the code as one step at a time. The software moves on to the next stage after each step is completed.

# PROPOSED SYSTEM

The asynchronous approach is used in the proposed method. Asynchronous methods start a job in the background and immediately return to the caller. Asynchronous programmes behave in a unique way. One execution step at a time is still required. The distinction is that the system might not wait for an execution step to finish before proceeding to the next. This means that even if a previous step hasn't finished and is still running elsewhere, the programme will carry on to the next execution phase. This also implies that the software understands what to do when a prior phase completes. We use zmap in our project since it performs better than other map tools.

# LITERATURE SURVEY

1. Improving Vulnerability Performance of the Scanner in Detecting AJAX- AJAX is a new technology that arose from the evolution of the internet and web applications. AJAX applications are web applications that use this technology to generate a new trend in web applications.
2. Web vulnerability scanner evaluation-In recent years, many web apps have been released around the world.Simultaneously, cyber attacks on web application vulnerabilities have proliferated.
3. A low-cost method of analysing security vulnerability scanners-Web applications are exposed to various threats and attacks,and therefore numerous tools are developed for detecting web application vulnerabilities.

# ALGORITHM SERVER

* 1. Scan for all the publically available IP addresses.
  2. Check if the specified port is open or not for that IP while scanning.
  3. If open collect the information about the IP.
  4. After scanning all the IP,upload all the data to the database.

# CLIENT

1. The user can look at a map or look for information on a certain IP address.
2. The user must input the IP address in order to view it.

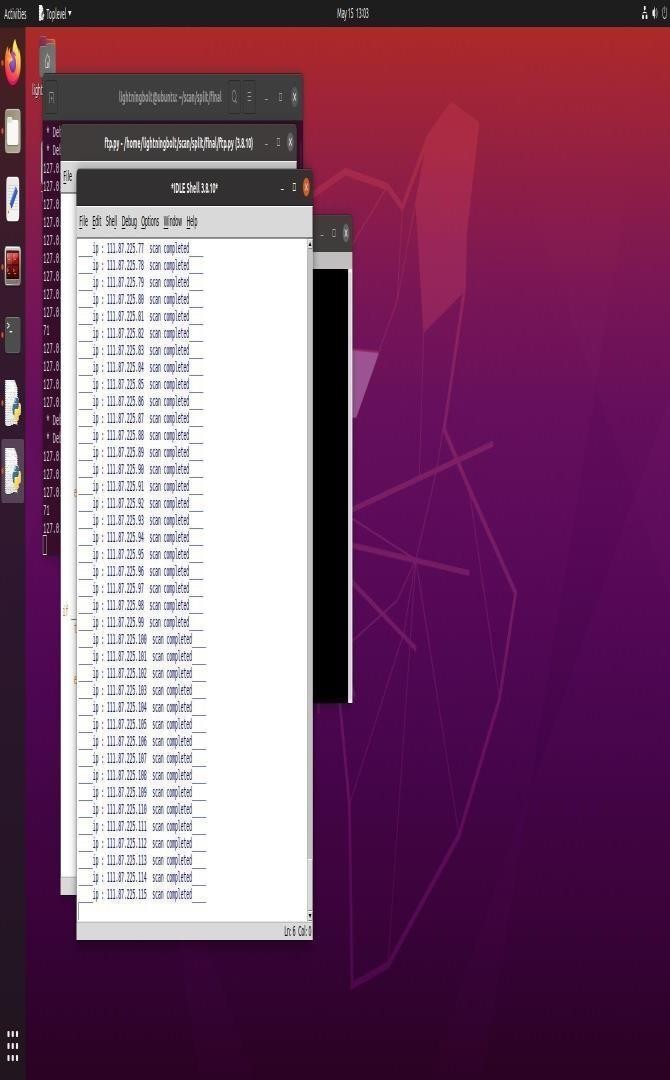
# RESULT AND ANALYSIS



1. **CONCLUSION**

In our project, we scan IP addresses and report whether they are vulnerable or not.The IP addresses are collected and stored in a database (Mongodb). The scanned data is retrieved from the database when a user enters a specific IP address and submits it. The map displays the database's gathered data, which reveals whether or not the IP is vulnerable. Finally, it displays the message "Scan done."

# REFERENCES

1. Indian Computer Emergency Response Team(CERT-In), “Annual Report- 2017”,Ministry of Electronics & Information Technology,Government of India,2018.
2. Z.Li,et AI., “VulPecker:an automated vulnerability detection system based on code similarity analysis”,ACM,Proc.of the 32 Annual Conference on Computer Security Applications,pp.201-213,2016.
3. S.O. Uwagbole, W.J.Buchanan,&L. Fan, “Applied machine learning predictive analytics to SQL injection attack detection and prevention”,IEEE, Symposium on Integrated Network and Service Management(IM),2017 IFIP/IEEE,pp.1087- 1090,2017.