International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 05-19 www.ijaem.net ISSN: 2395-5252

Security Vulnerabilities in Modern Web Applications: Detection and Prevention

Lawal, K.H
Computer Science Department Federal University of Technology Minna, Nigeria

Date of Submission: 25-12-2023 Date of Acceptance: 05-01-2024

ABSTRACT:
In the realm of computer science and its myriad innovations, we find ourselves immersed in a vast and ever-evolving domain. In the contemporary epoch, a ceaseless influx of novel applications, websites, and software is witnessed on a daily basis. In tandem with the advent of novel applications and software, there is a concomitant escalation in the proliferation of threats and the emergence of vulnerabilities in the realm of security. Web applications, in their essence, are software programmes that cater to the needs of customers by offering a plethora of practical functionalities. However, it is imperative to acknowledge that due to the proficiency of developers in adhering to sound programming principles, web applications possess a dual nature, wherein they can be exploited by malicious entities as well. The primary objective of web application security lies in safeguarding the integrity and confidentiality of vital web-based resources, while concurrently guaranteeing the secure transmission of data. The enforcement of application safety is imperative across all facets of infrastructure, encompassing the very web application that underpins the web applications in question. Numerous organisations presently employ a form of web application protection framework or endeavour to construct and cultivate one. However, the majority of these frameworks exhibit an inherent inability to consistently and effectively generate value. Consequently, they fail to enhance the mindset of developers in constructing and designing robust web applications.
The primary objective of this article is to undertake a comprehensive analysis of the various attacks perpetrated against websites, with a particular focus on the security scanners employed for web applications. By doing so, we aim to provide valuable insights and recommendations that can assist in effectively mitigating the challenges associated with web application security.

Keywords: web applications, threats, attacks, security

I. INTRODUCTION

In recent years, there has been a notable proliferation of online applications, particularly those that operate through the World Wide Web. While precise statistics regarding the global quantity of web applications remain elusive, it is worth noting that as of the initial quarter of 2020, an estimated 367 million domain names were recorded [1]. It is pertinent to acknowledge that each of these domains has the potential to encompass either a static or dynamic web application, thereby contributing to the overall landscape of this digital realm [1]. The aforementioned applications possess the capability to engage in the exchange and processing of sensitive information pertaining to the denizens of the World Wide Web. Consequently, these web-based applications tend to garner the attention of nefarious entities who harbour malicious intent. The proliferation of web applications has emerged as an indispensable facet of contemporary existence, both in terms of its economic implications and its impact on personal spheres.

Regrettably, a substantial proportion exceeding 90% of these systems exhibit vulnerabilities, thereby compromising their security. Moreover, it is noteworthy to mention that each programme, on average, manifests a total of 13 bugs. In the realm of web applications, it is imperative to acknowledge the paramount significance of security [2].

Numerous contemporary web applications represent highly utilitarian platform architectures that facilitate the transmission of services and information between diverse clientele and businesses. Enterprises, as exemplified, have employed web-based software as a means to fortify and augment their operational endeavours, thereby facilitating the optimisation of resources in the domains of production, cost savings, education, and

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 05-19 www.ijaem.net ISSN: 2395-5252

governance. The advent of the World Wide Web has necessitated the augmentation of intranet applications within the confines of corporate websites for each respective organisation. The proficient implementation of web applications in both the realm of communication and the corporate sector renders it a highly pertinent and indispensable domain within the realm of productive industries [3].

Over the course of approximately the past ten months, a considerable number of enterprises have embraced the utilisation of the Internet as a cost-effective platform for establishing communication channels and facilitating the dissemination of information to potential customers, as well as facilitating commercial transactions. The advent of the internet has bestowed upon advertisers a unique opportunity to acquaint themselves with and establish connections with individuals who frequent their online platforms.

One potential approach to achieve this objective entails soliciting online users to subscribe to electronic mail communications, submitting a formal inquiry form to obtain product-related information, or tailoring their browsing encounter to cater to their individual preferences during subsequent visits to a specific website [4].

In the contemporary era, online technologies have assumed a significant role in the automation of conventional daily tasks through the implementation of updated solutions. The ubiquity and popularity of the Internet and various web service providers can be attributed to their widespread adoption by a staggering 3.88 billion users across the globe [5]. This remarkable figure can be attributed to the inherent advantages offered by these digital platforms, namely their unrestricted availability and ease of access, which enable users to utilise them freely and conveniently from any location.

In recent years, the occurrence of IT security infringements has engendered significant predicaments for a multitude of stakeholders, encompassing customers, states, businesses, and companies alike. The contemporary occurrences of diurnal information attrition and the misappropriation of substantial monetary sums by a multitude of cyber adversaries are commonly observed phenomena. Despite the existence of a considerable body of research on the subject matter of cyber and web vulnerability, it is important to note that further investigation and analysis are still required to fully comprehend the intricacies and complexities of this phenomenon. Nevertheless, it is imperative that we now divert our attention towards exploring novel methodologies for mitigating the perils associated with risks, malware, cybercriminal activities, and other related detriments [6].

In the subsequent segment of this scholarly manuscript, we expound upon the contextual knowledge that elucidates the significance of web applications and their pervasive presence in our surroundings. This ubiquity has consequently engendered a multitude of security vulnerabilities and incursions. In addition, we shall expound upon the fundamental tenets of the Central Intelligence Agency (CIA) that necessitate implementation in order to ensure the utmost confidentiality and safeguarding of web-based applications. In Section III, we engage in a comprehensive examination of the various security threats that afflict web applications. In the fourth section, we present a comprehensive analysis of the security recommendations aimed at effectively mitigating the aforementioned threats.

The ensuing discourse shall be expounded upon in Section V. In the sixth section of our scholarly discourse, we proceed to draw a comprehensive conclusion and articulate the significant contribution that our paper has made to the existing body of knowledge.

II. BACKGROUND

The topic at hand pertains to the realm of web applications security, which encompasses the various measures and techniques employed to safeguard the integrity, confidentiality, and availability of web-based applications. This field of study is of utmost importance in

Security tests for web applications serve as a means of validating the secure execution of said applications. The primary objective of security testing is to detect and mitigate any potential flaws, thereby preventing their inclusion in the final product, and ultimately ensuring that the application's security measures are commensurate with the desired level of protection [7].

The exceedingly dynamic web framework expands its attack surface in order to encompass a diverse range of vulnerabilities. Web applications, when developed utilising the contemporary HTML5 specifications and harnessing the expanding capabilities of JavaScript, exhibit a lack of anomaly. Furthermore, these web applications possess the capacity to supplant traditional desktop applications, thereby encompassing a wider range of functionalities. One plausible approach to mitigating this augmented level of complexity entails the process of debugging various devices.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 05-19 www.ijaem.net ISSN: 2395-5252

The successful implementation of operating systems, libraries, and compiled programmes has been well-documented in the field of software development. However, it is worth noting that the extent to which these advancements can be applied to web applications has yet to be thoroughly explored [8].

The application of the CIA (Confidentiality, Integrity, Availability) principles is imperative for all individuals and organisations, as they serve as fundamental standards to be adhered to in order to guarantee the security of web applications. Figure 1 depicts the aforementioned principles.

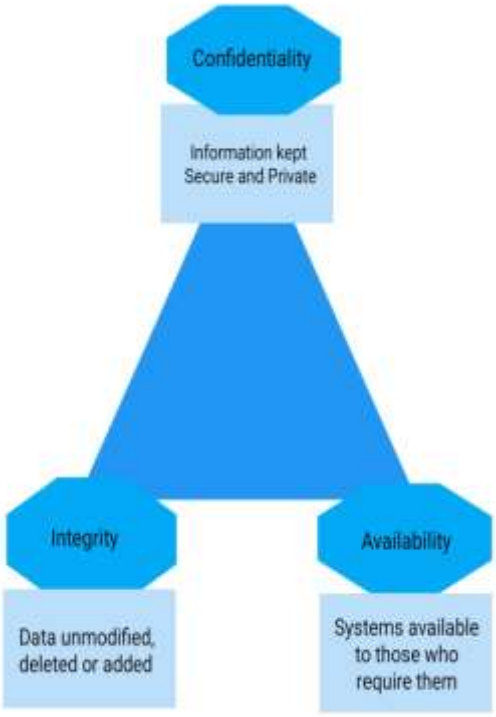

Fig 1: CIA Principles

Confidentiality:

The concept of confidentiality serves as a safeguard, ensuring that solely those individuals who possess the requisite authority are granted access to peruse or examine the contents of a given website. In order to anticipate the actions of unfamiliar individuals, designers employ the practice of premeditating the arrangement of various applications. Initially, the focus is placed on designing positions for these applications, as opposed to granting the ability to modify the administrator, website, theme, or plugin. Consequently, a user who is distinct from the administrator is unable to make alterations to the theme. Through the act of interchanging roles, specifically pertaining to the manipulation of data and user list records, it becomes apparent that the manager assumes a position of prominence and visibility.

The ability to forecast such occurrences can be achieved by developers through the strategic formulation of positions that cater to the needs and expectations of their consumer base, thereby preemptively addressing potential challenges posed by individuals lacking expertise in the field. The modification of the website theme and/or plugin is restricted solely to the administrator, thereby precluding any alterations by other individuals. Henceforth, it is imperative to acknowledge that any individual, apart from the designated administrator, lacks the authority to make alterations to the subject matter at hand. In order to gain visibility of this particular administrator, it is imperative to engage in a reciprocal exchange of positions, wherein pertinent information such as specific details or user listings are shared.

Integrity:

The concept of integrity acknowledges that the manipulation or deletion of data within a server or website is restricted to authorised individuals exclusively. Consequently, the process of transferring files between a server and a computer, or vice versa, commonly referred to as uploading or downloading, is not inherently secure in terms of website utilisation. In a parallel vein, one must contemplate the potential ramifications of a file undergoing modification, be it through alteration of its nomenclature or its substantive contents, in relation to the likelihood of a viral assault. Frequently, an individual occupying a subordinate role relative to that of a manager possesses the capacity, albeit lacking the requisite authorization for modifications or eradication of records, to engage in such activities (in specific instances, inadvertently). The aforementioned course of action may be one that the user finds displeasing, yet is nonetheless undertaken due to a technical glitch within the web application. The imperative task at hand necessitates the unequivocal avoidance of such practices in order to enhance the overall security of a website. One viable methodology entails the utilisation of a prescribed protocol, specifically the evaluative framework, which necessitates inclusion within the software engineering workflow. The testing procedure encompasses two distinct facets: The examination and analysis of the Black Box The

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 05-19 www.ijaem.net ISSN: 2395-5252

examination of the white box In essence, the evaluation of the black box entails a rigorous examination of the software's functionality, primarily targeting individuals who promptly engage with the website, thereby assuming the role of end-users. White box testing, also known as clear box testing or structural testing, is a meticulous testing methodology that endeavours to assess the internal workings of software functions written in various programming languages, including but not limited to PHP. The white box testing process is divided into three distinct tests, each contingent upon the nature of the input, the program's functionality, or the values of the input.

Availability:

The concept of availability pertains to the necessity of the site's accessibility for the user's intended utilisation. The ability to navigate a website without encountering errors is indicative of the website's adherence to the principle of compatibility. If feasible, it would be advantageous for a website to remain accessible for a continuous duration of 24 hours a day, spanning across all seven days of a week, commonly referred to as 24/7 availability. This necessitates the requirement for openness.

In the realm of information security, the preservation of confidentiality guarantees that the data residing within a computer system or database remains exclusively accessible to individuals who have undergone the process of registration. Conversely, the concept of functionality denotes the capacity of a web application to be conveniently accessed by its user at any desired moment. The apparent contradiction and resemblance to the initial theory notwithstanding, it is noteworthy that these two principles exhibit a degree of differentiation due to the presentation of divergent perspectives.

The paramount importance of website usability is underscored. The proposition at hand pertains to the formulation of a concept that encompasses the provision of instantaneous feedback. This notion revolves around the idea of promptly delivering evaluative information to individuals, thereby enabling them to receive immediate insights and assessments pertaining A method that operates in real-time, grounded in logical reasoning derived from factual information and the timely assessment of its effects on performance outcomes. By employing such a mechanism, various apparatuses such as engines, cables, telescopes, and other similar instruments can be effectively supervised and regulated.

In the context of developing a framework for a Web Security Analyzer, it is imperative to consider the provision of real-time power, which is frequently required for telecommunications equipment and computer systems. In this regard, the concept of real-time reviews would be expanded to encompass the search functionality of the website, thereby enabling the delivery of outcomes pertaining to securitization vulnerabilities. Furthermore, these outcomes would be accompanied by suggestions that possess the capability to effectively rectify the identified weaknesses.

Algorithms:

This scholarly article presents a novel approach for implementing an automated scanning procedure, wherein data from multiple resource shares are extracted from the system to facilitate the security validation process on a website. This approach leverages the model matching principle employed in the Microservice Architecture. The ensuing articulation pertains to a scheme designed for the purpose of conducting a comprehensive scan to identify deficiencies in the realm of website safety.

The user's text, "F," could be rephrased in a more scholarly manner as follows Moodle, an open-source framework that is readily accessible to the public, possesses the capacity to be utilised and modified by any individual in possession of a licence for the GNU (General Public Licence) programme. Users have the opportunity to procure the Moodle software by accessing the web address: http://www.moodle.org. Moodle serves as a catalyst for fostering student-centered pedagogy, which in turn facilitates the eLearning paradigm, commonly referred to as distance learning.

This particular model serves to facilitate students in not only accessing and retrieving the subject matter, but also actively engaging in the educational process. Moreover, it is worth noting that instructors possess the ability to disseminate educational resources to their students at any given moment, unencumbered by the constraints imposed by geographical distance and physical limitations. The instructor possesses the capability to upload supplementary materials from external online sources, encompassing textual statements, visual presentations, auditory recordings, audiovisual content, as well as hyperlinks [10].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 05-19 www.ijaem.net ISSN: 2395-5252

III. THE SECURITY THREATS THAT PLAGUE WEB APPLICATIONS.

It is an undeniable fact that the digital landscape is rife with pernicious elements seeking to exploit vulnerabilities in these applications. Thus, it becomes imperative to comprehend the nature and characteristics of these threats in order to fortify the system. Web applications are susceptible to a plethora of malevolent attacks that exert a detrimental influence on the functionality and performance of said applications.
Within this particular segment of our scholarly investigation, we shall undertake a comprehensive examination of the most perilous attacks and susceptibilities to which web applications are susceptible.

Cross Site Scripting (XSS):

This phenomenon commonly referred to as Cross Site Scripting (XSS) in the realm of web-based attacks is characterized by the submission or execution of malevolent web code through the victim's computer browser, typically in the form of scripts, within their Web applications. This execution process facilitates the extraction of personal data or pilfering of cookies from the user, thereby enabling the fraudulent acquisition of their identity during a session. Furthermore, this exploit empowers attackers to abscond with or gain control over other devices containing sensitive information [11].

SQL Injection:

The SQL Injection issue pertains to a vulnerability within the system's security framework, wherein an adversary is able to exploit the flaw by transmitting a SQL query to the database residing in the system's back-end. The inherent syntax and functionality of SQL, coupled with the robustness and adaptability of the underlying database and its associated features, can be leveraged by a malicious actor to manipulate the transmitted data in a manner that is advantageous to their nefarious intentions [12].

Remote File Inclusion (RFI):

This is a web server script attack, wherein an individual of nefarious intent seeks to exploit vulnerabilities within a web server's script functionality. The ultimate objective of this attack is to gain unauthorized access to the server and remotely introduce a file of the attacker's choosing. The aforementioned attack possesses the potential to facilitate the illicit acquisition of data or the execution of malicious code, notably JavaScript, thereby instigating subsequent assaults on the client-side. The presence of this limitation is a direct consequence of the user's input, which, unfortunately, lacks the necessary level of verification and confirmation [13].

Denial of Service (DoS):

A web security threat, in which an attacker deliberately disrupts the services of a host that is interconnected with the vast network of the Internet, results in the temporary or permanent inaccessibility of a computer or network infrastructure to its intended users. In order to circumvent the fulfillment of specific or all legitimate requests, it is customary to employ a technique known as network overload, whereby the target equipment is inundated with an excessive volume of undesired solicitations [14].

Buffer Overflow:

The occurrence of a buffer overflow arises when a malevolent attacker endeavors to intentionally transmit a quantity of data that surpasses the capacity of a given program or procedure to accommodate. The occurrence of such an aggressive act has the potential to result in a system failure [15].

Cross-Site Request Forgery (CSRF):

This is a popular internet attack which involves the deliberate manipulation of a user's behavior in order to elicit the transmission of erroneous and potentially harmful HTTP requests to a web application that is presently susceptible to such exploits. The fundamental tenet of CSRF resides in the fact that the user's browser inadvertently dispatches nefarious requests to the Web Application, thereby rendering them indistinguishable from the anticipated benign requests that have been duly authorized by the user [16].

Unrestricted File Upload (UFU)

This is the utilization of errors inherent in server-side web app content filtering tests. The aforementioned entity, widely recognized as an upload assailant, strategically leverages their restricted authorization to submit deliberately corrupted files, thereby exploiting the inherent susceptibilities of the UFU system. In the hypothetical scenario where a file is submitted under duress, there is a possibility for the emergence of a code execution vulnerability [17].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 05-19 www.ijaem.net ISSN: 2395-5252

SYN flood DDoS attack:

The TCP SYN flood, also known as a flood, represents a form of distributed denial-of-service (DDoS) assault that capitalizes on a vulnerability within the conventional three-step TCP handshake process. Its primary objective is to deplete resources and render the targeted server incapable of fulfilling its intended functions, thereby resulting in unauthorized access. The assailant primarily engages in the expeditious transmission of TCP link requests through the utilization of a SYN flood distributed denial-of-service (DDoS) attack, thereby inducing network saturation as a consequential outcome [18].

Broken Authentication and Session Management:

This is a manifestation of web vulnerability that arises as a consequence of inadequate configuration of session management protocols. Upon the successful completion of an authentication procedure, a session shall be established, thereby facilitating the seamless exchange of data between the server and an individual user [19].

Security Misconfiguration:

Sensitive data encompasses a variety of confidential information, such as usernames, credit card details, passwords, and other pertinent data of similar nature. Upon encountering a flaw within the application's security infrastructure, it became apparent that a vulnerability had manifested itself. The potential perpetrator possesses the capability to divulge the aforementioned data, thereby compromising its confidentiality. Furthermore, it is imperative to note that there exist three distinct vulnerabilities that can be exploited in order to carry out said attack. The initial concern pertains to an attack vector commonly referred to as an information leak. The second phenomenon under consideration pertains to what is commonly referred to as a transmission attack. The third pertains to the illicit acquisition of a database [20].

IV. SECURITY RECOMMENDATIONS

This particular segment of the research encompasses an extensive examination of numerous studies conducted by esteemed researchers, focusing on a plethora of solutions and methodologies employed for the identification and mitigation of security vulnerabilities that give rise to malevolent attacks. In the year 2017, a collective of individuals formed a study group with the intention of developing a tool for the analysis of malicious scripts within web applications. This tool, aptly named XSS-Check, was specifically designed to identify and detect cross-site scripting vulnerabilities. This particular system serves the purpose of ascertaining user feedback pertaining to a web page that has been returned, validating the functionality of web pages that involve login procedures, and furnishing details regarding encoded HTTP headers and the DOM parameter. Upon being explicitly defined, both the server and the client undergo validation processes within the realm of dynamic web pages. In order to provide a comprehensive understanding, Figure 2 illustrates the flow chart pertaining to the supplementary user interface designed for the purpose of XSS (Cross-Site Scripting) screening, as referenced in source [21].

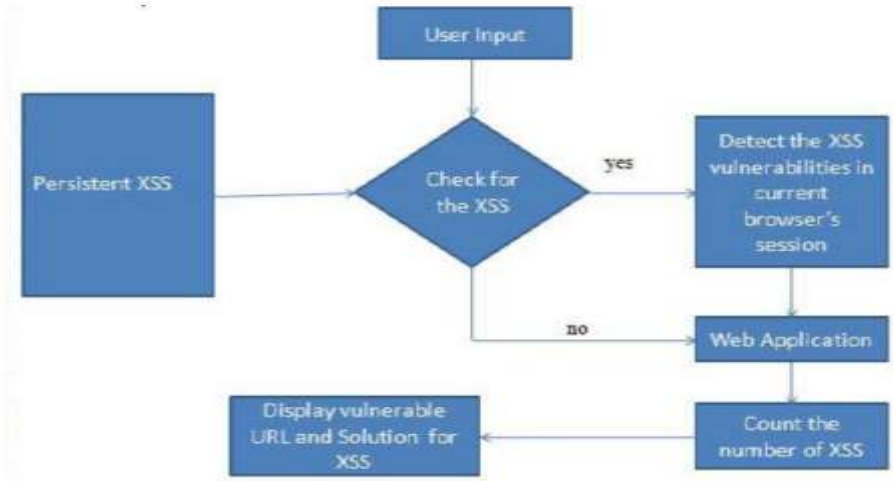

Fig. 2 Flow Diagram of XSS-Check add-on User Interface [21]

In the year 2019, a group of scholars introduced a novel approach for the identification and subsequent comparison of Elastic Pooling Convolutional Neural Network-based Structured Query Language (SQL) injection, hereafter referred to as EPCNN. The proposed EP-CNN-based SQL injection recognition system demonstrates the ability to autonomously extract latent SQL injection traffic characteristics, thereby effectively identifying attack traffic that manages to evade detection by the Fast SQL normal injection mechanism. The crux of the matter lies in a solitary letter, yet the veracity of one's credentials can be upheld through the examination of all interrogative assertions. In the event that the lexicon at one's disposal is constrained, it is plausible to mitigate the intricacy and expenditures associated with the pedagogical process. The conventional approach to identification can be wholly substituted by a proficient model that is subject to real-time modifications. Subsequently, we shall proceed with a comprehensive examination of the assault forms, employing a multi-class model that transcends the limitations imposed by a singular SQL attack definition. The aforementioned methodology facilitates the production of a stationary two-dimensional matrix that is devoid of any data truncation, while concurrently exhibiting a high level of proficiency in identifying instances of SQL injection within web-based applications [22]. In the year 2020, a comprehensive examination was conducted by researchers to identify and document the various vulnerabilities inherent in web applications. Among the weaknesses identified were the potential risks associated with remote file integration. To ascertain the extent of these security vulnerabilities and assess the potential for security breaches, the researchers employed the utilization of Open-Source software. This approach facilitated the identification of multiple security vulnerabilities and enabled the conduction of penetration testing, commonly referred to as Vulnerability Assessment and Penetration Testing (VAPT), specifically tailored to web applications. The identification of security infringements has come to the fore. The utilization of Vulnerability Assessment and Penetration Testing (VAPT) Security Test Tools proves to be highly advantageous in the realm of web application defense, as it effectively mitigates the risk of safety breaches and ensures the absence of any violations [23].

In the year 2018, the authors introduced Rampart, a novel mechanism devised to counteract the pernicious effects of sophisticated Denial-of-Service (DOS) attacks specifically targeting web applications. Through the utilization of mathematical methodologies and the meticulous analysis of program profiling within various functions, Rampar adeptly discerns and effectively mitigates the pernicious threat of advanced central processing unit (CPU) degradation stemming from denial-of-service (DOS) attacks. Moreover, it is worth noting that Rampart has been introduced as a notable augmentation to the PHP Zend engine. The aforementioned approach amalgamates and operationalizes various filtering mechanisms in order to identify and counteract forthcoming adversarial assaults, while concurrently minimizing the potential deleterious consequences on authentic users. The utilization of the filter serves the purpose of impeding subsequent perils and eradicating plausible detriment to individuals who abide by the law. The filter is synthesized and subsequently employed. The efficacy of Rampart in terms of overhead is relatively negligible, as it can be implemented in any PHP application without necessitating alterations to the program's source code. The aforementioned study demonstrates the efficacy of Rampart in providing security measures for two widely utilized web applications, namely Word Press and Drupal. Specifically, it highlights the effectiveness of Rampart in safeguarding against both real-world and synthetic CPU exhaust attacks. Furthermore, the study emphasizes that the Ram component of Rampart plays a crucial role in maintaining the overall reliability of web services. This is achieved by ensuring not only a minimal occurrence of false positives but also a significantly reduced rate of false negatives [24]. The implementation of mitigating measures against buffer overflow attacks encompasses the employment of restricted locks, the utilization of security libraries, and the practice of static code review. In order to impose limitations on the quantity of characters to be transmitted as input, software developers employ the utilization of JavaScript and HTML. Nevertheless, it is conceivable to modify the HTML structure by employing a skilled individual with expertise in hacking techniques, thereby disabling the Java Script functionality, subsequently executing a buffer overflow attack. The meticulous management of client feedback on the server is imperative in order to safeguard the program against this particular threat. Furthermore, it is worth noting that an application has the capability to deploy a firewall or security gateway in order to scrutinize requests that exhibit an exceptional duration [15].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 05-19 www.ijaem.net ISSN: 2395-5252

In the year 2018, a group of diligent scholars undertook the task of devising a contemporary web-based framework, which serves the noble purpose of safeguarding web applications against the pernicious threat of Cross-Site Request Forgery (CSRF) attacks. Through a comprehensive examination of the historical and behavioral aspects of consumer inquiries, the traditional WAF (Web Application Firewall) methodology has been expanded and enhanced. In light of the antecedent endeavors undertaken by the user, it is evident that a comprehensive analysis of their past activities is warranted. The esteemed scientists have undertaken the implementation of a traditional Web Application Firewall (WAF) program in order to safeguard against fraudulent attacks perpetrated by malicious software during the process of their downloading. The aforementioned approach enhances the overall efficacy and aesthetic of the submission. The potential for further refinement and enhanced efficiency in the future is evident [25]. In the year 2020, a group of esteemed researchers successfully devised FUSE, an advanced penetration testing platform specifically designed for the purpose of identifying vulnerabilities within server-side PHP web applications, with a particular focus on the UFU (Unrestricted File Upload) aspect. The primary objective of FUSE is to construct download inquiries, whereby each inquiry assumes the role of a payload exploit that subverts the integrity of UFU (University File Uploader) and UEFU (University External File Uploader). In the present inquiry, the user has expressed a desire to undertake a PHP programming examination pertaining to a specific method. A total of 30 instances of the UEFU (User-Executed File Upload) vulnerability were meticulously examined by the FUSE (File Upload Security Evaluation) research team. Within this corpus, a notable subset of 15 instances were identified as CVEs (Common Vulnerabilities and Exposures), which are standardized identifiers for publicly known cybersecurity vulnerabilities. The primary objective of this investigation was to illustrate the inherent functional benefits that can be derived from the deliberate exploitation of file upload mechanisms, specifically by inducing code execution errors. The aforementioned numerical notation, specifically denoted as [17], serves as a reference to a particular source or In the year 2020, a group of esteemed researchers proposed a novel approach aimed at mitigating the pernicious TCP SYN Flood (Denial-of-Service) attacks. Their method involved harnessing the capabilities of the venerable Linux operating system, specifically employing the CSF (ConfigServer Security & Firewall) and SPI (Stateful Packet Inspection) proof of concept (PoC) techniques. There exist three distinct methodologies by which the security process may be conducted.

In the pursuit of establishing a comprehensive IP server link and fortifying the security of incoming SYN packets, it has been observed that the frequency at which a minimum packet-based IP address encounters SYN breaches within a given timeframe is a crucial factor in determining the threshold at which the firewall intervenes. It has been ascertained that CSF, a sophisticated Linux firewall tool, possesses the intelligence required to effectively combat the TCP SYN Flood type of Denial of Service (DoS) attack, employing stateful packet inspection (SPI) techniques. The TCP SYN Flood (Denial of Service) attack modality can likewise be ameliorated in a prompt and effortless manner. Moreover, it is worth noting that CSF (ConfigServer Security & Firewall) presents a more streamlined and expeditious approach to mitigating a minor instance of network disruption, specifically the TCP SYN Flood (Denial of Service) attack. In addition to the aforementioned alternatives, it is worth noting the existence of other viable methodologies. These include the Advanced Political Firewall (APF), the conventional Firewall, the IP Blank Path server system, and the Cloudflare service. However, the utilization of CSF offers additional benefits that are contingent upon the specific configuration settings found within the /etc/csf/csf.conf file. In the realm of cybersecurity, the concept of attack avoidance holds paramount importance. It is worth noting that ConfigServer Security & Firewall (CSF) serves as a robust defense mechanism, effectively thwarting various forms of denial-of-service (DoS) attacks. Furthermore, it is pertinent to highlight that CSF offers the professional administrator the ability to tailor its functionalities to suit their specific requirements, thus enhancing its efficacy in safeguarding the system from potential threats.According to the provided reference, specifically CONF [26], it can be inferred that there is a specific piece of information or evidence that supports a particular In the year 2020, a diligent researcher successfully devised an algorithmic solution that exhibits the capability to securely facilitate the registration process and navigation of web applications. This accomplished individual meticulously crafted an algorithm that possesses the remarkable ability to safeguard the integrity of the registration procedure and ensure secure access

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 05-19 www.ijaem.net ISSN: 2395-5252

to web applications. The hypothesis proposed is based on the principles of zero-based awareness proof. The inception of a dynamic random number generation can be traced back to the utilization of the prevailing chaotic 6-dimensional hyperplane. It is essential to note that each facet of this hyperplane possesses a unique pin code, which is applicable to both the web client and the user. The completion of the registration process for these two numerical entities, devoid of any accompanying password, has been accomplished. The findings of the study have elucidated the inherent worth of the proposed approach, which adeptly and reliably oversees the management and dissemination of cryptographic keys. The utilization of chaos-induced stochastic processes in generating random numbers has been found to exhibit a commendable level of reliability. The methodology exhibits a pronounced propensity for randomness, as each numerical value manifests an inherent unpredictability. Through the utilization of the existing authentication scheme, it has been effectively safeguarded against potential malevolent actors and legitimate users from acquiring access to member keys. This fortification has been achieved by the strategic amalgamation of the Zero Knowledge method with the proposed intricate mechanism and the utilization of the robust RSA algorithm. The utilization of dynamic and robust keys is prevalent within the framework of the system under consideration. The aforementioned statement ensures that both the client and the web application maintain a state of confidentiality and authentication, as indicated by reference [27]. In the year 2018, a group of investigators undertook a comprehensive examination of an operator's perspective regarding the initial resolution to the multifaceted challenges arising from the implementation of defensive measures with potentially detrimental consequences for humanity. It has been observed that instances of security issues do not invariably result in accidents. A notable proportion of participants, precisely one-third, reported that their instances of misapprehension culminated in a safety event. Furthermore, it was discovered that human error was often instigated by the intricacies of device operations. Through the lens of systemic, personal, and interpersonal influences, one can discern the multifaceted factors that shape and mold individuals and their behaviors. These influences, which operate at various levels, intricately interact to shape the thoughts, beliefs, and actions of individuals within a given context. By examining these influences The scholars have put forth a series of imperative action items that are both necessary and beneficial in nature. Regrettably, these recommendations are frequently disregarded by various organizations, thereby resulting in a diminished effort to mitigate the frequency and impact of security configuration errors. The aforementioned text comprises the subsequent elements. The present discourse concerns the subjects of documentation, transparency, and post-mortems with a particular focus on the phenomenon of blurred post-mortems. Additionally, the matter of outsourcing systems and procedures shall be addressed. These topics have been extensively explored in the existing literature, as evidenced by the citation [28]. In the year 2017, a group of scholars put forth a series of proposed remedies to mitigate the risks associated with exposure to attacks targeting sensitive data. These solutions encompassed various measures, such as the safeguarding of sensitive data through the implementation of encryption techniques. Additionally, it was suggested that the storage of sensory data, while not an absolute requirement, could serve as an additional layer of protection. Furthermore, the utilization of standardized algorithms and robust cryptographic keys was recommended to fortify the security of sensitive information. Moreover, the deactivation of web pages containing sensitive data was advocated as a means to minimize the potential for unauthorized access. Lastly, the conscientious handling of sensitive data was emphasized as an essential aspect of safeguarding its integrity and confidentiality. The algorithm in question possesses a formidable capacity for preserving passwords in a secure manner. Employing Secure Sockets Layer (SSL) as an additional security measure. The user's text is a numerical value, which does not require any rewriting in the style of a university In the year 2020, a cohort of esteemed scholars put forth a proposition for a novel web-based detective model. This model, rooted in the principles of in-depth learning, possesses the capability to furnish the receiver launch curve's precision pertaining to both anomalous and benign web queries. The present model employs an automated coding mechanism, thereby enabling its capacity to acquire knowledge and assess various linguistic units, encompassing both words and letters, within sequences of textual content. To effectively categorize atypical inquiries based on the nature of their assault. The classification engine has undergone training using the results obtained from the ECML-KDD dataset. The empirical evidence presented in this study elucidates that the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 05-19 www.ijaem.net ISSN: 2395-5252

aforementioned model exhibited a commendable capability in discerning and identifying instances of web application attacks. The suggested classification engine exhibits a level of reliability that falls short of attaining a perfect score of 100%. However, it is worth noting that in subsequent endeavors, the incorporation of a larger corpus of data holds the potential to enhance the performance and efficacy of the classification engine [30].

In the year 2019, a group of esteemed researchers from the EPICS institution put forth a proposal pertaining to the security policy paradigm within dynamic network systems. Their focus was primarily centered around the fundamental notion that data, in contemporary times, possess the characteristic of being readily accessible from various locations. However, it is imperative to acknowledge that such accessibility is perpetually accompanied by a set of access policies, processes, and communication protocols. The process of data transformation gives rise to the emergence of EPICS, which stands for Extended Process Information and Control System. Furthermore, it is imperative to transform said entity into an active agent that possesses the ability to safeguard itself against undesired detection and manipulation. In the event of potential hazards, engine AB shall undertake the task of detecting and identifying said threats. EPICS, with the intention of circumventing identification, facilitates the dynamic loss of data. In order to illustrate the proposed system, the researchers opted to employ the context of e-commerce. The EPICS framework confers a substantial benefit. To ensure the preservation of data security, it is imperative to uphold the principles of regulated data dissemination and mitigate the level of transparency. In order to ensure the enforcement of policies at both ends of the relationship, it is imperative for consumers to engage in data exchange without possessing a comprehensive understanding of the direction of data divulgation. This approach enables the determination of access management rules, thereby facilitating the seamless flow of information between parties involved. The aforementioned entities exhibit a TTP-independent nature, thereby indicating a lack of reliance on trusted third parties. Furthermore, they explicitly request the data custodian to refrain from disseminating the data during the process of information exchange with the primary provider. Provide the instantiation of contextual adaptive data predicated upon the utilization of extrinsic information pertaining to the surrounding milieu (such as confidence metrics, emergency scenarios, or instances of hostile actions) and the malleability of governing principles. The mitigation of customer knowledge management liability for the service is achieved through the practice of selectively disclosing information that aligns with the parameters established by the customer's policy. In accordance with contemporary network infrastructures, particularly those predicated upon the principles of Representational State Transfer (REST), with a specific emphasis on the Hypertext Transfer Protocol (HTTP), the aforementioned system is deemed to be compatible. The system in question is devoid of any specific policies and instead encompasses a diverse range of prevalent authentication and authorization protocols. Furthermore, it possesses the capability to seamlessly integrate into any data distribution application. Figure 3 provides a visual representation of the endeavors undertaken by the EPICS (Engineering Projects in Community Service) program.

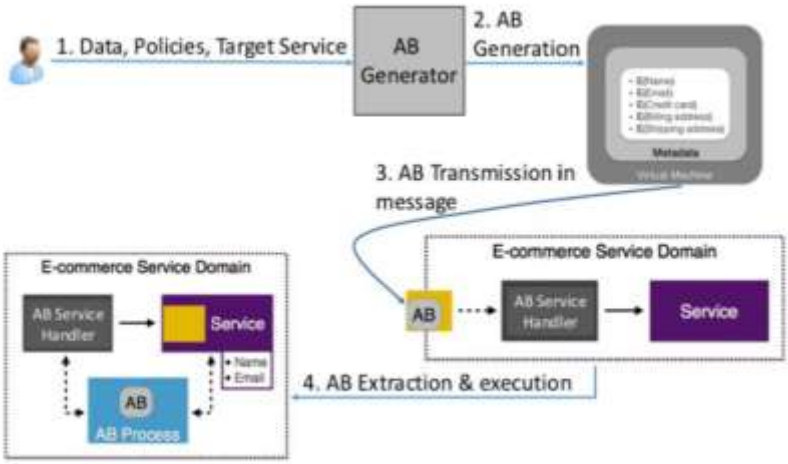

Fig. 3: EPICS operation [31].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 05-19 www.ijaem.net ISSN: 2395-5252

In 2020, developers proposed the utilization of SNEAKERS, a tool designed to detect and assess bugs within web applications. SNEAKERS has successfully identified and evaluated vulnerabilities present in exploitable networks, subsequently providing recommendations for their resolution. This discourse revolves around the exploration of strategies aimed at mitigating the risk of unauthorized access to sensitive company data and information. Specifically, the focus lies on the identification and rectification of security vulnerabilities within web applications, which are often targeted by hackers. SNEAKERS serves as a testbed application designed for utilization on both the Windows and Linux platforms.

The mentioned tool, known as SNEAKERS web vulnerability evaluation and scanner [32], serves the purpose of identifying web vulnerabilities and providing a Web Admin solution.

In 2020, researchers presented their findings on the design of static, dynamic, and collaborative protection methods for technical and algorithm testing. The objective of this analysis is to investigate methods for enhancing efficiency and reducing the occurrence of false positives. In order to comprehensively investigate the behavior of applications, it is essential to employ a combination of two static, two dynamic, and two immersive methods of data analysis. This approach allows for the consideration of vulnerabilities outlined in the OWASP Top Ten, as well as the evaluation of distinct scripts with varying levels of criticality within the analyzed applications. This study explores and analyzes the metrics utilized for each n-tool combination to enhance the security of web applications through the integration of an Interactive Application Security Testing (IAST) tool. One can infer that the utilization of both IAST and DAST tools typically results in favorable outcomes. However, it is worth noting that the rate of false-positives is higher in comparison to the individual utilization of IAST and DAST tools. The utilization of combined tools, such as Fortify + Arahni + CCE or Fortify + ZAP + CCE, along with the integration of SAST + DAST + IAST, has demonstrated excellent performance in the categorizations of large, medium, and small systems [33].

In the year 2018, vulnerability scanners were employed to optimize the performance of automated web applications. The JARVIS application, known as the JARVIS tool, offers feasible technological alternatives for various vulnerability detectors. These alternatives aim to address the limitations that currently prevent the availability of such detectors in the system. The utilization of JARVIS significantly enhances the efficacy of vulnerability detection by increasing the efficiency of five readily available scanners by over 100% in comparison to their default configurations. JARVIS's configuration effort is not dependent on the type of scanner being used, thus allowing for efficient utilization of multiple scanners simultaneously. The authors have conducted a study on the feasibility and limitations of employing multiple scanners simultaneously. Their findings indicate that the utilization of multiple scanners proves advantageous as the number of identified vulnerabilities increases. Furthermore, they observed no noteworthy adverse effects on the examination of false positives. The user has provided a numerical reference, [34].

V. DISCUSSION

The present analysis aims to explore various strategies that have been investigated by numerous researchers in order to protect web applications from the perils of malware threats. The OWASP software is widely recognized for its robust security features and is frequently employed to safeguard open-source web applications.

Researchers have developed a method to assess the safety efficiency of Static Application Security Testing (SAST) instruments. This method involves utilizing different forms of vulnerabilities from each OWASP group as test cases. The reproducibility of SAST instruments can be assessed and categorized by comparing them. The analysis of bugs found in these instruments reveals a significant variation in the percentage of bugs across different tools. Instruments with summon values falling within the range of 0.34 to 0.57, excluding spot-bugs, exhibit unfavorable consequences. Proficient individuals or teams possessing expertise in the target code's language and specialized knowledge of security vulnerabilities should consistently conduct comprehensive vulnerability assessments. The evolving design and advancement of technology in online applications have led to numerous enhancements in vulnerability categories throughout the years. Future studies are imperative for the tool to consistently identify the prevailing and significant vulnerability categories. Regular revisions are necessary for the OWASP Top Ten. The analysis further substantiates the enhancement of true positive (TP) and false positive (FP) ratios

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 01 Jan 2024, pp: 05-19 www.ijaem.net ISSN: 2395-5252

through the utilization of multiple static application security testing (SAST) instruments.

Several researchers have proposed the use of an OWASP Stinger-based tool for the purpose of validating input fields. Additionally, they have recommended the creation of a compilation of regular terms and a sterilizing mechanism. The objective is to establish effective security measures against common injection attacks in web applications. This involves the examination of essential characters (including letters, numbers, periods, dashes, question marks, and exclamation marks) as well as complex data formats such as JSON and XML files. The examination should be conducted for each domain to ensure comprehensive protection. A protection mechanism has been implemented to mitigate regular injection attacks. The attack tool consists of a console that has been developed in two phases to handle routing requests. The initial phase involves directing the first fictional submission to a later-phi, which is then forwarded to the web application if it is deemed incorrect. The proposal filter underwent testing in three standardized applications as well as a genuine application. The results indicate an accuracy rate of 98.4 percent and a total loading time of 50ms in a confidential web application. The proposed filter demonstrates a notable level of stability, leading to the inference that increased computational capacity can be achieved. The aforementioned requirements are not obligatory.

This section will discuss the features of Twitter spam detection. Twitter, a prominent website with 313 million daily monthly users, receives approximately 500 million tweets per day. Twitter is utilized by spammers for various purposes, including targeting genuine users, spreading harmful software and advertisements through tweets containing URLs, aggressively following legitimate users, and exploiting popular topics to attract attention and disseminate pornography. The effectiveness of these tactics contributes to the spammers' prominence. In order to maintain a spam-free environment on Twitter, it is imperative to implement measures that enable the tracking and filtering of spammers who target legitimate users. The identification of Twitter spam necessitates distinct approaches compared to conventional email spam detection methods. This study explores various approaches to spam detection, specifically focusing on account-driven, tweet-based, graphical, and hybrid methods. Spammers tend to avoid using complete URLs and instead opt for condensed URLs. Twitter, being a platform with a vast network of posts, profiles, lists, moments, and links, serves as a foundation for these detection techniques. The detection of spam on Twitter necessitates a rigorous approach due to the presence of legitimate users who, under certain circumstances, exhibit similarities to spammers.

Twitter, like any other platform, is not immune to false positive detections. It has been acknowledged that there are instances where spammers are mistakenly identified as legitimate users.

Account-based methods involve the examination of various account-related characteristics, some of which are commonly exploited by spammers. These characteristics include the quantity of tweets sent by the account, the number of account lists created, the frequency of account creation through the brand-new account function, and the amount of account mentions received. Additionally, the number of lists created by the account itself is also taken into consideration. A network of bots can exploit various factors, such as the number of supporters, the percentage of followers, the number of tweets liked by others, and the proportion of retweeted tweets.

Bots employ various mechanisms to execute automated tasks, such as tracking an individual's activities and posting tweets on their behalf. This study examines the identification of spam propagation by bots through the analysis of Twitter accounts. Specifically, it focuses on detecting a network of command and control (C&C) accounts and determining if their tweets exhibit significant similarities to recently posted tweets.

The utilization of real-time spam detection, enabling instant review, proves adequate for the effective utilization of account-based functionality. The quantity of user lists serves as a useful metric in identifying spammers, as it reflects the impact a user has on others. However, it is important to note that this measure can be manipulated through the creation of fraudulent lists and the inclusion of fictitious command and control (C&C) accounts within said lists.

Account-based features are effective in identifying real-time spam that requires immediate review. However, spammers are adept at circumventing these features. The methods of tweet identification involve analyzing various aspects of the tweet, such as the number of tweets and hashtags, the number of recipes sent and received, Twitter content, tweet analysis, tweet URL, tweet place, and tweet postal date.

The inspection of tweet URLs is imperative due to the prevalence of malicious URLs as a primary medium for spam transmission.

As a result, the majority of spam prevention methods employed on Twitter involve the examination of tweet URLs. The conventional approaches to spam filtering involve the utilization of blacklisting techniques, which involve the identification and blocking of specific domains and URLs associated with spam. Spammers often struggle to effectively identify and block harmful URLs on Twitter. This is primarily due to their preference for utilizing shortened URLs and relying on conventional methods such as blacklisting specific URLs or IP addresses. Grier et al. have further illustrated the inadequacy of blacklist-based solutions in effectively protecting users. This is due to the inherent sluggishness of these solutions, as the malicious URLs tend to emerge prior to their inclusion in the database. The tweet features, akin to accounts, possess a discerning ability to detect spam. This noteworthy attribute necessitates prompt and ongoing analytical evaluation.

Graphic methods are employed to identify spam by analyzing the connectivity and distance between spam accounts and the sender. These methods also assess the connectivity of these accounts to determine the likelihood of spam connectivity. Graph-based features pose a greater challenge for exploitation compared to accounts and Tweet-based features. The removal of these features necessitates a comprehensive examination of the intricate and resource-intensive Twitter graph. The insufficiency of graphical functionality in real-time spamming is a consequential outcome. The focus of this analysis lies in contrasting detentions with account-based and tweet-based features. The graph-dependent approach in analyzing tweets is commonly limited by the assumption that tweets from friends are always well-intentioned, regardless of their actual content. However, this assumption does not hold true in cases where attackers gain control of legitimate user accounts for malicious activities.

VI. CONCLUSION

Web applications have become integral to our daily lives, serving as a means of communication with various Internet-connected platforms. These applications are designed to meet diverse needs and have consequently gained significant importance. Our analysis focused on the protection of web applications, specifically addressing the most detrimental threats and security flaws that pose risks to both the applications themselves and their users. We explored the potential consequences of these vulnerabilities on the overall workflow and safety of web applications and their consumers. Our analysis encompasses a comprehensive examination of multiple studies pertaining to alternative approaches for enhancing the security of web applications, as well as the potential opportunities available to researchers in this domain. The method discussed exhibits positive attributes and holds potential for further improvement. Specifically, it focuses on the development of efficient solutions for detecting security vulnerabilities that lead to attacks on web applications. Through our analysis, we have identified various tools and scanners that aid in this process. Consequently, we have formulated recommendations for both developers and users.

The developers' contributions in our research involve recommending the development of detection and protection tools and scanners for future studies. Our research has reviewed several such tools, considering the continuous evolution of web applications. The aforementioned studies contribute to the advancement of standards in identifying security vulnerabilities that lead to malicious attacks. It is highly advisable for users to employ robust passwords and periodically modify them. It is advisable to exercise caution when interacting with links, notices, or advertisements, as well as refraining from downloading cookies from websites, unless the reliability of said website has been duly established. It is highly advisable to utilize browsers that are widely acknowledged and known for their security measures. It is advisable for the user to ensure that their web browsers are regularly updated to the most recent version.

REFERENCES

[1]. Sönmez, F. Ö., & Kiliç, B. G. (2021). Holistic Web Application Security Visualization for Multi-Project and Multi-Phase Dynamic Application Security Test Results. IEEE Access, 9, 25858-25884.

[2]. Zech, P., Felderer, M., & Breu, R. (2019). Knowledge-based security testing of web applications by logic programming. International Journal on Software Tools for Technology Transfer, 21(2), 221-246.

[3]. Raveena, K., Elavarasi, K., & Kaaviyapriya, M. (2018). Survey-web application development.

[4]. Dhivya, K., Kumar, P. P., Saravanan, D., & Pajany, M. (2018). Evaluation of Web Security Mechanisms Using Vulnerability & Sql Attack Injection.

International Journal of Pure and Applied Mathematics, 119(14), 989-996.

[5]. Shahzad, F. (2017). Modern and responsive mobile-enabled web applications. Procedia Computer Science, 110, 410-415.

[6]. Biswas, S., Sajal, M. M. H. K., Afrin, T., Bhuiyan, T., & Hassan, M. (2018). A study on remote code execution vulnerability in web applications. In International Conference on Cyber Security and Computer Science (ICONCS 2018).

[7]. Mohanty, S., Acharya, A. A., Mishra, D. B., & Panda, N. (2019). Security Testing of Web Applications UsingThreat Modeling: A Systematic Review. IJCSMC International Journal of Computer Science and Mobile Computing, 8(1), 50-57.

[8]. Azad, B. A., Laperdrix, P., & Nikiforakis, N. (2019). Less is more: Quantifying the security benefits of debloating web applications. In 28th {USENIX} Security Symposium ({USENIX} Security (pp. 1697-1714).

[9]. Ali, A. N. M. B. M., & Elshoush, H. T. Secure Web Application Service Detecting–XSS Attacks.

[10]. Andrian, R., & Fauzi, A. (2020). Security scanner for web applications case study: Learning management system. Jurnal Online Informatika, 4(2), 63-68.

[11]. [Wibowo, R. M., & Sulaksono, A. (2021). Web Vulnerability Through Cross Site Scripting (XSS) Detection with OWASPSecurity Shepherd. Indonesian Journal of Information Systems, 3(2), 149-159.

[12]. Akbar, M., & Ridha, M. A. F. (2018). SQL Injection and Cross Site Scripting Prevention using OWASP ModSecurity Web Application Firewall. JOIV: International Journal on Informatics Visualization, 2(4), 286-292.

[13]. Rahman, M. A., Amjad, M., Ahmed, B., & Siddik, M. S. (2020, January). Analyzing web application vulnerabilities: an empirical study on e-commerce sector in Bangladesh. In Proceedings of the international conference on computing advancements (pp. 1-6).

[14]. Rajakumaran, G., Venkataraman, N., & Mukkamala, R. R. (2020). Denial of Service Attack Prediction Using Gradient Descent Algorithm. SN Computer Science, 1(1), 1-8.

[15]. Awad, M., Ali, M., Takruri, M., & Ismail, S. (2019). Security vulnerabilities related to web-based data. Telkomnika, 17(2), 852- 856.

[16]. Khodayari, S., & Pellegrino, G. (2021). JAW: Studying Client-side CSRF withHybrid Property Graphs and Declarative Traversals. In USENIX Security Symposium.

[17]. Lee, T., Wi, S., Lee, S., & Son, S. (2020, February). FUSE: Finding File Upload Bugs via Penetration Testing. In 2020 Network and Distributed System Security Symposium. Network & Distributed System Security Symposium.

[18]. Zeebaree, S. R., Jacksi, K., & Zebari, R. R. (2020). Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers. Indones. J. Electr. Eng. Comput. Sci, 19(1), 510-517.

[19]. Hassan, M. M., Nipa, S. S., Akter, M., Haque, R., Deepa, F. N., Rahman, M., ... & Sharif, M. H. (2018). Broken authentication and session management vulnerability: a case study of web application. International Journal of Simulation Systems, Science & Technology, 19(2), 6-1.

[20]. Fredj, O. B., Krichen, M., Hamam, H., & Derhab, A. (2020). An OWASP Top Ten Driven Survey on Web Application Protection Methods.

[21]. Jasmine, M. S., Devi, K., & George, G. (2017). Detecting XSS Based Web Application Vulnerabilities. International Journal of Computer Technology & Applications, 8(2), 291-297.

[22]. Xie, X., Ren, C., Fu, Y., Xu, J., & Guo, J. (2019). Sql injection detection for web applications based on elastic-pooling cnn. IEEE Access, 7, 151475-151481.

[23]. Malekar, V.,& Ghode, S. A Review on Vulnerability Assessment and Penetration Testing Open Source Tools for Web Application Security.

[24]. Meng, W., Qian, C., Hao, S., Borgolte, K., Vigna, G., Kruegel, C., & Lee, W. (2018). Rampart: Protecting Web applications from CPU- exhaustion denial-of-service attacks. In 27th {USENIX} Security Symposium ({USENIX} Security 18) (pp. 393-410).

[25]. Meng, W., Qian, C., Hao, S., Borgolte, K., Vigna, G., Kruegel, C., & Lee, W. (2018). Rampart: Protecting Web applications from CPU- exhaustion denial-of-service attacks. In 27th {USENIX} Security Symposium ({USENIX} Security 18) (pp. 393-410).

[26]. Pratama, I. P. A. E. (2020). TCP SYN Flood (DoS) Attack Prevention Using SPI Method on CSF: A PoC. Bulletin of Computer Science and Electrical Engineering, 1(2), 63-72.

[27]. Mohammed, S. J., & Mehdi, S. A. (2020). Web application authentication using ZKP and novel 6D chaotic system. Indonesian Journal of Electrical Engineering and Computer Science, 20(3), 1522- 1529.

[28]. Dietrich, C., Krombholz, K., Borgolte, K., & Fiebig, T. (2018, October). Investigating system operators' perspective on security misconfigurations. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1272- 1289).

[29]. Vamsi Mohan, V., & Malik, S. (2017). DEBUNKING OF COMMON.

[30]. Alma, T., & Das, M. L. (2020). Web Application Attack Detection using Deep Learning. arXiv preprint arXiv:2011.03181.

[31]. Ranchal, R., Bhargava, B., Angin, P., & ben Othmane, L. (2018). Epics: A framework for enforcing security policies in composite web services. IEEE Transactions on Services Computing, 12(3), 415-428.

[32]. Darus, M. Y., Omar, M. A., Mohamad, M. F., Seman, Z., & Awang, (2020). Web vulnerability assessment tool for content management system. International Journal, 9(1.3).

[33]. Mateo Tudela, F., Bermejo Higuera, J. R., Bermejo Higuera, J., Sicilia Montalvo, J. A., & Argyros, M. I. (2020). On Combining Static, Dynamic and Interactive Analysis Security Testing Tools to Improve OWASP Top Ten Security Vulnerability Detection in Web Applications. Applied Sciences, 10(24), 9119.

[34]. Esposito, D., Rennhard, M., Ruf, L., & Wagner, A. (2018). Exploiting the potential of web application vulnerability scanning. In ICIMP 2018 the Thirteenth International Conference on Internet Monitoring and Protection, Barcelona, Spain, 22-26 July 2018 (pp. 22-29). IARIA.