IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 26-29

Website Protection And Analysis Using Dedicated Security Tool

Priyank Patil[1], Deepesh Warghade[2],Nileema Pathak[3]
[1](Information Technology, Mumbai University, India)
[2](Information Technology, Mumbai University, India)
[3](Information Technology, Mumbai University, India)

Abstract: *The number of users using the World Wide Web has crossed 3.8 billion and the number is increasing day by day. Today Internet touches all aspects of our life, education and economy. There has been a significant increase in hacking of websites on daily basis due to the vulnerabilities present in the websites. According to White Hat security's "2018 Website Security Statistics Report" more than 60 percent of websites had at least one serious and exploitable vulnerability open throughout the year – meaning the doors to easy exploits were wide open. It has become highly essential that each website should have a security measure in place. The main research goal of this paper is to overcome this challenge by presenting an tool which can present an analysis of websites and protection of websites from hackers.*

Keywords- *Website Security, SQLi Injection Attack , Mass Request Attack*

I. Introduction

Websites have the power to interact with their customers and thus most businesses depend on websites to sell their products. Internet currently hosts more than a billion websites and a wide range of heterogenous devices are used to access them. Due to this rapid advancements there has been a significant increase in the vulnerabilities of websites that are being hacked. Thus there are opportunities for individuals, groups or governments to perform cybercrimes and malicious activities due to this web vulnerabilities. According to White Hat security's "2018 Website Security Statistics Report" more than 60 percent of websites had at least one serious and exploitable vulnerability open throughout the year – meaning the doors to easy exploits were wide open.

The bad news is that there are number of people out there that are testing your website with a different attempt. They check your web server for vulnerabilities and unpatched flaws. The attacks range from using webpages to deliver malwares, phishing to more complex attacks like SQLi attack ,Cross site scripting ,Mass Request or Flood attack etc. With no effective website security tools in place one can expect the website security to be even more critical.

The main research goal of this paper is to overcome this challenge by presenting an tool which can present an online anomaly behaviour analysis of websites and protection of websites from hackers.

The remaining sections of the paper are organized as follows. In Section 2, we highlight how the web app work. Section 3 presents an overview of easeof use. In Section 4, we present necessity to use web security applications. In Section 5 and Section 6, we present System design and conclusions respectively.

II. Understand How Web Applicaition Works

Any program that runs in a web browser and can be accessed over the web is a web application. They provide functionality to user without having to download and install the application software. The web applications can be easily updated as the updates need not be sent to individual computers. There are three layers in a web application. The first layer is the user-side and consist of web browser that displays the content of the web pages. Second layer is the server side, that generates dynamic content pages. Third layer is the backend database where the data is stored.

III. Ease Of Use

The system consist of a simple software Web Interface and thus it would be easier for the user to analyze his/her website for any threats according to his/her convenience. The owner will just have to upload the necessary files to the server using an FTP and install our security application for his/her website. Once the system is started, the user can monitor his website and get the necessary notifications if there is any threat posing to his/her site.

IV. Necessity To Use

Sophisticated application are being developed on the web which is a complex application platforms. Hackers increasingly are targeting the web apps since software developers these days are writing secure code and developing and distributing patches to counter traditional forms of attack, such as mass requests.[2] Also, secure protection is being provided at host and network levels using the current security technologies like antivirus and network firewalls but not at application level. The main targets for attacker are the public interfaces to web applications.[1]

It is very difficult to remove the vulnerabilities in the web application mainly because of two reasons. First the web applications are developed in-house by some Management Information System engineers(MIS), most of whom have less training and experience in secure software development if compared to engineers at large software firms such as Accenture , Cognizaant , TCS , Facebook. Second, most applications go through rapid application development phases with extremely short turnaround time .

V. System Design

A. Block Diagram

Figure 1 below shows the System Block Diagram which serves as the framework of the system.

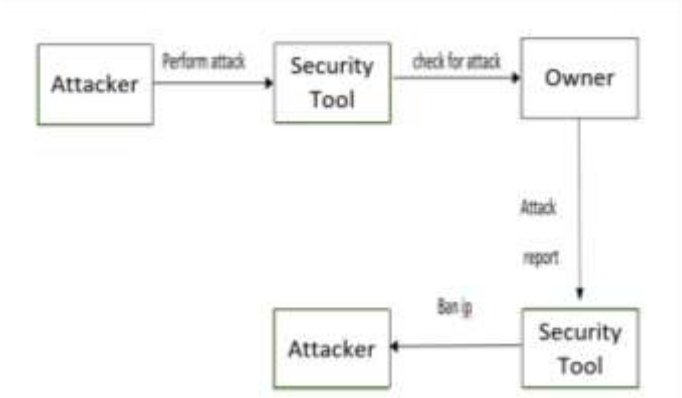

FIGURE 1 : System Block Diagram

The Attacker, Security Tool and the Owner are the main components of the system. Fig 3.1 has the following:
1)Attacker: A person who makes any attempt to expose, alter, disable, destroy, steal or gain unauthorized access.
2)ZunaSure: Software used to provides Website Security
3)Owner: A person who owes a Website and wants to secure it
SQLi Injection detection

Fig 2 below, explains the detailed steps of implementation of the system, which are as follows –

I. The attacker tries to perform an SQLi attack by inserting javascript, html tags , css tags , multiline comments, or malicious request (example: "+select+", "union+", "+or+")
II. ZunaSecure sanitizes all fields,inputs,forms by using php function filter_input_array(INPUT_GET, FILTER_SANITIZE_STRING) for both GET and POST types of submission.
ZunaSecure also performs a advanced sanitization of all fields, inputs, forms by using userdefined function cleanInput($input) which has an array of html ,javascript, css tags which need to be striped. The cleanInput($input) makes use of predefined PHP function preg_replace($search, '', $input) which helps in replacing the elements in the array with a blank field. Thus data is sanitized as ZunaSecure also has patterns, used to detect Malicous Request.
Example: $patterns = array("+select+", "+union+", "+or+",);
III. ZunaSecure notifies the owner of the site by sending an email which by sending an email notification by using an userdefined function which will make use of PHP predefined function mail($to, $subject, $message, $headers); which will include IP address of the attacker, date ,operating system information.
IV. The owner of the site can check the report on the admin panel of ZunaSecure
V. The attacker is banned by ZunaSecure by using a Ban function

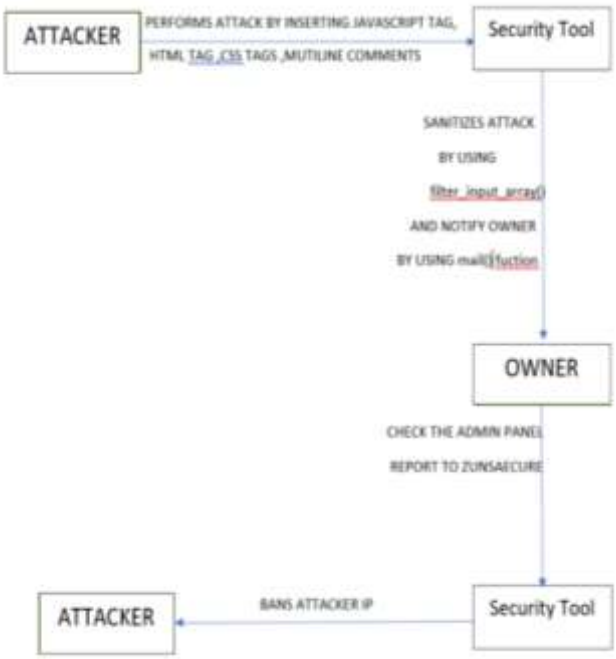

FIGURE 2: Detailed Block Diagram

Mass Request detection

Fig 3 below, explains the detailed steps of implementation of the system, which are as follows –

I. The attacker tries to perform an flood attack or mass request attack.
II. ZunaSecure checks for many requests in less than 0.1 seconds by checking the SESSION variable which is automatically generated by PHP for each browser which is live until the browser is closed . It makes use of predefined PHP function time() which deals in timestamp.
III. ZunaSecure notifies the owner of the site by sending an email which by sending an email notification by using an userdefined function which will make use of PHP predefined function mail($to, $subject, $message, $headers); which will include IP address of the attacker, date ,operating system information.
IV. The owner of the site can check the report on the admin panel of ZunaSecure
V. The attacker is banned by ZunaSecure by using a userdefined Ban function

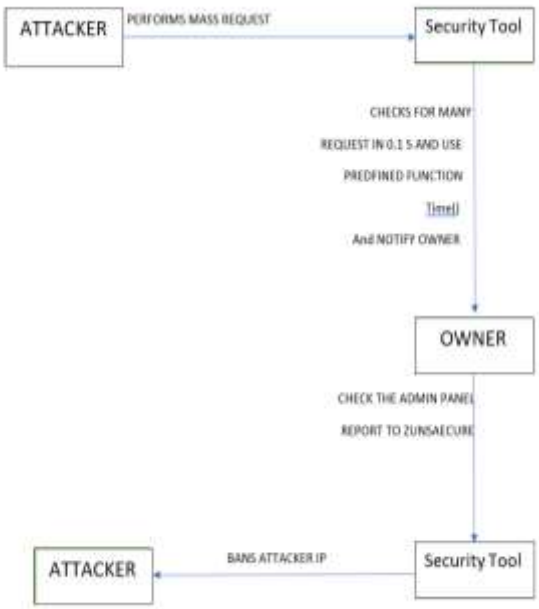

FIGURE 3: Detailed Block Diagram

VI. Expected Results

This paper aims to provide secure and reliable protection services to website users and owner through an dedicated security tool. Web Application Interface will be designed as such so as to monitor the websites and protection to the websites will be provided through autobanning of malicious IPs.

VII. Conclusion

The developed Security Tool will be a powerful website application that will protect websites of clients from hackers, attacks and other threats. It will give protection to website from SQLi Attack(SQL Injection),Mass Requests(Flood), Spammers. The admin panel will provide online anomaly behavior analysis of websites (e.g., HTML files) to detect any malicious codes or pages that have been injected by web attacks. Thus this Security Tool will personalise the website data and increases the website security.

References

[1]. Anomaly Behaviour Analysis of Website Vulnerabilty and Security.Author: Pratik Satam ,Douglas Kelly , and Salim Haririhttps://ieeexplore.ieee.org/document/7945697

[2]. White Hat security's "2018 Website Security Statistics Report"https://www.whitehatsec.com/blog/2018-whitehat-app-sec-statistics-report/