*SecureByte - An app for Web Pentesting*

Dineshkumar A, 2017PECCS385  
CSE Department  
Panimalar Engineering CollegeChennai, India  
dineshkumar.a2298@gmail.comImmanuel Sanjay J, 2017PECCS403 CSE Department  
Panimalar Engineering CollegeChennai, India  
immanuelsanjay71@gmail.com

Jeeva V, 2017PECCS406  
CSE Department  
Panimalar Engineering CollegeChennai, India  
vijayjeeva2408@gmail.com

***Abstract*—*This application combines various types of web pentesting tools which perform various operations on particular targets in a single application.It generates the report of particular operations then we can analyse the generated report.The Personalized reports will be saved as report file in a text format.The report will be sent to an Prior-organization to alert them about their application or websites vulnerabilities and the system weaknesses. And the Organization may get aware about the reports and will immediately fix the loophole of the particular application or website.***

***Keywords—securebyte, web pentesting, pentesting, tools, vulnerability, application.***

# Introduction

Pentesting is a specialized security auditing method where a tester simulates an attack on a secured system. Using this application we can perform various operations. The goal of this is not to cause damage,but instead to identify attack surfaces,vulnerabilities,and other security weaknesses from the perspective of an attacker. This application contains port scanner, web server fingerprinting, directory brute force, password cracker, hashing, proxy, wifi security auditing tool,network scanning etc..,Many different tools are available in this application so we won’t go to different platform for various purposes.This helps finding out loopholes related to a particular component, be it web service, coding language, server etc and can be treated then and then.It has various security attack vectors and exploitation of potential vulnerabilities.

# Literature Survey

**Wang, S., Wang, J., Feng, C., & Pan, Z. (2016).**

* They can analyze the vulnerabilities and types of attacks on WLAN which is specified as IEEE 802.11 standard. The IEEE 802.11 WAN is a wireless network which uses radio waves to transfer the data.
* So, it is most susceptible to the security issues like WPE/WPA/WPA2 cracking, Denial of Service (DoS), and rogue access points. By siht, a ylisae rekcatta eht csecse eht srefsnart ,atad evitisnes eht s sllawerif eht ssapyb dna ,stekcap eht tpecretni . ,stekcap suoicilamThe penetrating testing ensures the security of the wireless networks.
* WAIDPS is an open-source wireless Swiss-Knife which works on Linux and is written in Python.

**B L V Vinay Kumar, K Raja Kumar, & V. Santhi (2016).**

* They investigated different Penetration testing tools using Kali Linux. This research helped to understand how to perform the different penetration tests using private networks, virtualized tools, and systems.
* t lla tceted ot desu saw gnitset noitartenep ehThe skcatta l gniffins ciffart eki. kcatta elddiM-eht-ni- naM dnaF ces dna sisylana krowten retupmoc eht rou dna pacrettE ,gnitidua ytir desu si euqinhcet tentfirD.
* The implementation also used the Wireshark for traffic sniffing. The results demonstrated that the proposed technique for penetration testing could be used successfully in real time environment.

**Salas, M., & Martins, E. (2014).**

* They proposed a technique for security testing which used the two techniques in order to detect the XSS attacks against the web services. The two techniques are Fault Injection and Penetrating Testing.
* XSS is a cross-site scripting attack on Web services which raises new security challenges.
* This type of testing technique is used to identify the sender by combining the security tokens and WSS (WS- Security).
* It also ensures the authorized access to SOAP messages communication.
* Another injection tool that was used is WSInject which introduces the faults or errors on Web Services for checking the environment behavior.

# Technology Stack

**SOFTWARE**

* Python 3
* Windows 7/8.1/10
* Visual Studio Code
* Various python modules

**HARDWARE**

* 2 GB RAM/512 GB HDD
* i3/i5/i7 Processor, 2.4 GHz
* Wifi Module
* Monitor 14/15 color

# Implementation of the algorithm

**SYSTEM MODULE**

The SecureByte contains three modules functions namely:

* Pentest tools
* Other tools
* Report

**MODULES EXPLANATION**

* **Pentest tools**

Pentest tools allow you to quickly discover and report vulnerabilities in websites,applications and network infrastructures. It provides a set of powerful and tightly integrated pentesting tools which enable you to perform easier, faster and more effective pentest engagements.These Pentest tool perform individual operations such as port scanner, dns scanner, sql scanner, directory scanner, xss scanner.

* **Other tools**

Other tools are different from the pentest tools and the operation performed is also different. The other tools are hash creator, brute hash, zip file cracker,password brute forcing, system directory scanner.

* **Report**

The report is an account or statement describing in detail an event, situation, or the like, usually as the result of observation, inquiry, etc.Here the detailed output of the each scanners will be stored as an docx file. This docx file will be retrieved through the prior directory in the file explorer for the future use.

# Algorithm

1. Make sure the Internet must be turned on for the entire session of the program
2. Open the Application -> SecureByte.exe
3. By clicking on the pentest tools drop-down box different types of scanner that perform various functions and select one of them to perform operations.

* Port scanner
* Subdomain scanner
* Sql Scanner
* Directory Scanner
* XSS scanner

1. On the other side the other tools drop-down box contains some another type of tools

* Brute Hash
* Hash creator
* Password brute forcing
* System directory scanner
* Zipfile cracker

1. Output will be displayed on the current screen and also it will be saved as a text file.
2. The text file will be used as a report that can be sent to the prior-organization .
3. The report section contains the recent outputs that were previously generated

# **Port Scanner**

A port scan is a method for determining which ports on a network are open. As ports on a computer are the place where information is sent and received. Running a port scan on a network or server reveals which ports are open and listening (receiving information), as well as revealing the presence of security devices such as firewalls that are present between the sender and the target. This technique is known as fingerprinting. It is also valuable for testing network security and the strength of the system’s firewall.

**XSS Scanner**

Cross-Site Scripting (XSS) is one of the most well known web application vulnerabilities. ... Test for XSS: For each page discovered in the previous step, the scanner will try to detect if the parameters are vulnerable to Cross-Site Scripting and report them in the results page.

**Directory Brute Forcing**

Brute force directory guessing attacks are very common attacks used against websites and web servers. They are used to find hidden and often forgotten directories on a site to try to compromise.

**Subdomain Scanner**

The Subdomain Scanner is a subdomain discovery tool. It allows you to run a scan for a top-level domain name to discover target organization subdomains configured in its hierarchy.

**SQL Scanner**

A SQL injection scanner is an automated tool used to verify the vulnerability of websites and web apps for potential SQL injection attacks. During a SQL injection attack, the hacker attempts to illegally retrieve stored database information like usernames, passwords, etc. SQL injection scanners test the websites and web apps to check whether they are prone to SQL injection attacks.

**Hash Creator**

The MD5 hashing algorithm is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message.This tool is used to create a hash output for the given input string

**Brute Hash**

Brute force is also used to crack the hash and guess a password from a given hash. In this, the hash is generated from random passwords and This tool is used to give the original string for the hashed input string.

**System directory**

The Directory Scanner allows you to scan a certain directory on the file system for files containing XML messages. Once the messages have been read, they can be passed into the core message pipeline where the full collection of message processing filters can act on them. It shows the directories present in a particular system.

**Password brute forcing**

In cryptanalysis and computer security, password brute forcing is the process of recovering passwords from data that has been stored in or transmitted by a computer system in scrambled form. This tool shows how much time it takes to crack a password using brute forcing

**Zip file cracker**

ZIP password cracker is software that you use for recovering passwords of encrypted archive files.This tool is used to crack password protected zip files.

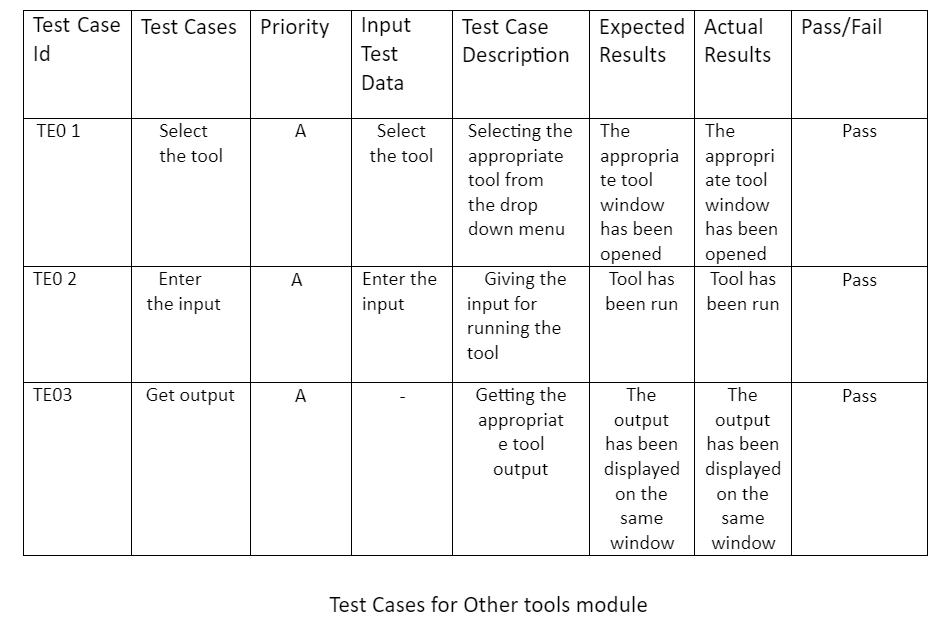
# Conclusion and Future Enhancement

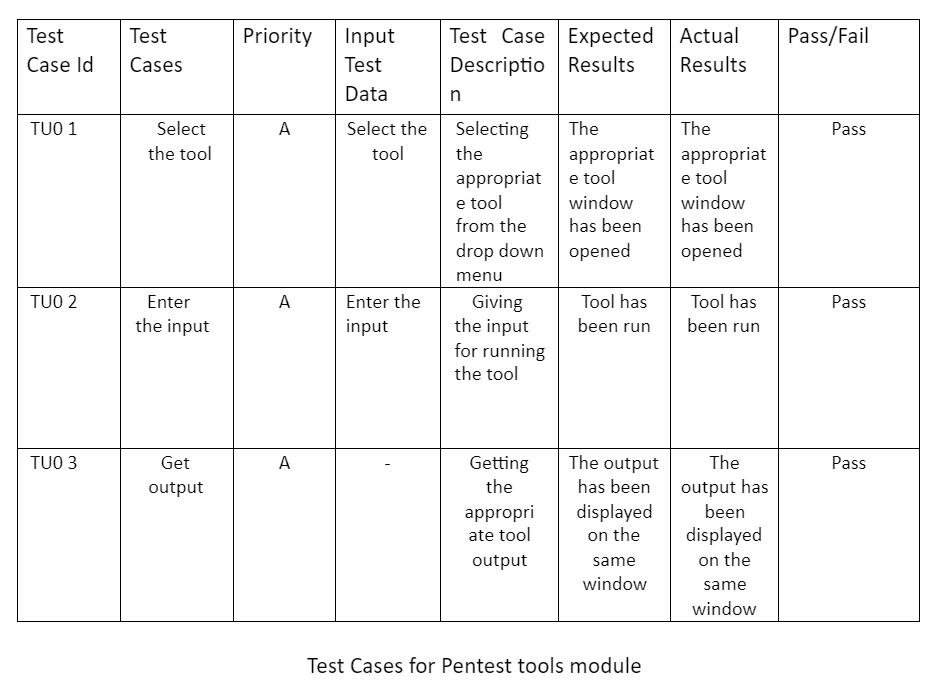
**CONCLUSION**

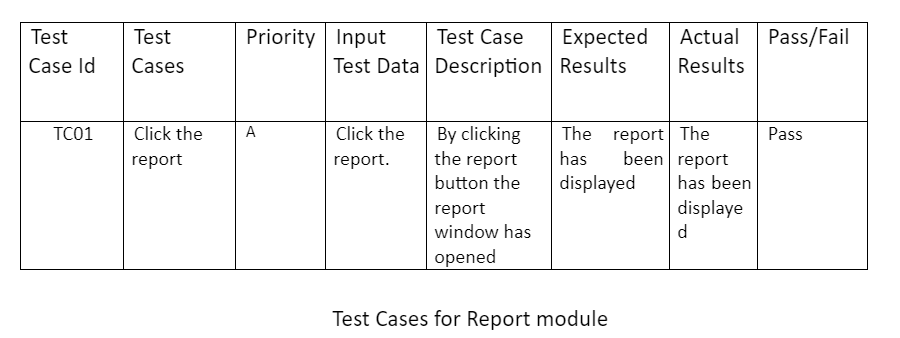
The objective of this work is to offer a fast, reliable and automated testing tool, which is also easier to use than existing tools. It contains almost all the needed tools for pentesting so it makes the process simple. It is an application so we can add as many tools as we can. It is portable, stable and reliable. Minimal configuration required. Quickly discover the attack surface of a target organization. Speed-up your pentesting engagements.

**FUTURE ENHANCEMENT**

We have created the second version of this application. In that application we have changed the UI and also we have reduced the number of files. So this application is easy to use and lightweight. The work is under progress.

1. **Testing and Performance Analysis**





##### References

[1]Mei, J. (2009). An approach for SQL injection vulner-ability detection. In Proceedings of the SixthInternational Conference on InformationTechnology.

[2] M. Khari, Sonam, Vaishali And M. Kumar, "Comprehensive Study Of Web Application Attacks And Classification," 2016 3rd International Conference On Computing For Sustainable Global Development (Indiacom), New Delhi, 2016, Pp. 2159-2164.

[3] Jose Fonseca, Marco Vieira, And Henrique Madeira, "Evaluation Of Web Security Mechanisms Using Vulnerability & Attack Injection", Dependable And Secure Computing, Ieee Transactions (Volume:11, Issue: 5)

[4]HTTPS://SIMPLYSECURE.BLOG/2017/07/05/FIVE-PHASES-OFPENETRATION-TESTING

[5] K. Nirmal, B. Janet And R. Kumar, "Web Application Vulnerabilities - The Hacker's Treasure," 2018 International Conference On Inventive Research In Computing Applications (Icirca), Coimbatore, India, 2018, Pp. 58-62.

[6] Padmaja K,"A Study On Web Application And Protection Against Vulnerability", In International Journal Of Engineering Research And Application, (Ijera),2012, Pp.001-006.

[7]"Security Code Review-Identifying Web Vulnerabilities", By Kiran Maraju.

[8] M.Khari And N.Kumar, "User Authentication Method Against Sql Injection Attack", International Journal Of Scientific And Engineering Research,2013, Pp. 1649-1653.

[9]Https://Hackernoon.Com/Timing-Based-Blind-Sql-AttacksBd276dc618dd

[10]Guo, F., Yu, Y., & Chiueh, T. (2005). Automated and safe vulnerability assessment. In Proceedings of the 21st Annual Computer Security Applications Conference.