ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Website Security with an Emphasis on AI»

ΕΛΕΥΘΕΡΙΑ ΝΤΟΥΛΙΑ
Α.Μ. CSCYB 22015

Εισηγητής: Παναγιώτης Γιαννακόπουλος

ΜΑΡΤΙΟΣ 2024

(Κενό φύλλο)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

WEBSITE SECURITY WITH AN EMPHASIS ON AI

Ελευθερία Ντούλια
CSCYB 22015

Εισηγητής:

Παναγιώτης Γιαννακόπουλος, Καθηγητής

Panagiotis Giannakopoulos
Digitally signed by Panagiotis Giannakopoulos
Date: 2024.04.26 22:32:36 +03'00'

Εξεταστική Επιτροπή:

Κωνσταντίνος Μαυρομάτης, Λέκτορας

Konstantinos Mavrommatis
Digitally signed by Konstantinos Mavrommatis
Date: 2024.04.29 09:54:23 +03'00'

Δημήτριος Κόγιας

Dimitrios Kogias
Digitally signed by Dimitrios Kogias
Date: 2024.04.26 22:23:21 +03'00'

Ημερομηνία εξέτασης 08/03/2024

(Κενό φύλλο)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη Ελευθερία Ντούλια του Αχιλλέα, με αριθμό μητρώου CSCYB 22015 φοιτήτρια του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Βεβαιώνω ότι είμαι συγγραφέας της παρούσας διπλωματικής εργασίας και ότι έχω αναφέρει ή παραπέμψει σε αυτή, ρητά και συγκεκριμένα, όλες τις πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, προτάσεων ή λέξεων, είτε αυτές μεταφέρονται επακριβώς (στο πρωτότυπο ή μεταφρασμένες) είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για την συγκεκριμένη διπλωματική εργασία».

Η Δηλούσα

(Κενό φύλλο)

Table of Contents

Introduction

The development of computer, network, and communications technologies has had a significant impact on the Internet economy. Decision-makers will have to address the strategic challenge of utilizing the information available on the internet to conduct e-commerce, boost customer satisfaction, reduce operating expenses, and improve operational efficiency. With greater flexibility and scalability brought by network-based distributed information technology, system security is closely linked to economic efficiency and interests, and information security has become increasingly important.

Importance of Website Security

Establishing an innovative, safe, and globally respected e-commerce system is a particular method to address the challenge of economic globalization. E-commerce's potential for advancement is determined by its inherent benefits. E-commerce allows businesses of every kind and size to expand their scope globally, reduce business cost and serve a wide range of client demands.

Information security is the basis for the development of websites. With the development of e-commerce, a variety of Internet transactions show the characteristics of diversification and the security issues have become much more prominent. Addressing the current risks and difficulties organizations encounter when protecting their websites from cyberattacks is crucial because the usage of artificial intelligence (AI) in cybersecurity is a rapidly growing field. Web applications are subject to attacks from different locations at various levels of scale and complexity Malicious actors can develop new capabilities with the aid of AI, extending or even expanding cyber threat practices that have been around for a while. These capabilities are progressively becoming automated and even harder to detect [1,3,6,12,20].

The growing sophistication and frequency of cyber threats underscores the significance of website security, particularly with regard to artificial intelligence. Without substantial automation, individuals cannot manage the complexity of operations and the scale of information to be utilized to secure cyberspace. Keeping websites safe from cyberattacks presents an array of difficulties for organizations, including new threats, physical security, cybercrime, and human error. Concerns about privacy to protect the increasing volumes of personal data submitted on the Internet, the need for a new generation of security tools to fend off advanced persistent threats, and the requirement to secure the Internet of Things (IoT) are among the emerging threats in cybersecurity [4,12].

The way that websites and web applications are created and used is constantly evolving. Websites and programs contain several types of components that interact with users by receiving user input and displaying it to them as output. Users could give inappropriate inputs intentionally or accidentally. From a security view, incorrect or malicious inputs should be recognized and rejected as soon as possible. Cyberattacks can be detected and identified, while their impact can be lessened with the application of AI-based tools and techniques. These technologies have the facility to provide real-time, cost-effective performance that meets the required expectations. AI can provide a wide range of security techniques and

capabilities, mechanisms that are becoming more and more popular and common in the field [2].

For the majority of organizations with an online presence, which is almost every firm in the twenty-first century, secure development methods are still behind. Even though applications have grown to constitute the largest security perimeter, organizations frequently see and handle IT security personnel and application developers as distinct entities. Security experts are often left to "slap a Band-Aid on" mistakes that could have been seen and fixed during development because of this lack of communication and ignorance about where the business's front line is at this time. Furthermore, security teams only address a relatively small percentage of the website vulnerabilities they discover after apps are live. This suggests that despite the threat that many vulnerabilities pose to the business, they have yet to be fixed [5].

Eliminating the boundaries that divide the development team and IT security is the most significant task that needs to be done right now. Organizations will significantly increase their willingness to write code, evaluate it for vulnerabilities, and address them by combining these two teams. From a management standpoint, cooperation is particularly vital because developers frequently view the security team as an impediment [5].

Security Threats

E-commerce's information security: Since the Internet's take off, e-commerce systems have faced numerous security risks. Currently, e-commerce presents significant security threats in the following domains:

1. Identity imitation → The attackers steal the identities of authorized users, forge those identities in order to trade them, and compromise the authenticity of the information. By using these methods they acquire illicit benefits. The most frequent operations are taking on another person's identity, using someone else's account to frame them, and tricking hosts and legal mainframes into giving up information.
2. Unvalidated Input → Web application development is predicated on the client-server communication process, in which the client submits a request to the server, which processes it as input through the web application. The legality of the input for the request cannot be verified by the web applications. Because of this security hole, attackers can gain undue advantage by inserting malicious data into the application and bypassing the website's protection.
3. Improper Error Management → The attackers deliberately introduced errors within the web application, which are displayed as error messages in the output once the application has been executed.
4. Network information security → The majority of attackers will use physical or logical methods to physically intercept, tamper with, remove, and inject data into network transmission channels. When physical signals are transferred over lines, an attacker may examine the network's various characteristics and collect useful or confidential data,

such as the customer's password or account number, among other things. To tamper with is to alter the sequence or content of information flow; to delete is to chop off a message or portion of a message; and to insert is to add new, confusing, or misleading information into the original.

5. Computer system security → Computer systems are the foundational equipment of e-commerce; if security concerns are neglected, they could jeopardize the information security of the industry as a whole. The problems with computer equipment itself include physical damage, data loss, information leakage, and so forth. Computer viruses and other external threats, coming from illegal sources, can occasionally assault a system and cause damage. In the meantime, issues with the staff management system may arise, such as unclear roles and responsibilities, which could compromise computer system security.
6. Denial of service → aims to disrupt the availability of an organization's services and data. If successful, a DoS attack prevents people from accessing online services, information, email services, websites, online accounts and other services that rely on the company's resources. As a result these attacks can cost an organization both time and money while their resources and services are inaccessible, resulting in a direct impact on availability.
7. Both sides deny trades → E-commerce security is essential to the success of any online business, and it consists of protocols that safeguard people who engage in online selling and buying goods and services. By implementing e-commerce security basics, organizations can gain their customers' trust and prevent both sides of a transaction from denying trades [6,7,8,10,14].

E-commerce security mechanisms

The term "e-commerce" has several definitions. E-commerce, as it is commonly known, is the utilization of easy, quick, and inexpensive electronic communications. In a faceless business transaction equivalent to e-commerce, a customer's decision-making is greatly influenced by their level of trust. The information acquired from the vendors' websites significantly impacts a person's level of trust in e-commerce. There are certain information elements e-commerce users consider or require to be present on websites, in order to be assured they are having a totally secured transaction

E-commerce technologies' development as an established method of conducting business has been impeded by concerns about the security, privacy, and integrity of online transactions. An e-commerce system needs to be secure and reliable for numerous reasons. First of all, it aids with the transmission of sensitive data, including passwords, credit card numbers, and personal information. In addition, it safeguards against viruses, malware and other cyber threats, restricts unauthorized access to the machine and protect sensitive information. Thirdly, it enhances the development of trust—a crucial aspect of any online

business—between the company and its clients. By expanding the traditional view of internal control and addressing the risks prevalent in e-commerce, organizations can achieve control or expectations equilibrium and gain acceptance and trust of their participants

1. Authentication: Authentication is the process of verifying the identity of a user or system. It is used to ensure that only authorized users have access to the system and its data.
2. Firewall: Packet filtering and proxy service mechanism are two types of current firewall structures. The first technique is the simplest and most common one; it verifies whether each packet should be transmitted to the intended destination by examining it as soon as it is received. By selectively filtering data, the firewall ensures the security of a dedicated private network by successfully preventing malicious or accidental attacks transmitted by those packets. Resolving security challenges can be achieved effectively by combining the previous two technologies. However, the firewall mechanism has limitations too:
    a. This technology is only able to block external attacks via a firewall; it cannot stop user-initiated internal attacks on the network.
    b. It can only adequately defend company networks from attacks and intrusions of the initiative; it cannot guarantee attacks by a virus from the same network.
3. Secure Sockets Layer, or SSL, is a security protocol that allows communication between a web server and a web browser in an encrypted and secure environment.
4. Virtual private network technology (VPN): VPN implementation requires a wide range of technology. For example, tunnel safety technology, information encryption, user authentication, access control technology and so on. Additionally, a VPN has several benefits, including low cost, ease of use, adaptability, and other features. VPNs can allow internal company networks, branch offices, business partners, suppliers, and remote users establish secure connections and assure the security of data transmission. By taking these steps, one can accomplish the goal of conducting electronic transactions over a company local area network or the open Internet.
5. Audit mechanism: The foundation of evidence for accident investigations and criminal prevention is internal audit. Through the recording of several significant incidents, the system is able to identify the mistakes and reasons behind successful attacks when it is assaulted in the incorrect location. There should be safeguards in place to prevent unauthorized access to or modification of audit information.
6. Encryption: Information can be protected by encryption, which modifies the access procedure and prevents an attacker from reading the content. Additionally, useful information can be buried within an additional message, evading an attacker's search. These two methods can safeguard not only confidential information but also the communication of parties.

7. Business filling mechanism: The system sends meaningless, random data during idle time to make it harder for attackers to obtain information over the communications channel. Simultaneously, the technique could potentially make it harder to understand the code message [6,10,11,15].

Enhancing e-commerce security with elliptic curve-based zero-knowledge algorithm

There are many tools, techniques and mechanisms that have been used to improve the security of websites and web applications. There was research conducted that revealed Elliptic Curve-Based Zero-Knowledge Proofs could increase the security of an e-commerce website. Superior security and privacy as well as increased efficiency can be achieved by this method. Zero-knowledge proofs (ZKP) in particular can be applied in cases when it is necessary to demonstrate the possession of crucial information without actually exchanging the data. Credit card verification, digital cash systems, digital watermarking, and authentication are a few examples of these usages.

Many e-commerce applications have been implemented, without using zero-knowledge proof techniques for verification purposes. Most of these solutions reveal more information in order to achieve verification. An anonymity revocable off-line electronic cash scheme is a type of electronic cash system that provides anonymity to users while allowing for the revocation of anonymity under certain conditions. By providing anonymity, unlinkability, double-spending checking, anonymity control, and fast anonymity revocation, these schemes aim to provide users with a secure and private way to conduct transactions online.

Zero-knowledge proofs are used when someone (the prover) has to prove to someone else (the verifier) his/her knowledge of secret information without revealing any information about the secret that the verifier cannot get without executing the protocol. There has been a high-level assessment of the proposed approach of using elliptic curve-based zero-knowledge proofs in e-commerce. The following key requirements are met by the suggested method:

1. Authentication → It provides user authentication via proving the possession of an authentication secret.
2. Privacy → The private information is not revealed; only the possession of such information is checked.
3. Security → Zero-knowledge proofs on DLEC provide a higher level of security than on discrete logarithm over Zn, or current RSA.
4. Ease of Use → The authentication process is performed transparently to the users.

Now defining the zero-knowledge proofs, they have two parts:

1. Proof → There should be solid evidence that Peggy is aware of the secret. Victor ought to be persuaded that Peggy is aware of the secret by the time the protocol is completed. Peggy shouldn't be capable to cheat (within a specific probability in iterative proofs) due to the protocol. Without knowing the secret, she must not be able to perform her part of the discussion.

2. Zero-knowledge → Victor shouldn't receive any information on the secret, via the secret. This points out that Victor shouldn't be able to extract the secret from the dialogue's content, computationally.

There are various classical problems that involve zero-knowledge proofs. Here we are going to present the Discrete logarithm over elliptic curve (DLEC) problem and its advantages.

- Given an elliptic curve E over a field Fn , G ∈ E/ Fn (where G is a generator, or its order contains a large prime), and B = m*G ∈ E/Fn , Peggy wants to prove in zero-knowledge that she knows m such that m*G = B.
- Solution: Since Peggy claims that she knows m such that m*G = B, where B is public, she generates a random r ∈ Fn and computes A = r*G. She sends A to Victor. Now Victor flips a coin and conveys the outcome to Peggy. If it is heads, Peggy sends r to Victor and he verifies that r*G = A. If it is tails, she sends x = r + m and Victor verifies x*G = A+B. Repeating these steps increases exponentially the confidence of Victor that Peggy knows the secret m.

		Peggy (P)	Victor (V)
0		G, B, m	G, B
1	Peggy generates random r	r	
2	P sends A = r.G to V	A	A
3	V flips a coin c = H or T	c	c
4	If c = H, P sends r to V		Check r.G = A
5	If c = T, P sends x = r + m		Check x.G= A+B
6	Steps 1-5 are repeated until Victor is convinced that Peggy must know m (with probability $1-2^{-k}$, for k iterations).		

Having DLEC as building blocks makes the zero-knowledge proof scheme more secure than the classical scheme. It has been proven that the classical DL problem in Fq * can be solved in sub-exponential time, L(1/3). The time complexity to solve the classical DL problem reduced to

$$Exp(O((\log q)^{1/3} (\log \log q)^{2/3})).$$

However, the best-known algorithm to solve the DLEC problem in E/Fq is by using giant-step baby-step approach, but it takes exponential time to be solved. The time complexity of the algorithm is $O(N^{1/2})$, where N is the group order. For an elliptic curve over the field Fq, the time complexity is $Exp(O(\log q))$. The observation we make here is that if the Elliptic curve scheme is not based entirely on DLEC, weaker parts in the scheme can be attacked in sub-exponential time, and hence using elliptic curve gives no more security than the classical ones.

In general in such crucial applications, zero-knowledge proof techniques are powerful tools for ensuring privacy and security in parallel. Elliptic curved-based zero-knowledge proofs give more security in the case of the discrete logarithm problem, but not in other cases, such as the one of the square-root problem. The improvement of security is due to the higher complexity of solving the discrete logarithm problem over elliptic curves than over the

multiplicative group Zn. This advantage is applicable to all applications, in which the zero-knowledge proof is based on the discrete logarithm over elliptic curve, including: anonymity revocable off-line digital cash, and its batching scheme [16 – 19].

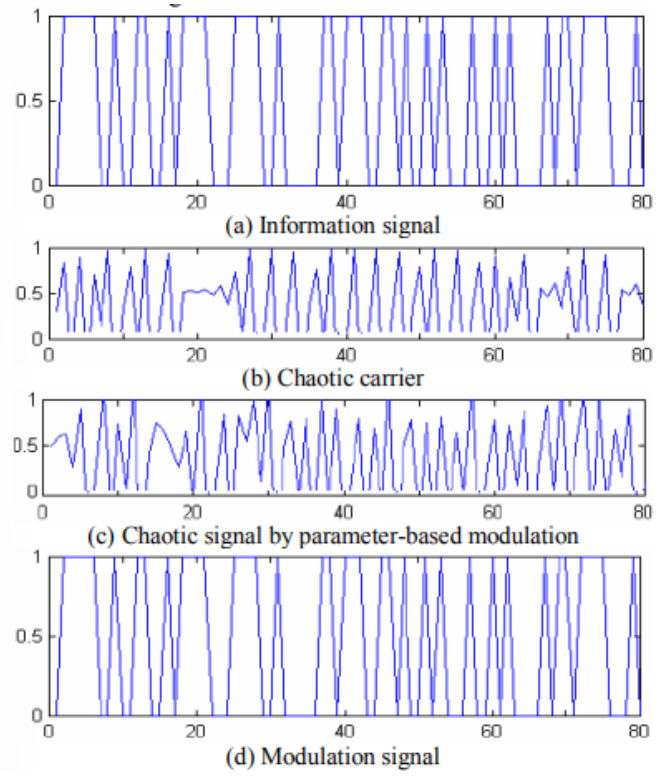
Chaotic Encryption Implementation in Ecommerce

Chaotic encryption is a type of encryption that uses chaos theory to generate keys and encrypt data. It has the ability to generate keys for digital signature algorithms, encrypt sensitive data, and randomly permute image pixels in order to improve website security. Although chaotic systems display complex and unpredictable behavior, they are deterministic and can be utilized to produce random numbers and encryption keys. Organizations can provide secure and efficient encryption for different types of data in website security by adopting chaotic encryption algorithms.

Chaos theory can be applied to cryptography and the chaotic control method of encryption in e-commerce. A chaotic encoding algorithm can provide encryption and decryption for the transferred data effectively. Chaotic encryption systems have unique natures such as the extreme sensitivity to initial value and higher randomness. Due to the same initial parameters, the data will also be repeated.

Here a discrete example of a chaotic system is simulated, which shows the perfect confidentiality.

A parameter-modulation-based chaotic encryption method uses the chaotic system as a chaotic sequence carrier and the information signal as chaotic system parameters in its chaotic region are modulated. The receiver uses the rules by a chaotic sequence to extract the chaotic carrier from the received signal. After a simple signal processing, the information signal is resumed. On the basis of chaos switching, a threshold process is introduced, which strengthens the system's level of confidentiality.



Both the chaotic carriers and the chaotic signal by parameters-based modulation have relatively perfect randomness. In the process of transmission, it is difficult to decode even if it is intercepted. (a) to (d) in the displayed figure show that the results by modulation and the original information signal are the same.

The parameter-based modulation chaotic encryption has several advantages. It can be precisely matched at both transceiver ends by using digital circuits. The digital signal itself offers notable immunity during transmission. Error propagation does not occur since it is always the last to receive signals from the chaotic carrier extract. System confidentiality can

be improved by implementing threshold processing, a nonlinear transformation. The outcomes demonstrate that chaotic encryption is successful in maintaining confidentiality [20,21].

Session Security Management in E-Commerce

The demand for efficient communication between departments and businesses is growing as e-commerce develops. In order to effectively carry out the business processes, the information systems of multiple companies have to cooperate. As a result, the traditional EDI mode (*Electronic Data Interchange* mode refers to the computer-to-computer exchange of business documents in a standard electronic format between business partners) can no longer fulfill the requirements. The development of web services presents a number of considerations and challenges for the construction of the e-commerce infrastructure and the integration of corporate data.

The more complex business requirements cannot be addressed by the traditional interaction between two entities. Instead, numerous web services operating in session mode in a distributed environment must address this issue. This creates a number of unexpected dangers In response to this situation, IBM and Microsoft released the WS-Conversation security specification, which strengthens the security requirements for web services.

The web service is a brand-new distributed computational model using the SOA (Service Oriented Architect) which is composed of three participants and three basic operations. The three participants are the Service Provider, the Service Requester and the Service Broker. The three basic operations are Publishing, Searching and Binding. All these act on the component and software module of the web service and their description. The framework of the SOA of web service is shown in the figure below.

The SOA (Service Oriented Architect), which is composed of three participants and three fundamental operations, is implemented in the web service, an innovative distributed computing model. The Service Provider, the Service Requester, and the Service Broker are the three participants involved. The three basic operations are Publishing, Searching and Binding. Each of these has an impact on the web service's software module and component. The web service's SOA framework is shown below.

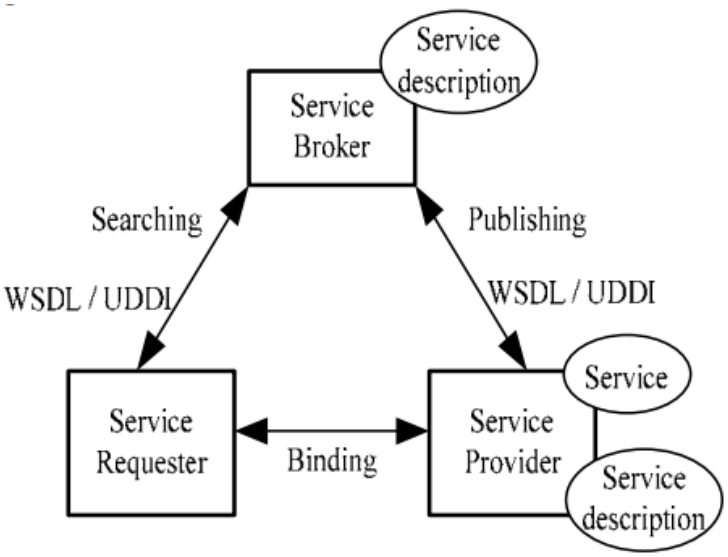


Figure 1. Framework of web service

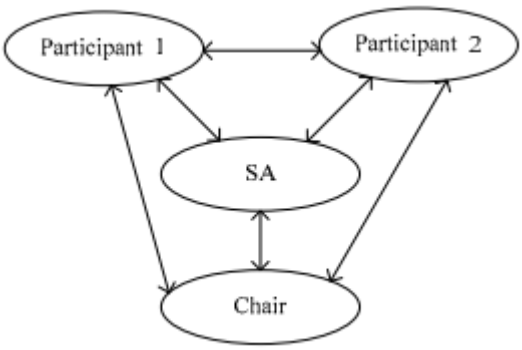
There are three primary elements regarding web service:

- SOAP → Simple Object Access Protocol, is a messaging protocol used for exchanging structured information in the implementation of web services in computer networks. SOAP messages are purely written in XML, which is why they are platform and language independent. The purpose of SOAP in web services is to provide a standardized way of exchanging data between different systems, regardless of the programming language or platform used.
- WSDL → Web Services Description Language is an XML-based language used for describing web services. It provides a standard format for describing a web service and defines the operations in a web service, the messages used by each operation, and what each message should look like.
- UDDI → Universal Description, Discovery, and Integration is a directory service where businesses can register and search for web services. It is an XML-based standard for describing, publishing, and finding web services. UDDI is often compared to a traditional telephone book's white pages, where businesses can list their services and contact information.

Regarding security specification in web service, the most authorized and comprehensive web service security standard nowadays is the WS-Security, published jointly by Microsoft, IBM and Verisign. It is the foundation of web service security and it also integrates the commonly accepted security models, mechanisms and technical support. The purpose of the WS-Security standard published by IBM is to provide message-level security for web services. It is based on securing SOAP messages through XML digital signature, confidentiality through XML encryption, and authentication through the use of security tokens. WS-Security is often used in combination with other web service security standards, such as WS-Policy and WS-Trust, to provide a comprehensive security solution for web services.

Based on the WS-Security, the Web Service Secure Conversation Language provides the mechanism that creates and shares the security session and derives the session key. The session management is in charge of the whole process of the session from beginning to ending and ensures the legitimating of the user’s identity and the security of the

messages in the communication. It is shared among the session participants. The session management model is shown below:



Session management oversees the entire process of the session from the beginning through end and makes certain the user's identity is verified and that the communication's messages are secure. It is shared among every session participant. The roles in the model are as following:

- The SA (Session Authentication), who provides the establishment of the session, the management and the authentication for all the participants of the web service session.
- The Chair, the initiator, also the Moderator of the session, who starts the web service and the application of the server or the client of the session.
- The participant, the other web service, server or client application in the session except the Chair.

The web service or application program must first send a request to the Session Service in order to acquire the session context before initiating a session. The session handle and session secret are contained in the context. The session handle indicates the conversation. The session secret derives all kinds of the session keys. Once the context is obtained, the requester takes on the role of Chair of the discussion and can invite other web services to join the session by sending them an invitation with the session handle.

Once the web service receives the session handle, it sends a request to SA for obtaining the whole context of the session. WS-Security states that once all session participants possess the context, they can sign and encrypt the SOAP message using the same session key. This achieves the purpose of session security. Every time a new participant enters the session after the initial one, the SA modifies the Session Secret to safeguard the previous communities. The SA also modifies the session secret once a participant departs in order to continue protecting communication. It provides updated session secrets to every remaining participant. Since there is a great deal of critical and regular communication between the session participants, it is important to create an ideal communication method in order to successfully conduct the session [22–27].

Framework to secure Web Applications

Due to the increasing number of attacks to websites and web applications, the need for new, efficient and updated tools and mechanisms for defense is vital. Various methods can be implemented in order to secure a website, but here we are going to analyze a secure

framework which analyzes the source code implemented by web developers, it modifies it if needed, and it detects the vulnerabilities in the source code dynamically. This framework makes detecting actual attacks, authentication leaks and SQL injection attacks possible, with the aid of dynamic queries.

To improve the security functions or methods of web application frameworks, an effective framework has been proposed that has features of analyzing callback functions and can modify the source code of an application if necessary. Web application frameworks provide application developers with a variety of functions to improve the security of their web applications. However, developers that use web application frameworks sometimes implement vulnerable applications because not every developer is capable of using these frameworks' functions properly. In addition, many web application frameworks do not analyze and modify callback functions that developers implement.

Some web application frameworks are equipped with unit test tools for developers. These tools enable application developers to dynamically analyze their callback functions. However, the use of these tools requires developers to describe various test data, leading to increased development time and workload. Furthermore, it can be challenging to describe test data for each vulnerability. As a result, while these tools offer dynamic analysis capabilities, they also introduce complexities related to test data description and increased development efforts.

Web application firewalls (WAFs) are a recommended method for reducing vulnerabilities in web applications. WAFs serve as a protective system placed between clients and web applications, monitoring and filtering incoming traffic. They are effective in blocking or sanitizing attack requests, such as cross-site scripting (XSS) or SQL injection (SQLi), without directly modifying web applications. However, WAFs are not a comprehensive defense solution, as they do not consider the status of applications or modify them. Additionally, some attacks, particularly those related to authentications and authorizations, are challenging to detect using WAFs, as they can be carried out without the use of special characters. Therefore, while WAFs are valuable for reducing vulnerable attacks, they are not a fundamental solution and may not address all types of vulnerabilities, particularly those that do not involve special characters.

In response to these challenges, a web application framework is presented that incorporates a feature for analyzing source code. This framework has the capability to dynamically analyze the source code implemented by web application developers, particularly focusing on the detection of vulnerable aspects within callback functions. Upon identifying vulnerable source code, the framework is designed to either insert functions to secure the source code or replace the source code with a secure alternative. Through the utilization of this proposed framework, web application developers can conduct dynamic verifications of their applications without the need for additional implementation for vulnerability analysis. Furthermore, the framework is positioned to proactively prevent vulnerability attacks, addressing limitations associated with general web application frameworks and WAFs, such as the challenge of mitigating authentication leaks. This framework represents a significant advancement in the realm of web application security, offering a more comprehensive and proactive approach to vulnerability detection and mitigation.

The proposed framework modifies callback functions in four steps. Firstly, it retrieves the source code of callback functions from live objects. Secondly, it creates abstract syntax trees based on these callback functions. Thirdly, it modifies the created abstract syntax trees using vulnerability handling functions implemented by the framework developers. Finally, the framework generates live callback functions from the modified abstract syntax trees, which

are then stored in the framework. To validate the framework's ability to verify callback functions using vulnerability handling functions, experiments and analysis were conducted. The proposed framework offers a proactive approach to vulnerability detection and mitigation by analyzing and modifying source code, particularly callback functions, to secure the source code or replace it with a secure alternative. This framework enables web application developers to conduct dynamic verifications of their applications without additional implementation for vulnerability analysis. Additionally, the framework can prevent vulnerability attacks that are difficult to address using traditional web application frameworks and web application firewalls (WAFs), such as authentication leaks. The proposed framework represents a significant advancement in web application security, offering a more comprehensive and proactive approach to vulnerability detection and mitigation. It demonstrates the ability to address two vulnerabilities: authentication leaks and SQL injection vulnerability.

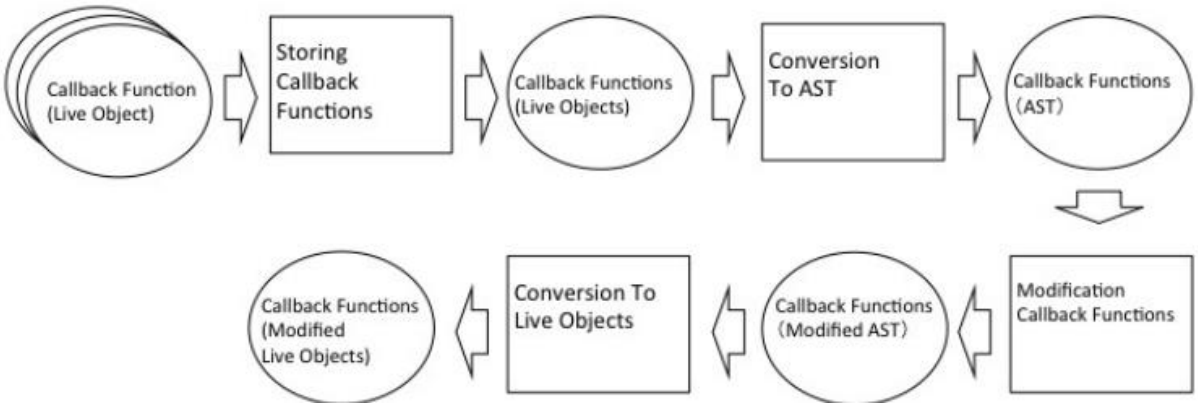
The use of web application frameworks, which encompass numerous libraries, can significantly aid developers in enhancing the efficiency of their applications. These frameworks offer security helper functions, such as auto-sanitization, which automatically secure callback functions or add appropriate sanitization code to web applications. While these security helper functions can streamline the development of secure applications, the proper invocation of these functions by web application developers is essential, as improper usage can lead to errors. Auto-sanitization, a feature of these frameworks, delegates some of the security responsibilities from developers to the framework itself, wherein developers specify the variables to be sanitized, and the framework performs the sanitization. However, the reliance on developers to indicate the variables that require sanitization can potentially result in the creation of vulnerable web applications. Additionally, the scope of auto-sanitization is often limited to template processing, thereby reducing its effectiveness in mitigating certain vulnerabilities. Therefore, while web application frameworks and their associated security helper functions offer valuable support, it is crucial for developers to exercise diligence in their utilization to ensure the creation of robust and secure web applications.

WAF serves to safeguard web applications from malicious attacks by acting as a barrier between clients and the web application server, scrutinizing HTTP requests to determine their potential as attacks. Upon identifying an attack, WAF either transforms the request into a secure one and forwards it to the web application or provides an error page to the client. The primary determinant for WAF in discerning attacks is the nature of the request, with a higher prevalence of special characters making attacks easier to detect. Consequently, WAF exhibits a strong capability in detecting attacks like XSS and SQLi. However, it is unable to thwart attacks devoid of special characters and is also utilized for regular communication. Notably, one such attack targets the absence of authorization control, a vulnerability that permits unauthorized users to execute specific operations.

The proposed web application framework, which possesses the capability to modify callback functions, is outlined as follows. The framework offers three key advantages in terms of cybersecurity. Firstly, it eliminates the need for developers to implement certain security functions in callback functions, as the framework can modify them instead. This feature allows the framework to take on some of the responsibility for cybersecurity in callback functions. Secondly, the framework can address vulnerable attacks that cannot be countered by WAF, which typically detects attacks by examining features or traces in request messages, so it is difficult for WAF to prevent attacks from requests that do not include special characters and/or meaningful strings about other programming languages. The framework can detect and modify vulnerabilities in callback functions that WAF cannot, such as authentication leaks caused by

careless web application development. These vulnerable attacks happen because privileged resources can be accessed from actors without any privileges on resources in callback functions. Lastly, the framework fundamentally removes vulnerabilities by fixing callback functions, which WAF cannot do. This feature ensures that even if countermeasures are taken for a specific attack request, the framework can prevent attacks that bypass WAF.

When an application utilizing this framework is executed, communication occurs in four stages. The following figure illustrates the steps for modifying callback functions. Initially, the framework stores callback functions along with the necessary routing information. At this point, the callback functions exist as live objects, represented as binary data. Subsequently, to facilitate the processing of callback functions, our framework converts the stored callback functions from live objects to abstract syntax trees (AST). An AST serves as an intermediate code generated during the process of creating executable binary code for a program. The components of the AST are depicted as nodes, with each element representing a program's code object. As each node in the AST possesses a meaningful or attribute name, it is easier to modify compared to directly parsing and modifying the binary. Additionally, the AST offers the advantage of being more amenable to modification than altering the source code. In our approach, it is challenging for the web application framework to take the source code as an argument and directly modify it, as the developer implementing the vulnerability handling function cannot directly access the callback function. This is due to the unsuitability of detecting source code vulnerabilities using regular expressions and other string patterns. The AST is easily parsed and modified because it eliminates parts of the source code that are irrelevant to the code object. It also categorizes operators with similar code generation rules. The third stage involves modifying the callback functions. Developers of the web application framework implement functions that alter the callback function. These functions are being utilized, which can manage vulnerability functions. These functions recursively examine the syntax tree of the callback function, identifying vulnerable nodes based on node attributes and names, and subsequently modifying these vulnerable nodes. The list of callback functions serves as the argument for the vulnerability handling function. This process enables the verification of conditions in other callback functions based on the conditions specified in other callback functions. Finally, by converting the modified AST back into a live object, it becomes feasible to utilize the modified callback functions for client communication.



A web application framework that incorporates a feature for automatically analyzing and modifying callback functions has been described in the above paragraphs. To evaluate this framework and its functions, experiments were conducted by implementing the web application and necessary steps. The results of the experiments and evaluations indicated

that the proposed framework could partially address SQL injection vulnerabilities and vulnerabilities related to a lack of authorization control. However, the framework faced challenges, as implementing vulnerability handling functions without implementing the callback function proved difficult. To detect a wide range of vulnerabilities, it is necessary to increase the vulnerability handling functions, which we believe could be achieved by applying these functions to each callback function. Future improvements are expected to facilitate the implementation of secure applications [60,61].

How to build an effective application security program

A robust application security program involves integrating security into the Application Development Lifecycle (S-SDLC), developing security guidelines and standards, creating awareness and security training, executing effective web application security assessments, and establishing meaningful security dashboards for each stakeholder, from executives and directors to program managers and developers. To ensure the security of web applications, it is essential to follow a comprehensive testing methodology that includes identifying the scope of testing, implementing each tool on all resources, performing a risk assessment, providing security training for developers, using various security layers, and automating security tasks. Penetration testing and Runtime Application Self-Protection (RASP) are also effective methods for identifying vulnerabilities and mitigating security risks in web applications.

After interacting with various organizations and analyzing their challenges in obtaining effective output from vulnerability assessment programs, a detailed analytical study was conducted to understand the type of security program being executed. The study revealed that most security programs are application assessment request-driven, where any application requiring vulnerability assessment services places a request, and the web application security team fulfills the service request based on available bandwidth. The fundamental issue with this approach is the lack of risk-driven action, where any application can take priority based on request instead of assessing highly risky applications. Another major challenge observed was distributed security programs, where one program, such as dynamic analysis, does not interact with others, such as static analysis. This lack of collaboration between such groups was the cause of not being able to identify all vulnerabilities and obtain an accurate risk posture. These challenges also caused problems in driving effective remediation due to multiple channels of reporting.

In order to establish an effective web application security program or service, it is essential to adopt a risk-based model rather than a request-driven model. After extensive research and analysis, it was determined that an approach fully owned and managed by the web application security program is necessary. Given the increasing threats, attack vectors, and the challenge of identifying the impact of zero-day threats, an application risk score model serves as a robust foundation for promptly developing a program. A comprehensive approach was undertaken to construct an application risk score model, utilizing various attributes and their respective exposure or score to derive a detailed risk score for all applications.

The entire program is founded on the aforementioned application risk score-driven model and is segmented into various dynamic and static analysis offerings to provide a precise application risk posture. These multiple offerings not only engage in communication with each other but also foster robust collaboration to pursue the broader objective of safeguarding applications.

Some of the attributes that an effective web application security program is consisted of, are the following:→

a. Application Risk Score Development → A risk score is a numerical representation of the likelihood and impact of a potential security threat or vulnerability, allowing organizations to prioritize and allocate resources effectively to manage risks. Organizations better manage and mitigate IT-related risks with the aid of Application Risk Score Development.
b. Scoping, Scheduling & Planning based on Application Risk Score → It refers to the process of defining the scope, setting the schedule, and planning risk management activities based on the Application Risk Score. This approach involves using the risk score of an application to determine the scope and schedule of risk assessment and management activities. The risk score provides a quantitative measure of the potential impact and likelihood of risks associated with an application, allowing organizations to prioritize and allocate resources effectively. The meaning of Scoping, Scheduling & Planning based on Application Risk Score is to ensure that risk assessment and management activities are focused on the most critical applications and are conducted in a timely manner. The risk score also helps in setting the schedule for risk assessment and management activities, ensuring that they are conducted at appropriate intervals and are aligned with the organization's risk management process. By focusing on applications with the highest risk scores, organizations can prioritize their efforts and allocate resources where they are most needed.
c. Security Assessments
    - Dynamic Manual Deep Dive Annual Assessments → This approach involves conducting a deep dive into the IT system or application to identify potential risks and vulnerabilities, and then developing a risk management plan based on the findings. The deep dive assessment is a detailed and thorough examination of the IT system or application, which includes a review of the system architecture, data flows, and security controls. By conducting a deep dive assessment, organizations can identify potential risks and vulnerabilities that may not be apparent through other assessment methods.
    - Dynamic Light Annual Assessments → It is a type of vulnerability assessment used to identify and mitigate security risks in web applications. LAVA is designed to be a lightweight and efficient approach to vulnerability assessment, focusing on identifying the most critical vulnerabilities that pose the greatest risk to an organization's web applications.
    - White Box (Static) Source Code Security Assessments → They refer to a method of evaluating the security of an application's source code by analyzing its internal structure, logic, and implementation. This assessment is also known as white-box testing, clear-box testing, or structural testing. It provides a comprehensive view of the application's internal workings, allowing for a thorough examination of potential security vulnerabilities. White box testing is based on an analysis of the code of the software, enabling the tester to determine the entry and exit points of each. This assessment is typically performed on the source code after it has been compiled, examining the program’s internal

structure or logical design. It can help to optimize the code by identifying any performance issues, redundant code, or other areas that can be improved.

- Continuous Security Assessments → This approach involves the regular and repeated assessment of security controls, processes, and systems to ensure that they are functioning as intended and effectively addressing the organization's security requirements. Continuous Security Assessments are a proactive and dynamic method of security testing that provides organizations with a current and up-to-date snapshot of the threats and risks to which they are exposed. This approach allows for real-time vulnerability detection, ensuring that security teams can promptly address and mitigate emerging threats, keeping the environment secure and updated against the ever-changing threat landscape.

d. Remediation Tracking & Storm Management → It refers to the process of tracking and managing the remediation of identified security vulnerabilities and risks. This process involves identifying and prioritizing vulnerabilities, developing a remediation plan, and tracking the progress of remediation efforts. Remediation Tracking & Storm Management is a critical component of an organization's overall security strategy, as it ensures that identified vulnerabilities are addressed promptly and effectively, reducing the organization's exposure to potential threats. It is typically implemented using a combination of automated tools and manual processes. Automated tools are used to identify and prioritize vulnerabilities, while manual processes are used to develop remediation plans and track progress.
e. Vulnerability Data Analytics & Prediction Modeling → It refers to the use of data analytics and prediction models to identify, prioritize, and predict potential security vulnerabilities in software applications. This approach leverages historical data, statistical analysis, and machine learning techniques to analyze software vulnerabilities and predict future vulnerabilities, allowing organizations to allocate resources more effectively and mitigate risks. Vulnerabilities that may have been overlooked or missed during manual or automated vulnerability assessment processes can be identified.
    - Data Driven Decisions refer to the use of data to inform and improve decision-making processes in software engineering. The process of implementing data-driven decisions involves:
        - Data Collection → Gather relevant data from various sources, such as logs, metrics, user feedback, and system performance monitoring tools.
        - Data Preparation: Clean, normalize, and preprocess the collected data to ensure its quality and suitability for analysis.
        - Data Analysis: Perform statistical analysis, data visualization, and machine learning techniques to identify patterns, trends, and insights in the prepared data.
        - Decision Making: Use the insights gained from the data analysis to inform and improve decision-making processes, such as planning, design, development, and maintenance of software systems

- Monitoring and Evaluation: Continuously monitor the effectiveness of data-driven decisions and evaluate their impact on the software system's performance, security, and user satisfaction.

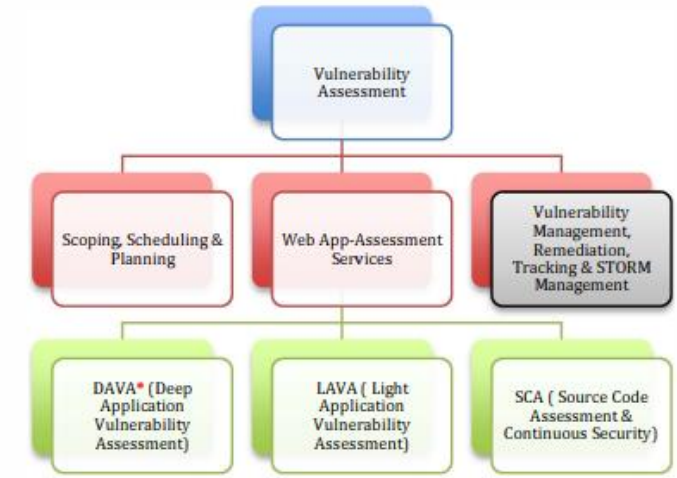
This approach leverages historical data, statistical analysis, and machine learning techniques to analyze software systems, identify patterns, trends, and potential improvements, allowing organizations to make more informed decisions and optimize their processes.

f. Training & Awareness.

The application risk score model is developed by considering various attributes such as the application's availability on the internet, data classification, previous security reviews, compliance, and business criticality. The actual risk score modeling and respective calculation are presented below:

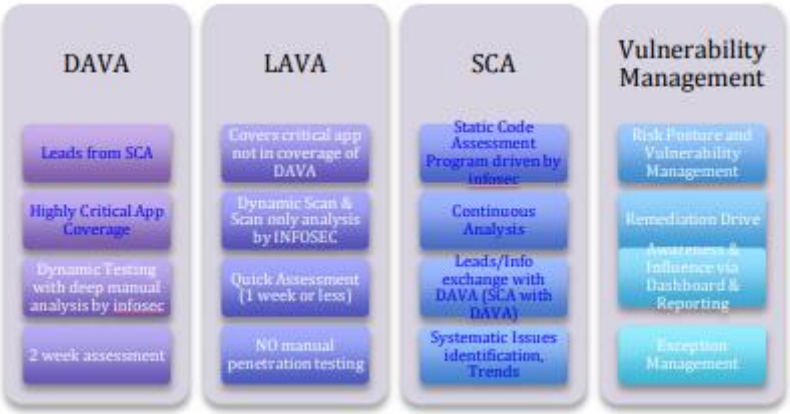
Attribute	Components	Weightage - Component Internal	Weightage - Group	Weightage - Component Wise
Application Availability	Internet (Public Internet)	75	25	25
Only one will be applicable	Intranet	25		8.33
Data Classification	Restricated -R	40	25	25
	Highly Confidential - H	30		18.75
	Confidential -C	20		12.5
Only one will be applicable	Public -P	10		6.25
Regulations/Compliance	SOX, HIPPA etc	100	10	10
Security Review Not Performed (Web)	Web Application Architecture (2 Year)	40	10	10
Security Review Not Performed (DAVA)	DAVA (1 Year)	40	10	10
Security Review Not Performed (BAVA)	BAVA (6 month)	20	5	5
Business Criticality	C1	45	15	15
Only one will be applicable	C2	30		10
	C3	20		6.67
	Other	5		1.67
Total	NA	NA	85	100

The scheduling and scoping of the program are defined using the aforementioned risk score to conduct web application assessments. A high-level overview of the program components is as follows:



The scoping of such program follows using the following approach:

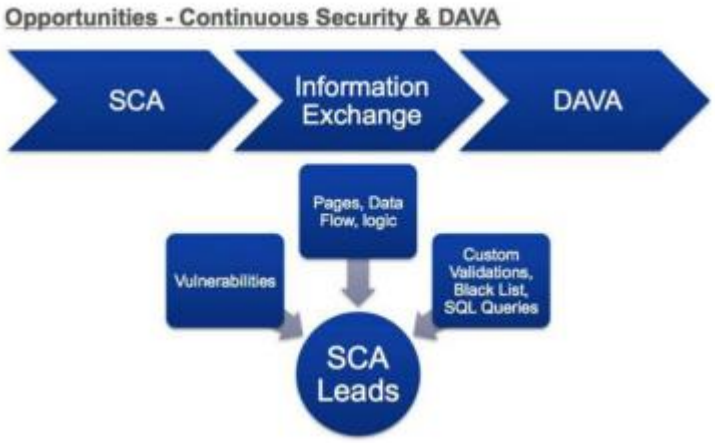
- Top 10*% Critical Apps applies for DAVA (Deep Application Vulnerability Assessment)
- Next Top 20*% Critical Apps applies for LAVA (Light Application Vulnerability Assessment)
- All apps go for SCA (Source Code Assessment & Continuous Security)



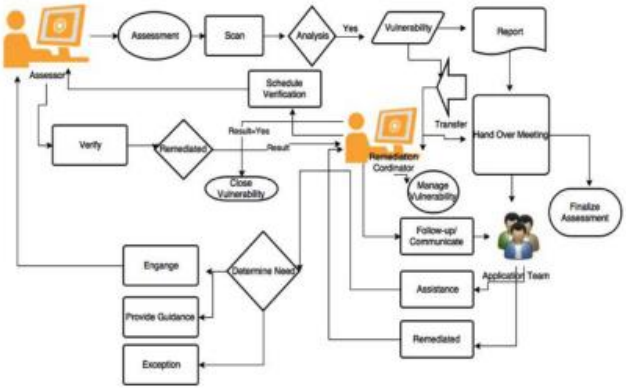
A team of 4 assessors will be able to handle approximately 80 DAVA assessments in a year while another team of 4 will be able to handle approximately 150-200 LAVA assessments.

An exchange of information occurs as depicted below to enhance the inter-program offerings and operations.

The comprehensive web application security assessment program necessitates the presence of a robust vulnerability remediation program. The vulnerability management



framework presented below exemplifies an optimal approach to addressing and resolving vulnerabilities.

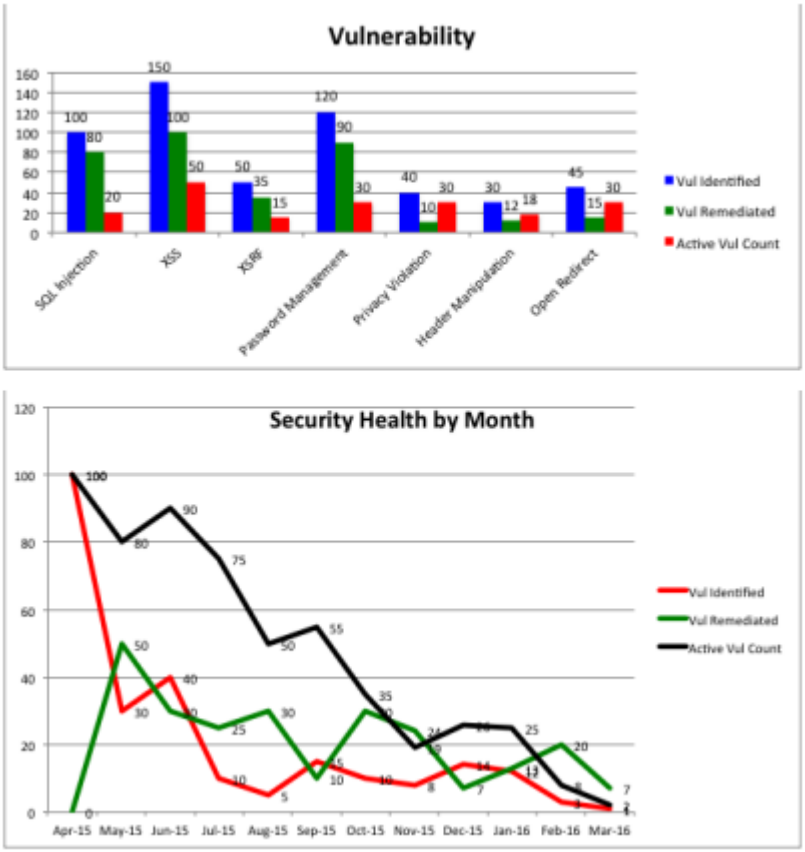


The implementation of an effective web application security assessment program is incomplete without a robust vulnerability remediation program in place. The vulnerability management framework presented below serves as an ideal approach to address and resolve vulnerabilities. This framework provides a simplified view of the security health or risk posture of the entire application, allowing for the identification of trends and patterns across the organization. The same dashboard is applicable at all levels, from developers to top management, to monitor the security health status of their portfolio. Additionally, the establishment of a well-defined application security policy and processes, asset discovery and management, controls analysis, threat intelligence, continuous application scanning,

penetration testing, and false positive management are among the crucial components recommended for a satisfactory web application security assessment.

The entire program facilitates the prompt identification of security vulnerabilities by application development teams. This is achieved through the integration of automated security assessment tools and the continuous web application security process, allowing for the early and frequent detection of defects when they are least costly to remediate. This proactive approach to vulnerability identification and resolution is essential for ensuring the robustness of web application security and minimizing the potential impact of security vulnerabilities on the overall application.

The implementation of processes and tools for a comprehensive review of the overall architecture and the necessary steps for remediation is facilitated by the program. The primary



focus of the continuous web application security program is to minimize the number of defects at the time of launch, thereby saving both time and the costs associated with rectifying defects. This strategic vision is aimed at reducing the occurrence of defects during the Go-Live phase, leading to efficiency gains and cost savings in addressing such issues.

The utilization of vulnerability analytics not only furnishes an accurate depiction of an application's security posture but also facilitates the development of predictive models. These models have the capability to forecast the introduction of specific types and quantities of vulnerabilities when an individual writes the next 1000 lines of code. This level of insight is achievable through the comprehensive program approach and represents a significant advantage. It not only provides an accurate security posture for the entire organization, from the highest to the lowest levels, but also contributes to the implementation of an effective remediation program.

Many organizations mistakenly believe that security can be ensured solely through testing. However, security is a continuous process that requires ongoing effort and attention, making a comprehensive web application security program essential for maintaining a robust security posture. In conclusion, an effective web application security program is essential for every web application, as it enables continuous monitoring and improvement of the application's security posture. This approach helps identify and address vulnerabilities before they can be exploited, ensuring the ongoing security and resilience of the web application [51−59].

Enhancing Website Security with AI

Our society has become more reliant on artificial intelligence (AI) as it helps many industries address complex problems and overcome antiquated practices. Artificial intelligence (AI) models are used in numerous applications, including people's smartphones, cars to prevent accidents, banks to manage loan and investment decisions, hospitals to assist physicians in diagnosing and detecting diseases, law enforcement to assist officials in recovering evidence and streamline law enforcement, the military in many nations, insurance companies to assess risk, etc. Furthermore, a lot of businesses are actively attempting to incorporate AI into their workflows because of its exceptional performance, which outperforms human performance in a range of activities.

Data-driven decision-making systems are made conceivable by AI. In order to create a massive amount of data, a precise AI model is required. Since they rely on the assumption of smooth linear or sub-linear data, primitive machine learning (ML) models like logistic regression, Decision tree (DT), and linear regression are less accurate. Real-world data, however, is extremely complicated and non-linear, which makes it difficult to process in order to extract knowledge and insights. Deep neural networks (DNNs) are used in these situations to extract information from extremely complicated datasets.

In earlier times, organizations used web proxy servers, firewalls, antivirus software, and other tools to defend themselves against the emerging internet threats. Although these models were rather effective in the past, their efficacy has decreased as a result of recent developments brought about by "Industry 4.0" and the cyber-threat scenario. With machine learning, you can use a computer to analyze data, identify patterns, and make decisions without much human intervention. AI is no longer a new word in the eCommerce industry; from personalization to facial recognition to virtual assistants, this is how AI is used to boost cybersecurity in the eCommerce sector [1,29,31].

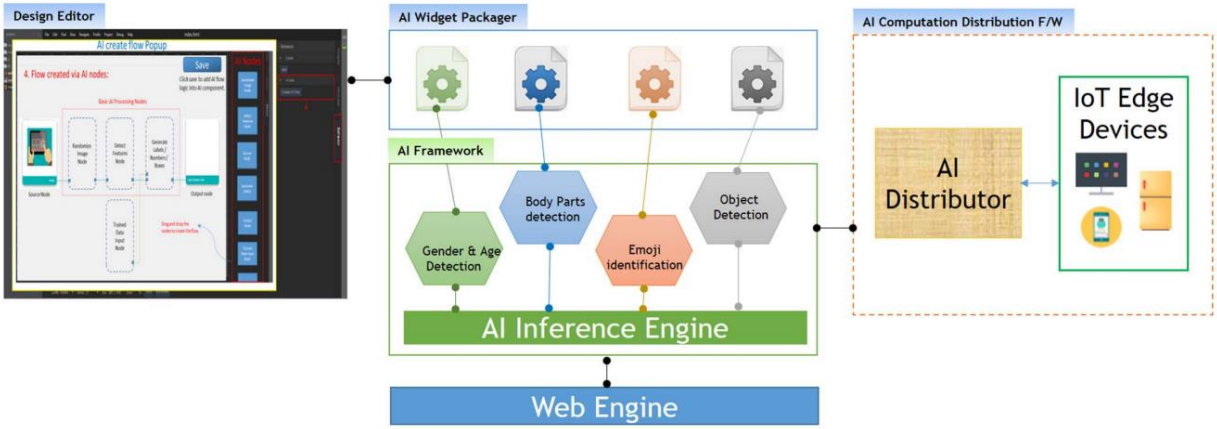
AWAF : AI Enabled Web Contents Authoring Framework

As a result of how extensively the internet has become a part of our everyday lives, companies in particular are benefiting from AI. Companies specifically utilize AI to create their websites and web applications, promote their products properly, and increase brand visibility. Web app developers can find solutions to issues with security, user experience, content analysis, quality assurance, and many other areas with the aid of artificial intelligence (AI) or

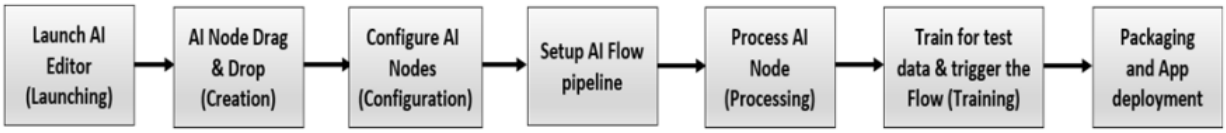
machine learning (ML) models. This highlights the need for a framework or tool that enables third party developers to create AI-based applications with ease. Recently an AI Enabled Web Contents Authoring Framework (AWAF) has been presented, where AI models can be simply dragged into workspace, provide options to build, train Deep learning models using a simple web visual interface, and ultimately ship the AI features into the web application.

Also, an option to connect together smart blocks called AI Nodes is provided, in order to create custom deep learning models. This framework can allow web app developers to simply drag an AI feature in the workspace area, and connect as input/output of preexisting web functionalities. Thus making the prebuilt and tested AI features readily available for developers to ease the process of importing, testing and shipping the feature in a web product. The prebuilt AI features are called as AI Nodes in AWAF. These nodes are basically backend implementations of familiar AI models combined with functionality for connecting and communicating between themselves in a pipelined manner which provides greater reusability, particularly in AI based web applications. Web Developers can reuse these AI Nodes thus avoiding the effort required to connect those AI Models manually, thereby effectively reducing man hours and LOC during development phases.

The architecture diagram of AWAF is presented in the following figure and it has the below components:



This is the core of an AI Node where actual AI functionality is defined and implemented, or in other words, the AWAF workflow. It imports AI models, loads library script files, JSON files, calls appropriate APIs to process the input and produces expected output which is passed as input to the next node and so on.



This AWAF takes advantage of the edge-computing scenario, which means that each participating device acts as a processing node on the network. Computational work can be offloaded to these eclectic nodes. This allows use of a highly industrious ML model without the need to run it on cloud. For ex., Process of image classification can be initiated on a camera with the clicking of the picture and the ML model can be run on a high-end device like TV.

Finally, this was a presentation of how third party developers can seamlessly build and ship AI features into their web applications through visual web interface. This AWAF can be used in deploying the AI features that exist, regarding the security of the websites, too [13].

Neural network model for botnet detection system

The widespread use of botnets as a platform for malicious attacks presents a serious threat to internet security. These days, botnets have been classified as one of the biggest security risks. Since botnet detection and monitoring are thought to be extremely difficult and complex tasks, they have received a lot of attention in recent years. The adoption of common protocols like HTTP by the most recent botnets makes it even more difficult to identify their communication patterns. Most of the HTTP bot communications are based on TCP connections. Honeypots were the foundation of one of the first techniques for identifying botnets.

Botnets are organized networks of infected (Zombie) machines running bot codes, categorized by their use of a command and control (C&C) channel. Using the command and control of botnet, a botmaster can control a large group of compromised bots and then perform malicious attacks. Initially, the Internet Relay Chat (IRC) protocol served as the basis for C&C communications. Formerly, the attacker would actively issue commands to every bot on the IRC server's dedicated channel. Lately, HTTP has grown in popularity as a bot communication protocol . Given that HTTP is a widely used network communication protocol in many applications, these web-based C&C bots attempt to blend in with regular HTTP traffic, making it more difficult to identify them.

The HTTP bots frequently request and download commands from web servers under the attacker's control. As a result, detecting bots with web-based controlling is more intricate than bots with IRC-based controlling. Anomalies in web flow behaviors of HTTP botnets are identified, TCP related features are extracted and the neural network is used with a bold driver back propagation algorithm for botnet detection.

The neural network model was created with features that were extracted by the TCP connection behavior shared by web-based botnets and is able to detect the HTTP botnet traffic. This method's performance, which is utilized by the aid of AI, is compared with that of some more classifiers like Decision Tree C4.5, Random forest, Radial Basis function network. The results obtained showed that the proposed method using neural networks is able to achieve good identification results with less false positives. Another advantage of the proposed model is that it can detect HTTP botnets even if the communications are encrypted. It is clear that the AI implementation in the botnet detection problem has been more efficient than the traditional algorithms used until now [28,29].

Website Fingerprinting Attacks

XAI has become a popular research subject within the AI field in recent years. Thus, the need for eXplainable AI (XAI) methods for improving trust in AI models has arisen. Website Fingerprinting attacks attempt to track the websites that users visit on their browsers and deduce personal information about them. Despite the presence of several defense mechanisms in the network, a number of studies have shown that recent developments in Machine Learning (ML) and Deep Learning (DL) algorithms make it feasible to execute website fingerprinting attacks. Nevertheless, trained models for website detection are not thoroughly examined to identify the leakage sources which are not always visible to both attackers and Cyber Threat Intelligence engineers.

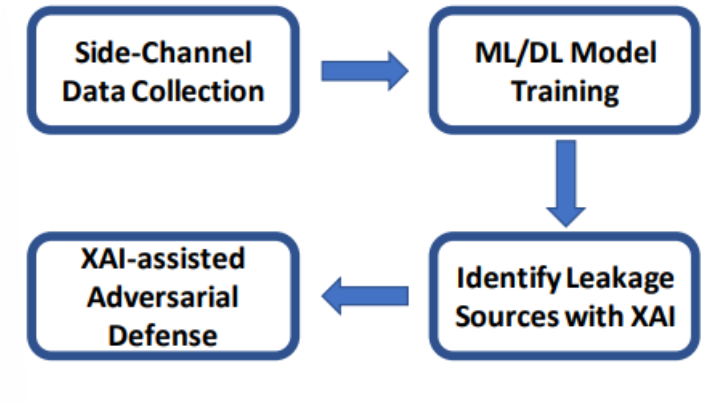
Although the Internet has significantly enhanced people's lives, carefully designed networks, such as the darknet provide an anonymous environment for illegal activity. Cyber Threat Intelligence (CTI) aims to safeguard government, businesses, and public assets from malicious actors operating in the darknet by identifying and, if feasible, detecting illegal activity and the individuals behind it.

End-to-end encryption, notably Hypertext Transfer Protocol Secure (HTTPS), safeguards the privacy and integrity of data transferred between a website and a user. HTTPS does not, however, safeguard user identities because the user's SSL/TLS certificates contain personal data. In response to this, Tor network was created to conceal user data (identity) at the application layer of the communication protocol stack, preventing network observers from discovering the identity of the user.

It has been proven that website fingerprinting (WF), which can also be used to increase CTI in the darknet, is effective for de-anonymization on encrypted networks. In network-based attacks, a local passive eavesdropper observes a number of network traffic metrics, including packet size, direction, and round-trip timing, to determine which website the victim visited. In a distinct scenario regarding website fingerprinting, an attacker can conceal malicious code in a browser or userspace application to gather hardware-related side-channel data.

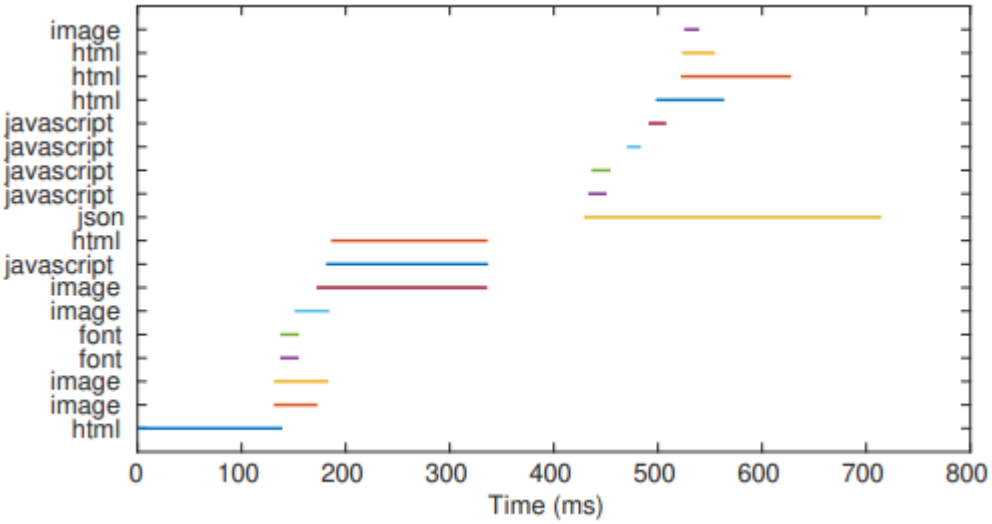
The majority of WF attacks are automated with the implementation of advanced Machine Learning (ML) and Deep Learning (DL) algorithms. These algorithms extract and learn characteristic features of individual websites using side-channel data. Website fingerprinting techniques are used with a variety of machine learning (ML/DL) algorithms, including random forests, naive bayes, Support Vector Machines, k-NN, CNNs, and LSTMs, in order to improve accuracy in large-scale website fingerprinting attacks. This is due to the fact that each learning algorithm possesses unique advantages and drawbacks in terms of accuracy, timing, and complexity. The main concern at this point is the explainability of black-box models that are used for side-channel website fingerprinting attacks.

We are going to consider two microarchitectural attack scenarios where the adversary and victim share the same hardware. The adversary, who has a malicious application installed in the victim’s device, either has access to performance counters or implements a last-level cache monitoring technique in the victim userspace. In the meantime, the victim performs privacy sensitive activity, such as browsing. We assume that the adversary can detect the browser activity start time by observing the high variation in the side-channel data. The browser cache is disabled to only capture the network fingerprint rather than the website's memory utilization. To reduce the effect of rendering, the browser page is kept minimized after the website starts loading. The diagram for the website fingerprinting attack and its explanation with XAI algorithms are shown in the following figure.



The network data is captured by using Google ChromeDevTools in Google Chrome browser. First, the recording is started, then, the website is loaded. Since the browser cache is disabled, the websites are rendered as if the victim visits the website for the first time. Therefore, the side-channel data contains more information about the network requests compared to an attack scenario that has the browser cache enabled. At the same time, the rendering takes longer than a repeated visit to a website as the whole content of the website is requested from the website server altogether.

The network trace includes the URL, starting, connecting, blocked, waiting and download time as well as the type of the downloaded object. The file download process has more fingerprint on the microarchitectural components since the network adapter directly uses the last-level cache [60]. Once the network data is captured, a parser code is used to determine the start and end time of each download request. As illustrated in the following figure, the network requests can be issued in parallel, which yields a higher increase in the hardware instructions counter. The drawback of the parallel requests is that it is difficult to distinguish the source of the website specific leakage in XAI analysis. In order to achieve a more precise matching between network requests and leakage points in the measurements gathered during the XAI analysis, the network trace and side-channel measurements are finally aligned in a suitable manner.



Once an ML/DL model is trained, there is a variety of XAI methods to determine which features in the input are the most dominant . Therefore, a number of metrics have been presented to assess the effectiveness of XAI techniques throughout numerous fields. Since the Tor attack scenario is more complex and realistic than the performance counter-based attack scenario, the Remove and Retrain (ROAR) metric is utilized in this study.

Side-channel website fingerprinting attacks have become one of the most dangerous threats against internet users. Even though there are many defense techniques to prevent hardware-based and browser-based attacks, new microarchitectural attacks are still being constantly developed to track user activities on the web. The method that has been introduced here shows how to defend the web browsers against ML/DL-based website classification techniques by implementing a XAI-assisted adversarial defense technique [30–32].

Enhancing Website Security with ML algorithms

Web security is being revolutionized by Artificial Intelligence (AI) and Machine Learning (ML), which offer analysis and optimization for proactive threat detection and prevention. By analyzing behavior patterns and detecting anomalies that might indicate security breaches, artificial intelligence (AI) and machine learning (ML) technologies are being utilized to identify and prevent cyber threats. Websites and applications can be protected against unauthorized access, data breaches, and other security threats by incorporating these technologies. The following are some ways that web security is evolving as a result of AI and ML:

1. Threat Detection and Prevention: One important field of scientific research and development is the implementation of artificial intelligence (AI) and machine learning (ML) to threat detection and prevention in website security. These technologies are being used to analyze user behavior patterns and identify anomalies that might lead to possible security breaches. Websites and web applications can be protected from unauthorized access, data breaches, and other security threats by integrating these technologies.

   By analyzing huge amounts of data to find patterns and abnormalities that can point to possible security breaches, AI and ML play a critical role in threat detection and prevention. Cyber attacks can be detected and prevented in real-time by analyzing user behavior and identifying abnormal activities, improving the overall security posture.

2. Large-Scale Attack Detection: Large-scale attacks pose a serious threat to website security, in particular to large scale organizations. Collaboratively, hackers breach websites holding tens of thousands of credit card numbers, addresses, and names. AI has made it easier to identify large-scale attacks than it previously was since it can examine multiple data points simultaneously and set apart normal and abnormal events. Consequently, attempts to breach websites of all sizes are impeded through the application of artificial intelligence.

   The potential of AI and ML to improve Security Orchestration, Automation, and Response (SOAR) platforms by offering sophisticated analytics to support decision-making or just cutting down on the time and effort needed for manual investigations is being studied by researchers. Threat response workflows can be optimized by applying these technologies to integrate and automate various security tasks, procedures, and applications in response to security incidents. AI and ML act as force multipliers, empowering security analysts by providing advanced analytics and automating responses to security incidents. It has been determined that future research needs to focus on the application of AI and ML in SOAR platforms, as this has the potential to greatly enhance efforts related to cyber threat detection, mitigation, and prevention.

   In a similar way, AI and ML can rapidly examine millions of events and identify a wide range of threats, such as malware that takes advantage of zero-day

vulnerabilities or risky behavior that may turn into a phishing attack. Given time, these technologies become more intelligent, using past collected information to identify novel attack kinds. Real-time research and analysis of potential online threats is made feasible by AI and ML. Additionally, they employ computers to create behavioral models of people, which they subsequently utilize to forecast cyber threats as new data becomes available. When these technologies integrate, businesses can improve the effectiveness of their security defenses by responding more quickly and accurately.

3. Individual Behavior Observation: AI-powered tools have proven to be able to produce behavioral insights faster and more accurately than human capabilities, making it possible to analyze and predict human behavior with previously unheard-of speed and accuracy. Neural networks are used in machine learning, the primary technology underlying automated insights generation, to carry out specific tasks in a manner akin to that of the human brain. These tools can offer both high-level overviews and detailed information on data from a variety of sources, including survey results, product reviews, social media comments, and call center transcripts, by utilizing proprietary algorithms and AI.

   Additionally, AI and ML have been employed to predict human interactions and body language in videos, enabling machines to make better predictions about human behavior and coordinate their actions with humans. These developments highlight how AI and ML can be used to comprehend and analyze human behavior, providing insightful information for a variety of fields including public policy, behavioral sciences, social welfare, and healthy lifestyle interventions.

4. Web Shell Detection: Web shells are web-based applications that allow threat actors to access a system (from file access and upload to the ability to execute arbitrary code on the exploited server). This interaction can result in unauthorized access, data theft, and other security breaches, so web shell detection is a vital component of cybersecurity. Given that these web shells are often written in a variety of languages, such as PHP, ASP, Java, and JavaScript, it can be difficult to detect them because of how easily attackers can alter and obfuscate them. They affect everyone who has a website or web application (even those built on WordPress or other similar platforms). Artificial Intelligence (AI) and Machine Learning (ML) are being utilized to improve web shell detection capabilities in order to overcome this challenge.

   ML excel at automating time-consuming and error-prone security tasks, such as network log analysis, threat analysis, and vulnerability assessment. These technologies are capable of assigning precise risk scores, prioritizing resource allocation to address pervasive attacks, and analyze prior cyberattack datasets to identify areas targeted by particular attacks. AI and ML can also be used to train models to distinguish between malicious and legitimate activity, securing mobile endpoints and thwarting voice-based commands.

Various scientific papers have introduced tools to address web shell detection problems. For instance, a study proposed a novel method based on an optimal threshold to identify files containing web shells, while another source emphasized the use of machine learning for detecting unusual behavior, identifying new attack patterns, and mitigating zero-day attacks. To sum up, AI and ML play a crucial role in enhancing web shell detection by analyzing patterns of malicious activities, improving the accuracy of threat detection and classification, and automating security tasks.

5. Threat Detection and Classification: AI and ML models can be trained on labeled and unlabeled sample sets, improving the accuracy of threat detection and automating response tasks. Furthermore, AI and ML can automate the classification of new threat patterns, enabling security teams to predict and mitigate the impact of identified vulnerabilities and potential threats. They also play a vital role in automating tasks related to threat detection, response, and classification, ultimately enhancing the efficiency and effectiveness of security operations.

   Threat intelligence involves forecasting potential attacks and enticing potential attackers to take the bait, triggering signal detection, which starts an inquiry into shady activity on the network automatically. ML models are trained on historical datasets to identify patterns and predict potential security threats, enabling security teams to proactively respond to evolving cyber threats. ML algorithms use supervised learning to classify data as neutral or harmful, allowing for the identification of potential attacks in their earliest stages. ML's ability to analyze large volumes of data and spot patterns makes it ideal for detecting attacks, uncovering network vulnerabilities, and anticipating when and how future cyber attacks will occur.

   There are three types of ML used in cybersecurity, supervised learning, unsupervised learning and reinforcement learning. Supervised learning trains an algorithm on how to organize labeled data according to the relationships between inputs and outputs, through the use of labeled data. Unsupervised learning is the process by which an algorithm that has been trained on raw or unlabeled data labels and classes the data without the assistance of a human. Unsupervised learning is utilized by security teams to train algorithms to identify novel and complicated cyberattacks, particularly as hackers evolve their methods for breaking through corporate defenses. Reinforcement learning is a trial-and-error approach where an algorithm learns new tasks by using rewards for right action and penalties for wrong ones.

6. User and Entity Behavior Analytics (UEBA): User and Entity Behavior Analytics (UEBA) is a cybersecurity technology that uses machine learning (ML) algorithms to build a baseline of normal user behavior inside a network. UEBA extends User Behavior Analytics (UBA) to cover entities, such as routers, servers, and endpoints, and highlights anonymous behavior that could be the sign of a cyberattack.

Because UEBA solutions can detect sophisticated attacks on multiple users, IT devices, and IP addresses, they are more effective than earlier UBA approaches. UEBA is applicable in machine learning and behavioral analytics to users, machines, and entities, helping to detect and stop threats that traditional security tools might miss, like malware, insider threats, and advanced attacks.

By analyzing activity from hosts, apps, data repositories, network traffic, and other entities, such as network users, ML can assist with UEBA. To create a baseline of typical activity, machine learning is applied by ML algorithms to both historical and real-time data. The algorithms can identify potential threats and detect anomalies once a baseline has been established. Additionally, even in the absence of a known threat, ML might notice something strange and notify security teams to look into it further.

The application of unsupervised learning algorithms is one way machine learning (ML) can assist with UEBA. These algorithms are capable of analyzing vast amounts of data to find anomalies and potential threats, including system logs, network traffic, and user behavior. Over time, these algorithms can improve their ability to identify and stop threats by learning from this data. Furthermore, data can be classified as neutral or harmful using supervised learning algorithms, which enables the early detection of possible attacks [33−41].

Website challenges and protection techniques

Nowadays websites are interactive and data and information can be transmitted and updated into the systems, thus Web 2.0 or current websites are coming with different challenges and risks, such as

- SQL Injection → It is a widely known code injection technique that allows attackers to execute malicious SQL queries by inserting them into an entry field, such as a login form or search bar, on a website. They can be used to target any application that uses a SQL database, including MySQL, Oracle, and Microsoft SQL Server. SQL Injection attacks work by exploiting vulnerabilities in web applications that allow user input to be included in SQL statements without proper validation or sanitization. Attackers can use various techniques to inject malicious SQL code into the application, such as using SQL comments, modifying existing SQL statements, or using UNION statements to combine multiple SQL queries. Once the malicious SQL code is executed, attackers can gain access to sensitive data, modify or delete data, or even take control of the entire database server.
- Cross Site Scripting → It is a prevalent and severe security vulnerability that can be found in web applications. It enables attackers to inject malicious scripts into web pages viewed by other users. XSS attacks occur when a web application includes untrusted data in a new web

page without proper validation or escaping, allowing an attacker to execute scripts in the victim's browser. The impact of XSS attacks can range from petty nuisances to significant security risks, depending on the sensitivity of the data handled by the vulnerable site and the nature of any security mitigations implemented. The effects of XSS attacks can include the theft of session cookies, account hijacking, and unauthorized access to sensitive data. These attacks are typically classified into three main categories: stored/persistent XSS, reflected/non-persistent XSS, and DOM-based XSS. Each category has its own unique characteristics and potential impact. The actual attack occurs when a victim visits a web page or web application that executes the malicious script. Attackers often initiate an XSS attack by sending a malicious link to a user and enticing the user to click on it. If the application or website lacks proper data sanitization, the malicious link executes the attacker's chosen code on the user's system. As a result, the attacker can steal the user's active session cookie, gaining unauthorized access to the user's account. To prevent XSS attacks, developers must ensure that all user input is properly validated and sanitized before being included in web pages. This can be achieved by using secure coding practices, as well as implementing web application firewalls (WAFs), that could be used to detect and block XSS attacks by analyzing incoming web traffic and blocking any requests that contain suspicious scripts.

- Denial of Service Attack → It is a cyber attack aimed at making a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network. The primary goal of a DoS attack is to overwhelm a target with traffic or send information that triggers a crash, making the target inaccessible to legitimate users. Some common methods for carrying out a DoS attack include "Buffer overflow attacks" (These attacks involve sending more traffic to a network address than the programmers have built the system to handle, causing the target to crash or become unresponsive), "ICMP flood" attack (this attack leverages misconfigured network devices by sending spoofed packets that ping every instance of a specific machine instead of just one, then the network is triggered to amplify the traffic, leading to a smurf attack or ping of death) etc.
- Arbitrary Code Execution → Arbitrary Code Execution (ACE) in computer science refers to the ability of an attacker to run any code or commands of their choice on a target machine or in a target process. ACE is a serious security vulnerability that can be exploited by attackers to gain control of a system, and it can be taken advantage of without the need for any user interaction. ACE vulnerabilities can be classified into several categories, including memory safety vulnerabilities, deserialization vulnerabilities, type confusion vulnerabilities, and GNU LDD arbitrary code execution. ACE attacks can have significant consequences for organizations, including data theft, system compromise, and unauthorized access to sensitive information.

- Data Breach → It is a cyber attack in which sensitive, confidential, or otherwise protected data has been accessed or disclosed in an unauthorized mode. The consequences of a data breach can be severe, including identity theft, financial loss, and damage to an organization's reputation. To mitigate the risk of data breaches, organizations should implement various security measures, such as using strong encryption, implementing proper access controls, and providing regular security training for employees.
- Remote File Inclusion → RFI is a web vulnerability that allows a malicious attacker to exploit a web application and cause it to include a remote file. This vulnerability occurs when a web application dynamically includes external files or scripts, and the URL of the remote file might be passed in a user input parameter. RFI vulnerabilities can lead to arbitrary code execution, sensitive information disclosure, cross-site scripting (XSS), and even full system compromise. RFI attacks work by manipulating the URL of a remote file to include malicious code, which is then executed by the web application.
- Insecure deserialization → Insecure deserialization is a type of vulnerability that arises when an attacker can manipulate the serialized object and cause unintended consequences in the program’s flow. An insecure deserialization bug can often result in remote code execution, granting attackers a wide range of capabilities on the application. Even in cases where remote code execution is not possible, insecure deserialization can lead to privilege escalation, arbitrary file access, and denial-of-service attacks. The impact of insecure deserialization can be severe, as it provides an entry point to a system, allowing an attacker to reuse existing application code in harmful ways, resulting in numerous other vulnerabilities. Deserialization-based attacks are made possible due to the number of dependencies that exist in a typical site, creating a massive pool of classes and methods that is difficult to manage securely. Defending against deserialization vulnerabilities is extremely difficult, and there is no one-size-fits-all solution. Some ways to defend include monitoring the deserialization process, encrypting serialization processes, not accepting serialized objects from unknown or untrusted sources, running the deserialization code with limited access permissions, and using a firewall that detects insecure deserialization
- Implemented components with known vulnerabilities.
- Insufficient logging and monitoring → Insufficient logging and monitoring is a vulnerability that occurs when an application or system does not adequately record and monitor events, making it difficult to detect and respond to security incidents.
- Buffer overflow → It occurs when a program writes data to a buffer beyond the buffer's boundary, overwriting adjacent memory locations. Buffers are areas of memory set aside to hold data, often while moving it from one section of a program to another, or between programs. When a buffer overflow occurs, it can lead to corruption or overwriting of the data in adjacent memory locations, potentially causing the

program to crash or allowing an attacker to execute arbitrary code. This vulnerability is a common target for cyber attackers, as it can be exploited to gain unauthorized access, modify data, or disrupt the normal operation of a system. To prevent buffer overflow vulnerabilities, developers should use secure coding practices, such as input validation and proper bounds checking. Additionally, organizations can implement runtime protections, such as address space layout randomization (ASLR) and data execution prevention (DEP), to make it more difficult for attackers to exploit buffer overflow vulnerabilities.

- Local file inclusion → LFI is a web vulnerability that allows an attacker to trick a web application into including files on the server. This can lead to a range of security issues, including information disclosure, remote code execution, and even Cross-site Scripting (XSS). LFI occurs when an application uses the path to a file as input. If the application treats this input as trusted, a local file may be used in the include statement, allowing an attacker to access or run files on the server. LFI is similar to Remote File Inclusion (RFI), but instead of including remote files, only local files on the current server can be included for execution. LFI attacks are often found in poorly-written applications and can allow an attacker to read and sometimes execute files on the victim's server. An attacker may use remote code execution to create a web shell on the server, and use that web shell for website defacement. Successful exploitation of an LFI vulnerability can result in remote code execution on the server, allowing an attacker to gain unauthorized access and potentially compromise the entire system. One of the most common causes of LFI vulnerabilities is the use of unvalidated user-input with a filesystem function that includes files. In PHP, for example, the include and require statements are often the source of these vulnerabilities [63 – 71].

Technical steps on how to maintain a wordpress website secure

The use of WordPress as a content management system offers convenience and flexibility for website managers, but its popularity also makes it a target for malicious activity. The platform's widespread use and ease of website design create vulnerabilities that can be exploited by hackers and malware. Securing a WordPress website is crucial to prevent unauthorized access and potential threats. Implementing security measures is essential to protect user information and prevent potential attacks. The use of a web application firewall (WAF) is recommended to block malicious traffic and enhance security. Additionally, installing SSL certificates, removing unused themes and plugins, and enabling two-factor authentication are effective methods to improve WordPress security. Trusted security plugins such as Wordfence and BulletProof Security can provide real-time malware signature updates and alert notifications to protect against suspicious activity. It is also important to use strong passwords, manage file permissions, and restrict access to sensitive files to enhance security without relying solely on plugins. Furthermore, securing a WordPress website is essential to prevent Google blacklisting, retain user trust, and reinforce revenue. By prioritizing security,

website owners can protect user data, maintain a positive reputation, and achieve their website's goals effectively.

WordPress is a popular content management system that offers convenience and flexibility for website managers. However, its popularity also makes it a target for malicious activity. Securing a WordPress website is essential to protect against potential threats and ensure the safety of user data. There are several tools and methods available to enhance WordPress security, each with its own advantages and disadvantages. Implementing a combination of these tools and methods can significantly improve the security posture of a WordPress website.

One of the most effective ways to secure a WordPress website is by using security plugins. These plugins offer comprehensive features to keep websites safe and secure. Some of the most popular and widely recommended plugins include iThemes Security, Patchstack, Sucuri Security, Wordfence Security, MalCare and All In One WP Security & Firewall. Using any one of these WordPress security plugins can help you protect the web users that visit your website from unauthorized hackers and programs.

- Wordfence Security: The Wordfence security plugin is a popular tool for securing WordPress websites. It has a value for money free version and is a great option for brand new sites or those with a low budget, concerning the pretty good percentage protection against malware attacks.
    - Pros →
        - The plugin provides real-time malware signature updates and alert notifications, helping to prevent unauthorized access and potential security breaches.
        - A specialized 24-hour incident response team is in place to respond to security incidents within one hour for priority customers.
        - It is known for its user-friendly interface.
        - The endpoint firewall protects the site effectively against most threats, as it is frequently updated, the newest firewall rules are applied and malicious IP addresses are addressed accordingly.
        - The integrated malware scanner blocks requests that include malicious code or content. It also checks core files, themes and plugins for malware, bad URLs, suspicious contents in files, backdoors, SEO spam, malicious redirects and code injections.
        - It compares the site’s core files, themes and plugins with what is in the WordPress.org repository, checking their integrity and reporting any changes to the administrator.
        - Its free version is capable of repairing the unhealthy files and successfully removing the malware files that exist. It successfully cleans the known malware it discovers.
        - When it comes to login protection, brute force protection is in the firewall section and is enabled by default. There is a set of customizable options if you go into the settings.
        - Two factor authentication and recaptcha can be enabled as a free version feature.

    - There are options that can enforce strong passwords, prevent the use of passwords found in data breaches, prevent discovery of usernames and much more.
    - It gives the ability to disable or add 2FA to XML-RPC. XML-RPC (XML Remote Procedure Call) is a protocol that allows software running on different operating systems in disparate environments to make procedure calls over the internet. It uses HTTP as the transport mechanism and XML as the encoding mechanism. It is designed to be as simple as possible while allowing complex data structures to be transmitted, however it has some security concerns and this is the reason it is widely recommended to be disabled if it is not completely necessary, as it can pose a security risk.
    - Regarding the *premium version*, some of the extra features provided are that real-time firewall rule and malware signature updates are applied via the Threat Defense Feed and country blocking can be implemented. It checks to see if the site or IP have been blocklisted for malicious activity, generates spam or other security issues. A real-time IP Blocklist blocks all requests from the most malicious IPs and therefore protects the site while reducing load.
    - Excellent documentation is provided, explaining each option's functions and the best ways to apply them to protect the website. Plus, since it’s an official wordpress plugin, it enables deep integration with the famous platform.
    - Unlike cloud alternatives it does not break encryption, cannot be bypassed and cannot leak data.
    - It checks the site for known security vulnerabilities and alerts the administrator to any issues. It also alerts for potential security issues when a plugin has been closed or abandoned.
    - Out-of-date plugins are flagged as a medium threat, as well as plugins with discovered vulnerabilities are flagged as critical threats correctly.
    - It blocks crawlers that are using too many resources or stealing content.
- Cons →
    - The biggest disadvantage of this plugin is that it can scan for malware in the core files and non-premium plugins and themes, but it does not detect malware in the database, which is often a target for malware. This limitation can be a disadvantage for website owners who require comprehensive malware detection and protection, since database-based malware is a very real and dangerous problem.
    - Wordfence does not come with CDN, so it’s suggested to pair it with a reliable free *CDN*.
    - The free version of the plugin loads as a regular plugin after WordPress has loaded, which is only somewhat effective.

Ideally, a firewall should load before WordPress to block out all malicious traffic.
- The free version firewall only receives updates after the premium version, which can take up to 30 days.
- It can have quite an impact on your server resources. Every time a scan runs, you will notice a significant reduction in your site's performance. It is not a cloud-based platform.
- The firewall also runs on the site's resources, so if the site gets hit with a sustained attack, there would be trouble even if it's protected against these exploits.
- It does not inquire about any bot protection by itself.
- It can't remove newly discovered malware, since it is only capable of removing files of already known types of malware.
- It isn't able to deal with malware that is in the database. It also does not remove malware from non-core WordPress files or premium plugins, and themes.
- It is recommended to keep the learning mode active for a week before turning it on. This is because firewalls require live traffic to learn, so that it can reduce the chance of the firewall blocking out legitimate traffic.
- To acquire an activity log one should enable debugging from the diagnostics section which gives more verbose logs. Also enabling the debug mode will take up more server resources.
- Malware cleanup costs 490$ and is included in a annual care plan.

- Sucuri: Sucuri Inc is one of the top website security companies in the world and it provides security software and services. It offers a powerful WordPress plugin that one can install to protect their website from malware and hacks. It creates multiple layers to safeguard a website from security threats and acquires a cloudproxy firewall that bypasses all the website's traffic before sending it to the hosting server. The wordpress security plugin that Sucuri offers possess multiple features, some of which are shown below.
    - Pros →
        - Remote Malware Scanning: Uses Sucuri's scanner, SiteCheck, to search the site for malware.
        - Security Activity Auditing: Logs all security-related activity on your site, including logins, failed login attempts, etc.
        - Effective Security Hardening: Security hardening removes vulnerabilities, such as removing your WordPress version display and protecting your uploads directory.
        - File Integrity Monitoring: Automatically detects any changes to your files.

- Blacklist Monitoring: Checks with blacklist engines to make sure your site isn't being blocked for security issues.
- Security Notifications: How and how often the administrator is notified of every activity done by the plugin is customizable.
- Post-Hack Security Actions: A checklist of actions one should take in case their site is compromised, is offered.
- The Pro version includes Sucuri's Website Firewall, which is a reverse proxy that filters all your traffic through one of various Points of Presence (POPs) around the world. It will proactively defend the website from DDoS, brute force and other attacks.
- Sucuri maintains a huge knowledgebase on their website with all the information needed to provide a security environment to a website and they have a blog where they post security tips as well.
- For the free version of the plugin, one can post in the WordPress.org support forums for help. The developers are active there and most threads are responded to and resolved quickly.
- The Pro version of the plugin includes customer support from the developers via support tickets, and there's a Business plan that includes live chat support.
- The DNS level firewall helps address attacks and improves loading speeds when DDoS, brute force, spam or other attacks are taking place.
- Sucuri keeps logs for every activity.
- Takes precautionary measures to prevent the website from succumbing to harm and blocks all attacks at the server level. Server-level scanning is provided and protects the WordPress websites servers from attacks. Also new and potential security threats are monitored. The Sucuri team informs these security issues to WordPress' core team and work side-by-side to patch the servers.
- All the website's traffic is firstly filtered through Sucuri's cloud servers and is being analyzed in order to decide whether something malicious is going through and if so, it is being discarded.
- The vulnerabilities are patched at firewall-level and the website remains protected from the majority of malware, as it is addressed very soon.
- It hardens the WordPress security with the 1-click hardening feature.
- The premium version comes with CDN which adds to the performance optimization.

        - It has a 24/7 customer support. The premium users have an extra available feature, the instant chat.
        - It offers Firewall plans that start at $9.99 per month. This is perfect for bloggers and small site owners requiring occasional cleanups with ongoing security scans.
    - Cons →
        - By installing the firewall, you'll allow Sucuri to see all incoming traffic.
        - Sucuri is a bit pricey for small businesses, as the lowest price available is $199.99.
        - The Web Application Firewall (WAF) is available only for Premium customers.
        - The free version of Sucuri has some limitations, such as the absence of bot protection and an activity log, which are important features for comprehensive website security.
        - Performance Impact: Some users have reported that Sucuri can have a significant impact on website performance, which may be a consideration for website owners with high-traffic websites.
        - Complexity: Sucuri can be complex to configure and manage, which may require technical expertise and time to set up and maintain.

- Malcare: The MalCare WordPress security plugin offers a range of security features to help protect websites from malware and other security threats. It is one of the fastest malware detection and removal plugins. It possesses an automatic one-click malware removal which cleans the wordpress website before google blacklists it. MalCare has analyzed over 240,000 websites and acquired an intelligent scanning methodology that adds to the website's performance, while in the meantime it is able to identify even the most complex malware.
    - Pros:
        - The inbuilt plugin cloud-based firewall is free and ensures round-the-clock website protection against spam attacks.
        - The Cloud Based Deep malware scanner is *free* and one the most important and useful features it posseses.
        - The one-click malware cleaner offers unlimited automated cleanups.
        - It comes integrated with a complete website management module that ensures better WP security and site management to multiple websites from a single dashboard.
        - It notifies you if the WordPress site goes down.
        - A premium White-Label solution is offered that lets agencies provide better website security to their clients without risking their business.

    - It adds to the website's performance, as the cloud-based malware scanning is *free* and has no impact on the website's resources. Their owners claim MalCare finds complex malware that is usually missed by other security plugins.
    - Login protection from bots, malicious traffic identification and blocking, website hardening, brute-force attack prevention.
    - Some of the features in the paid version include identification and viewing of hacked files, folders and plugins, instantly cleanup of a hacked site (in less than 60 seconds), website hardening with the wordpress recommended best security practices, geo-blocking and uptime monitoring to ensure downtime is not happening.
- Cons:
    - The most advanced security features are only available with a paid subscription. For example, the support via email and chat is only offered in the paid version, as well as Geo-Blocking, Website Hardening, the instant One-Click Clean Ups, the automatic Clean-Ups, etc.
    - The free version of MalCare has some limitations, such as the absence of database scanning and backup, while in other security plugins you can find these features in the free version.
    - Potential Target for Attacks: Due to its popularity, MalCare may be a bigger target for attacks, as it has thousands more installs than some other security plugins. Of course this is something you find in every popular wordpress security plugin, but this may make it more vulnerable to potential security breaches and attacks.

To compare the above plugins, MalCare and Sucuri are the only security software providers that include Malware removal as part of their pricing. MalCare, Sucuri, and Wordfence include machine learning and improve their algorithm as they encounter other compromised sites. This cuts down on false positives and fixes false negatives. However, MalCare goes a step further with constant evaluation of 100+ signals to stand out from the crowd.

Another useful technique to harden a wordpress website is to disable php file execution in certain wordpress directories, where it's not needed, such as the directory "/wp-content/uploads/". In order to accomplish this, create a file and paste the following code inside. Next, you need to save this file as .htaccess and upload it to /wp-content/uploads/ folders on your website.

WordPress uses wp_ as the default prefix for all tables in its database, which can make it easier for hackers to guess the table name. Changing the prefix can improve the security of the site. There are several ways to change the prefix, including using a plugin, editing the wp-config.php file, or using phpMyAdmin. Changing the prefix involves modifying the database tables and updating all references to the old prefix. It is important to choose a new prefix that

```
<Files *.php>
deny from all
</Files>
```

is not too common and to avoid using personal information. Changing the prefix can be risky, so it is recommended to create a pre-production site to test the changes before making them live.

Directory browsing is a security vulnerability that can be exploited by hackers to gain access to files with known vulnerabilities. It can also be used by unauthorized individuals to view files, copy images, and obtain information about the directory structure. To prevent directory browsing, it is recommended to turn off directory indexing and browsing. This can be achieved by connecting to the cPanel's file manager, locating the .htaccess file in the website's root directory, and adding the following line of code to the end of the file.

```
Options -Indexes
```

Taking in mind everything said above, choosing the best security plugin for your needs is an important decision which should be made wisely. Some of the features one should consider are the following:

- Malware scanning → There are various techniques to scan for malware, and it may come in various forms. A method known as signature-matching involves comparing the malware's code to a database of known malware signatures. This is dependent on the accuracy of the signature database, which must be updated on a regular basis. Even so, there's never a 100% assurance that all malware will be found because the developers may not even be aware of the most recent threats.
- Malware removal → Malware removal from a website can be a challenging procedure. In certain instances, it is possible to remove the files that the malware added or repair the malware affected site files.
- Firewall → Unwanted or unnecessary traffic will be filtered out by an appropriate firewall, allowing only legitimate traffic through. For the newest security measures to be in place, a firewall needs to be updated on a regular basis.
- Vulnerability detection → The majority of hacking attempts are the result of system vulnerabilities . With the aid of a vulnerability scanner, you can quickly identify and patch any security holes in a website and have an adequate security setup.
- Activity log → It's critical to monitor any modifications made to a website in order to ensure that it remains safe and secure. By doing so, any suspicious behavior or malicious attacks can be identified and prevented immediately. The activity record facilitates constant monitoring and prompt identification of any security event.

Another essential tool for securing a WordPress website is an SSL certificate. Installing an SSL certificate is crucial for ensuring secure data transfer and encrypting sensitive information. SSL certificates help establish a secure connection between the web server and

the user's browser, preventing unauthorized access to data during transmission. By enabling HTTPS, websites can provide a secure browsing experience for visitors.

Web Application Firewalls (WAFs) are another critical security tool that blocks malicious traffic before it reaches the website. WAFs help protect against various cyber threats, including DDoS attacks, SQL injection, and cross-site scripting. By filtering and monitoring HTTP traffic, WAFs can prevent unauthorized access and potential security vulnerabilities.

In WordPress 3.5, the default prefix for all tables in the WordPress database is wp_, which is used to connect the WordPress site with web and mobile apps. However, the powerful nature of XML-RPC, which is enabled by default, can significantly amplify brute-force attacks. For instance, a hacker can use the system.multicall function to try thousands of passwords with a small number of requests. Therefore, it is recommended to disable XML-RPC if it is not being used. The .htaccess method is suggested as the best approach to achieve this, as it is the least resource intensive. Several methods, such as using a plugin or editing the .htaccess file, can be employed to disable XML-RPC.

The security of a website can be compromised when logged-in users leave their screens unattended, allowing unauthorized individuals to hijack their sessions, change passwords, or make changes to their accounts. To mitigate this risk, it is recommended to install an "Inactive Logout" plugin, which automatically logs out users after a specified period of inactivity. This feature is particularly important for e-commerce stores, where sensitive information is often stored. Inactive Logout is a security measure that enhances security and protects privacy by automatically logging out users after a period of inactivity. The plugin is easy to use and can be installed by uploading it to the WordPress plugins menu. Once installed, users can configure the plugin settings to suit their needs, such as setting the time period for inactivity and customizing the message displayed to inactive users.

Choosing a secure hosting provider is also critical for WordPress security. Reliable hosting companies offer robust security measures, including server-level firewalls, regular backups, and malware scanning. Secure hosting providers prioritize website security and provide a secure environment for hosting WordPress websites.

An identity theft protection service (like Aura) is important for a WordPress website because it provides an additional layer of security against cyber threats, as it is a common tactic used to gain unauthorized access to sensitive information. Identity theft protection services can help prevent identity theft by monitoring the dark web for stolen personal information, such as social security numbers, bank account numbers, and credit card information. They offer device and Wi-Fi network protection through VPN, which is crucial for when one is connecting to their WordPress admin from a public place. The VPN provides a secure and private connection, protecting the data from prying eyes. The dark web monitoring service constantly monitors the dark web using artificial intelligence to detect if your personal information has been compromised. This allows the user to act faster and better protect their digital identity. Identity theft protection services also offer credit file monitoring, public records monitoring, and identity recovery insurance and assistance. These services can help one recover their identity and assets in the unfortunate event that he’s a victim of online fraud.

Using reputable themes and plugins from trusted sources is essential for maintaining WordPress security. Nulled themes and plugins should be avoided, as they may contain malicious code that can compromise website security. Trusted theme providers offer regularly updated and secure themes, reducing the risk of potential vulnerabilities.

Two-factor authentication (2FA) is an additional layer of security that requires users to provide two forms of identification to access their accounts. 2FA can prevent unauthorized

access and protect against potential security breaches. WordPress offers several 2FA plugins, including Google Authenticator and Duo Security.

In conclusion, securing a WordPress website involves implementing a combination of tools and methods to protect against potential threats and ensure user data safety. By leveraging these tools and methods, website owners can enhance the security posture of their WordPress websites and provide a safe browsing experience for visitors

AI tools to maintain a wordpress website secure

WordPress is quite vulnerable to attacks. As it is open-source and comprises various components like plugins and themes, cybercriminals are always working to exploit the system's vulnerabilities to launch multiple attacks like data breaches, malware infections, and DDoS. AI technology has emerged as a game-changer in the realm of cybersecurity, bringing innovative solutions to protect WordPress websites from potential threats.

AI uses machine learning algorithms and advanced data analysis techniques to identify and respond to security threats. It does that in real-time and significantly reduces the risks of cyber threats. It analyzes vast amounts of data to understand the pattern of unusual activities that may indicate security breaches. So, whenever an attack occurs, AI detects the anomalies early, and AI-powered WordPress tools alert the website administrators to take appropriate attention to prevent potential damage. With Machine learning algorithms, AI analyzes user behavior and website traffic patterns that prevents it from causing unnecessary disruption by minimizing the occurrence of false positives.

AI-powered website security tools are also great at automating various tasks. Like scanning and updating plugins, themes, and core files to ensure there are no holes in the lineup. Similarly, it can also monitor and manage access control, ensuring that only authorized users have access. It also has a crucial role in strengthening the user authentication process. Instead of relying on the traditional password and username process. AI-powered authentication, like biometric identification and behavioral analysis, prevents brute force and phishing attacks.

Some of the most widely used and useful to have are the following:

- Quttera Web Malware Scanner: Quttera's patented AI scan engine scans your WordPress website for threats like malware, worms, backdoors, and more. The AI scan engine then investigates the files run through the scan, determining whether it is safe or if the administrator needs to clean up the website. Quttera uses three types of scanners to keep your WordPress website clean. Firstly, there is the external scanner that checks for threats from the perspective of a web browser. Secondly, the internal scanner checks the WordPress source files. Lastly, Quttera has developed a highly sensitive heuristic scanner that uses machine learning and AI to look for patterns in code that may showcase unknown, hidden WordPress malware within your code.
    - Pros:
        - One-click malware scan.
        - Patented artificial intelligence scan engine.
        - Detailed investigation reports.
        - Tracks block status on Google and other blocklisting authorities.

        - Detection of external links, malware, injected PHP shells, and more.
        - Malware detection and removal.
        - Comprehensive vulnerability assessments to fortify the site's defenses.
    - Cons:
        - It does not protect a website from getting affected.

- Beagle Security: It is a web-based solution designed to discover and address vulnerabilities in real-time. It uses machine learning algorithms to identify and address security vulnerabilities and complex attack vectors WordPress vulnerability scanners fail to detect, as the creators support. By leveraging an AI-powered core, Beagle Security does in-depth penetration tests on your website and discovers all the loopholes in it. With evidence-based vulnerability reporting, you get insights into the occurrence of each vulnerability on your website and actionable recommendations on how to fix the discovered security issues and secure your website.
    - Pros:
        - Easy to implement and user-friendly interface.
        - It provides detailed reports and workflow automation, helping users understand the risks and take appropriate action.
        - The primary goal is to test for cross-site scripting (XSS), SQL injection, and file inclusion exploits using its AI-powered core.
        - In addition to website security, Beagle Security also offers API security, ensuring that APIs are secure and protected from various security threats.
        - It allows for white-labeling, which is particularly useful for security service providers who want to offer their clients a branded solution.
        - Complete domain verification with just a button's click.
        - Classification of vulnerabilities according to the severity.
        - Gives the security score of the assessed website.
        - It is compliant with global security standards like OWASP and SANS.
    - Cons:
        - The initial scan can be slow.
        - The automatic scans feature is only available in the most expensive plan, which may be a limitation for users who want a more comprehensive solution.

- Astra: Astra is installed as an extension. Web Application Firewall to protect your website in real-time, on-demand machine learning-powered malware scanner, immediate malware cleanup, community Security & Vulnerability Assessment & Penetration Testing (VAPT) to find all possible flaws & business logic errors are offered.
    - Pros:
        - Malware scanning & removal.

        - Malicious file upload prevention, IP range blocking/whitelisting, bad bots blocking, fake search engine bots blocking, admin brute force protection, file Injection/Webshell protection, code Injection protection, directory traversal protection, layer 7 DDoS protection, smart honeypot system to trap hackers, htaccess security, turbo security engine that takes less than 0.002s to detect threats.
        - Fixing SEO spam / SEO poisoning (Japanese, Pharma or Gibberish hack), website redirect hack, admin panel hack, Credit Card or Payment Checkout Page hack, backdoor removal.
        - Ever updating rules engine
        - Database security.
        - Whitelist or Blacklist GET/POST/URLS.
        - Information about threat origin country, browser, device, etc.
        - Slack notifications: One can set custom rules to notify specific events on slack.
        -
    - Cons:
        - Astra's firewall has limited customization options, which may be a limitation for users who want more control over their website's security.
        - The free plan is limited to basic malware scanning and firewall protection, while the paid plans offer more advanced features such as real-time security alerts and malware removal.

- Akismet Spam Protection: Akismet is the plugin That comes packed in WordPress core package. Akismet helps WordPress users detect and manage spam comments.
    - Pros:
        - It uses advanced AI and ML algorithms to analyze and learn from a vast amount of data, enabling it to effectively identify and filter out spam comments and form submissions in real-time.
        - While Akismet is compatible with WordPress, it may not be as effective on non-WordPress platforms, limiting its utility for websites built on other content management systems.
        - By reducing the amount of spam content on a website, Akismet can help improve website performance by reducing the load on the server and improving page load times.
        - Akismet allows users to customize the plugin's settings to meet their specific needs, providing more control over the security of their website.
        - Akismet integrates well with other WordPress plugins, providing a more comprehensive security solution for website owners.
    - Cons:
        - Akismet's effectiveness is dependent on a stable internet connection, and it may not function optimally in offline or low-connectivity environments.

- While Akismet is compatible with WordPress, it may not be as effective on non-WordPress platforms, limiting its utility for websites built on other content management systems.

Overall, the role of AI is becoming increasingly essential to ensure WordPress website security, and cyberattacks are constantly evolving. Machine learning and data analysis techniques have made AI capable of understanding attacks and preparing itself to counter them at the right time. It has saved hundreds of websites and businesses from potential attacks by forcing a robust and efficient defense [43 − 50, 71−73].

Conclusion

In conclusion, the integration of artificial intelligence (AI) in website security presents a transformative shift in the cybersecurity landscape. The benefits of AI in cybersecurity are significant, including enhanced threat detection, reduced response times, and improved scalability. AI-powered security systems can detect possible infractions, automate compliance monitoring, and produce reports that adhere to legal requirements. The use of AI in cybersecurity is increasing rapidly, with many companies adopting it as a key tool in their cybersecurity strategy. However, it is important to note that while AI brings enhanced scalability to cybersecurity, it should be complemented by human expertise.

AI algorithms can process vast amounts of data and identify potential threats, but human analysts play a crucial role in interpreting the results, validating findings, and making informed decisions. The combination of AI's scalability and human intelligence creates a powerful synergy in enabling organizations to stay ahead of threats and protect their assets effectively. As attackers constantly evolve their tactics, AI capabilities allow website security to keep pace with the volume and complexity of modern threats.

By detecting risks sooner, responding faster, and adapting more autonomously, AI systems provide website owners the protection they need to operate with confidence. AI is no silver bullet, requiring integration and oversight by skilled teams. Therefore, the use of AI in cybersecurity is a game-changer, revolutionizing the approach to cybersecurity by providing advanced techniques to detect and prevent threats. It is important for organizations to carefully consider the benefits and limitations of AI in cybersecurity and to ensure that it is integrated and managed effectively to maximize its potential in enhancing website security [74].

Bibliography

1. ENISA (2023). Artificial Intelligence and Cybersecurity Research.
2. I. Alsmadi and F. Mira. Website security analysis: variation of detection methods and decisions.
3. R. Das and R. Sandhane (2021). Artificial Intelligence in Cyber Security
4. Attacking Artificial Intelligence
5. J. Grossman. The State of Website Security
6. H. Jiang and Z. Cui. Study on Problems and Countermeasures of E-commerce Information Security.
7. Canadian Centre for Cyber Security. Protecting your organization against denial of service attacks - ITSAP.80.100.
8. CISA. Understanding Denial-of-Service Attacks.
9. Why E-Commerce Security Matters Now More Than Ever
10. R. Duh, K. Jamal, S. Sunder (2002). Control and Assurance in E-Commerce: Privacy, Integrity, and Security at Ebay.
11. X. Hong (2012). Research of E-Commerce Security Technology.
12. M. Aydos, C. Aldan, E. Coscun, A. Soydan (2022). Security testing of web applications: A systematic mapping of the literature
13. R. Nanjundappa, S. Prasad, V. Musham, G. N, M. N, E. NamGung, Lakshya and A. Pahuja (2020). AWAF : AI Enabled Web Contents Authoring Framework
14. D. Yadav, D. Gupta, D. Singh, D. Kumar and U. Sharma (2018). Vulnerabilities and Security of Web Applications.
15. Z. A. Bakar and M. S. Shahibi (2010). Information Elements of a Website that Promotes Trust in e-Commerce
16. S. Almuhammadi, N. T. Sui and D. McLeodBetter Privacy and Security in E-Commerce: Using Elliptic Curve-Based Zero-Knowledge Proofs
17. M. Gaud and J. Traore. On the Anonymity of Fair Offline E-cash Systems
18. C. Fan and Y. Liang. Anonymous Fair Transaction Protocols Based on Electronic Cash
19. K. Nguyen, V. Varadharajan and Y. Mu (1999). Batching proofs of knowledge and its applications
20. Z. Qu, T. Ma and Y. Zhang (2008). Application of Parameter Modulation in E-Commerce Security Based on Chaotic Encryption
21. L. Kocarev (2001). Chaos-Based Cryptography: A Brief Overview
22. B. Xu and S. Xie (2009). Research of Session Security Management in E-Commerce System
23. Web services; SOAP and REST- A simple introduction
24. IBM - What is WSDL?
25. IBM - Web Services Security specification
26. Service Architecture - Web Services Explained
27. IBM - Web Services Secure Conversation standard
28. G. Kirubavathi and A. Nadarajan. HTTP Botnet Detection Using Adaptive Learning Rate Multilayer Feed-Forward Neural Network
29. How AI can Help Prevent Cyber Attacks in the eCommerce Sector
30. B. Gulmezoglu. XAI-based Microarchitectural Side-Channel Analysis for Website Fingerprinting Attacks and Defenses

31. S. Ali, T. Abuhmed, S. Sappagh, K. Muhammad, J. Moral, R. Confalonieri, R. Guidotti, J. Ser, N. Rodriguez and F. Herrera (2023). Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence
32. A. Panchenko, F. Lanze, A. Zinnen, M. Henze, J. Pennekamp, K. Wehrele and T. Engel. Website Fingerprinting at Internet Scale
33. M. Bautista. How AI and Machine Learning are Revolutionizing Web Security
34. T. Griffin. How AI Can Improve Your Website Security
35. K. Meehir (2023). How AI And Machine Learning Are Helping To Make The Internet Safer
36. IBM. What is SOAR?
37. O. Keyes (2019). Web Shells 101: Detection and Prevention
38. Z. Ai, N. Luktarhan, A. Zhou and D. Lv (2020). WebShell Attack Detection Based on a Deep Super Learner
39. SOCRadar. What are the Different Methods of Threat Detection?
40. G. Gottsegen. Machine Learning in Cybersecurity: How It Works and Companies to Know
41. M. Buckbee (2022). What is UEBA? Complete Guide to User and Entity Behavior Analytics
42. M. Bautista (2023). How AI and Machine Learning are Revolutionizing Web Security
43. N. Leonardus (2023). How to Improve WordPress Security: 22 Methods to Protect Your Website
44. 7 Best WordPress Security Plugins
45. Wordfence Security – Firewall, Malware Scan, and Login Security
46. Sucuri Review 2023: Why We Love Sucuri + Pros and Cons
47. The Complete WordPress Security Guide
48. Sucuri vs Wordfence: WordPress Security Plugins Showdown
49. MalCare WordPress Security Plugin – Malware Scanner, Cleaner, Security Firewall
50. MalCare Review PROS & CONS (2023) – MalCare vs Hide My WP vs Swift Security
51. M. Bang and H. Saraswat. Building an effective and efficient continuous web application security program
52. J. Grant. An 8-Step Application Security Risk Assessment Checklist for 2023
53. G. Stoneburner, A. Goguen and A. Feringa. Risk Management Guide for Information Technology Systems
54. Deep Dive: Current models of distributed assessment systems in science
55. White box Testing
56. S. Gantz and D. Philpott (2023). Security Assessment Plan
57. A Vulnerability Analysis and Prediction Framework*
58. I. Sarker (2021). Data Science and Analytics: An Overview from Data-Driven Smart Computing, Decision-Making and Applications Perspective
59. 12 Crucial Components Required to Conduct a Satisfactory Web Application Security Assessment
60. K. Kubota, W. Oo and H. Koide (2020). A New Feature to Secure Web Applications
61. Improving Web Application Firewalls to Detect Advanced SQLi Attacks
62. Cross-site scripting (XSS)
63. SQL Injection
64. What is a denial-of-service attack?
65. Denial of Service (DoS) guidance
66. Arbitrary Code Execution (ACE): Definition & Defense

67. Remote file inclusion (RFI)
68. What is insecure deserialization?
69. Deserialization Is a Core Component of Web Applications
70. Buffer Overflow Attack
71. File Inclusion Vulnerabilities: What are they and how do they work?
72. The Ultimate WordPress Security Guide – Step by Step (2023)
73. How is AI Enhancing Your WordPress Website Security?
74. The role of AI in Enhancing Website Security: Detection and Prevention