Journal of Education and Science (ISSN 1812-125X)

www.edusj.mosuljournals.com

Web Attacks and Defenses: Review Paper

A. A. Ahmed, N. B. Al Dabbagh

Department of Computer science, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq

Article information

Article history:
Received: January 18, 2023
Accepted: April 02, 2023
Available online: June 01, 2023

Keywords:
Security
Web Security
Web Attack
Cybercrime
Cybersecurity

Correspondence:
A. A. Ahmed
Email:
Ammaraladel@uomosul.edu.iq

Abstract

Because of the limited data that web applications collect from users, they are subject to information security risks. The most effective way to retain data in the modern era is through online applications. The process of providing data and data systems with appropriate procedural and sophisticated security safeguards is known as cybersecurity. Threats to cyber security are increasing at times. A flaw or weakness in a computer system, security tactics, internal controls, planning, or implementation that can compromise the security policy of a framework is known as a web vulnerability. The social, economic and political spheres of governments can be disrupted due to a vulnerability in the Internet, which can have an impact on the state. An effort is made to identify the defects and weaknesses while studying the weakness in order to take advantage of these weaknesses. The aim of this review is to understand the nature and scope of attacks targeting web applications and services. By analyzing web attacks, in addition to identifying attack patterns, web attack analysis can also help identify the root cause of the vulnerabilities being exploited by attackers. By understanding the nature of web attacks and the vulnerabilities that are commonly exploited, it is possible to Develop more effective defenses and countermeasures. Overall, the overarching goal of this review is to improve web security by identifying and mitigating vulnerabilities and threats.

DOI:10.33899/edusj.2023.137855.1319 , ©Authors, 2023, College of Computer Science and Mathematics, University of Mosul.
This is an open access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

Introduction

In the more than 30 years since its inception, the World Wide Web has advanced significantly. The web was mostly used in the 1990s to publish HTML text posts. At the time, a typical web page was just a regular HTML document displaying data for informational purposes only. In other words, Web 1.0 could be described as a “read-only” internet because websites at that time were not concerned with user experience and did not allow users to send any input back to the server that could change the flow of website interaction [1].

As web pages began to retain user-submitted data, permit input to change the website's flow, and most crucially, allow user communication, Web 2.0 came into being in the early 2000s [1]. The ability to create participatory blog sites, media sharing websites, and support for user profiles and data permanence made it feasible for these significant innovations to come together, essentially laying the groundwork for digital networking as we know it today. From that point on, the web shifted away from being a platform for document exchange and toward being a medium for exchanging web applications.

The modern web is an ever-expanding world of web pages, software, and associated media files, including movies, music, images, and other interactive materials. It is currently estimated that six out of ten people are "online" thanks to the massive advances in computing, miniaturization, and telecommunications, allowing more people each year to have a tool that allows them to access the Internet. 332 million people used the internet for the first time in the last year alone [2]. It is estimated that

each person on Earth generated 1.7MB of data every second in 2020. Although it takes time to explore, the truth is that all of our digital activity—including searching, streaming, scrolling, clicking, and making purchases—generates data.

Federal agencies, businesses, and NGOs are increasingly interested in web security. To enhance commerce and protect data, customers, and organizations from hazards, web security is essential. A network's continuation can be ensured by data technology security, which continuously monitors the network for dangers and mounts an effective defense against malicious attacks [3]. Dynamic websites are host machine software installations that provide client interactivity and a variety of other activities. Web applications are dynamic websites. Any business with a network of web servers needs to priorities web server security in order to guarantee users of their websites have a safe connection to the Internet [4].

People today save a huge amount of information on laptops and other devices with internet access. Because we want to keep data, information, and technology private and secure, cyber security is important. They appear to exchange private information, use passwords to steal money, or even change data to their advantage. In order to identify and fix any vulnerabilities, a penetration test simulates an attacker's behavior (often known as a hacker) in a controlled setting. A staggering number of businesses offer tools and services to examine security, including pen testing, risk analysis, threat modelling, and even ethical hacking training [5].

The primary steps of a security study are listed in Review of Security Testing and Vulnerability Scanning Method. Data sharing is carried out by the penetrator via a variety of ways, counting: the specific networks and systems that have been identified through discovery, Identification of Vulnerabilities: The penetration testing process's significant indication phase is crucial. This enables the client to identify the weaknesses of the target system and the best places to execute attacks. Aside from that Exploitation and attack launch: Following the discovery of flaws in the target architecture [3].

Cybersecurity is necessary at the company to protect its data, assets, and creative works. Regardless of the fact that copyright is less important and there is a greater chance of losing important files, such as family photos, people still need cyber security for the same reasons [6]. Cybersecurity plays a significant role in ensuring that the society can continue to rely on administrative units or state institutions. For instance, a city-wide blackout might result from a cyberattack that targeted a power station. It could steal from hundreds of thousands of people if it targeted a bank [7].

In this work, we seek to review electronic crimes, cybersecurity, and analyze web attacks with the aim of reaching a method through which the identity of the hacker and infiltrator can be proven and presented as criminal evidence in the courts.

Cybercrime and Cybersecurity

The rise of cybercrime has led to an increased focus on cybersecurity in recent years. Organizations, governments, and individuals are all vulnerable to cyber threats, and the consequences of a successful cyber attack can be severe, including financial loss, reputational damage, and even physical harm.

Cybercrime

The term "cybercrime" refers to a wide range of criminal activities that target computers, networks, networked devices, websites, or data, or that use ICT to support more conventional criminal activity [8][9]. Cybercrime is one of the illegal activities that is expanding the fastest in the world and has the potential to affect people, businesses, and organizations [10]. The primary factors driving the exponential expansion of cybercrime are its ability to cross geographical and physical barriers and its relative ease and speed of execution compared to traditional crime [11][12].

Digital ward violations and digital empowered wrongdoings are the two primary classes into which cybercrimes can be isolated, as per Europol. Cybercrimes that must be carried out with the guide of PCs and PC networks make up the principal class. Since all periods of these wrongdoings expect admittance to computerized foundation and can't be completed without admittance to PCs or the web, digital ward violations are once in a while known as "unadulterated digital violations" [13][14]. Cybercrimes that depend on innovation incorporate hacking of PCs, organizations, mists, and different frameworks, as well as PC infections, ransomware, and dispersed forswearing of administration (DDoS) attacks [15].

Conversely, digital empowered violations are more "customary" offenses like burglary and misrepresentation that have been committed utilizing PCs. Digital empowered violations contrast essentially from digital ward wrongdoings in that the last option can likewise be carried out without the guide of PCs or organizations. The degree and nature of violations permitted by the web have changed lately because of inescapable admittance to PCs and the web. Online misrepresentation, sentiment tricks, and Visa information burglary are only a couple of occasions of wrongdoings made conceivable by the web [16].

With regards to online protection, the expression "danger entertainer" is utilized to portray somebody who means to or has the ability to sabotage the IT security of an association by acquiring unapproved admittance to its information, organization, or frameworks. A danger entertainer is all the more especially someone who coordinates or participates in an unsafe assault planned

to hurt an outsider. Danger entertainers may be an individual, a gathering, an association, or even an administration sending off a cyberattack. Their ability levels can fluctuate [17].

Script kids are a gathering of unpracticed assailants. Script kids as often as possible use apparatuses made by other, more experienced danger entertainers to execute their assaults. Teens are oftentimes remembered for this class, but one shouldn't underestimate the assaults they commit. A delineation of one of the most notable content youngster hacks occurred in 2015 when a 15-year-old involved a SQL infusion weakness in the TalkTalk site, a UK telecom administration [18]. A great many shoppers' banking and individual data were disclosed because of the attack.

The entertainers in the classification of coordinated wrongdoing can be genuinely different, yet they all share one thing practically speaking: they are totally determined by the craving for monetary profit. As indicated by the Verizon Information Break Report, coordinated wrongdoing is answerable for around 40% of all assaults (Verizon, 2021). This posse utilizes different strategies, including more steady and centered assaults as well as untargeted, low-tech assaults like ransomware. Mage cart is one of the most dynamic organizations of coordinated wrongdoing programmers. They go after internet shopping basket frameworks to take installment card data through web skimmers. This gathering has pursued assaults against organizations like Ticketmaster, English Aviation routes, and Forbes magazine [19][20].

Hacktivists are a collective term for a number of activist groups who use cyberattacks to advance their sociopolitical agendas. These threat actors frequently use Distributed Denial of Service (DDoS) assaults on big businesses or governments in order to steal sensitive data. The most well-known hacker collectives are Anonymous and LulzSec, and both have attacked corporations including Fox Television, Sony, Nintendo, and even brought down the websites of the FBI in 2011 [21].

High level determined dangers are normally connected to country expresses that take part in cyberwarfare. These associations every now and again do attacks for the benefit of government organizations and are upheld, supported, and prepared by them [22]. Their essential targets are commonly other countries' crucial foundation; to which they endeavor to acquire unapproved access to direct insight activities. Legislatures have held onto APTs like Lazarus, which North Korea supports and which was answerable for the overwhelming Winery ransomware attack in 2017 [13]. APTs much of the time sendoff extensive assaults in light of the fact that the frameworks they target are excessively confounded and all around safeguarded to be penetrated by straightforward or mechanized techniques. APTs incorporate various preparation, perception, and different strides before the eventual outcome is understood [23].

Cybersecurity

Network protection, at its generally fundamental, is the discipline of forestalling unapproved access and different sorts of advanced assaults on networks, gadgets, frameworks, projects, and information [24]. Data innovation security is one more name for it that is much of the time utilized in a scope of utilizations, including business and portable registering [25]. Table (1) and Figure (1) and the following passages likewise give portrayals of the different parts of network safety.

Table 1. Cybersecurity Elements

Element	Description
Infrastructure and network security	The method involved with safeguarding PC organizations, frameworks, and different resources from assaults, unapproved clients, and gatecrashers
Application security	The most common way of keeping up with application security by looking at an application's source code to track down defects and weaknesses. Preferably, security ought to be incorporated into the application all through the plan stage as opposed to being added after it has previously been sent off.
Cloud security	Safeguarding distributed computing frameworks against interruptions, unapproved access, and assaults. Applications, information, and characters are currently put away on the cloud, where they are generally accessible to approved clients as well as danger entertainers whenever left unprotected. Hence, it is pivotal that arrangements like two-factor confirmation (2FA), VPNs, security tokens, information encryption, and firewall administrations be utilized to design allowed admittance in a legitimate way.
Information security	The act of securing data to prevent unwanted access, theft, or exposure while it is being stored or transported.
End user education	The most common way of expanding security mindfulness among end clients and other association laborers. The most erratic part of network protection is human way of behaving, which can unexpectedly make weaknesses by opening questionable connections in messages, utilizing unstable stuff like USB drives,

	having terrible secret word cleanliness, and so on. End-client security is eventually reinforced through instructional meetings pointed toward raising end-client security mindfulness.
Disaster recovery	The demonstration of setting up frameworks and practices that will send off the appropriate business activities response on account of impromptu events like cyberattacks, regular calamities, or power or organization blackouts. The catastrophe recuperation techniques basically give a system to how an organization will continue tasks and information after a disaster and return to the same old thing.

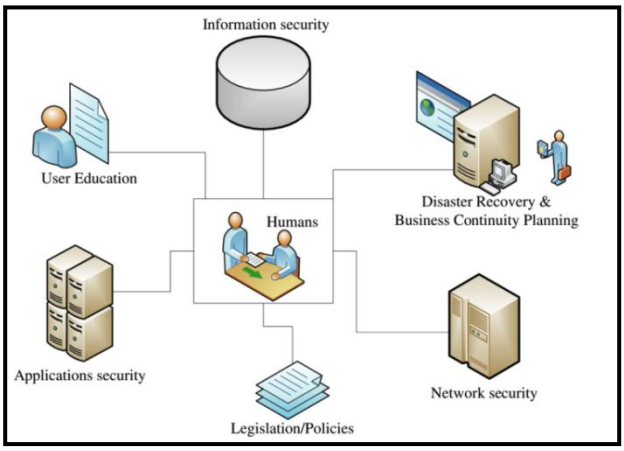

Figure 1. Cybersecurity components [25]**.**

Data security and network safety have some cross-over on the grounds that data security additionally manages safeguarding information in the internet. Online protection expands the act of guaranteeing the secrecy, uprightness, and accessibility of information that is put away on an organization, PC, server, or in the cloud. Today, most of data is saved carefully[26].
The expression "CIA triangle" alludes to a model of data security that comprises of three sections: secrecy, respectability, and accessibility, every one of which represents a vital objective of data security (See Figure 2).

Figure 2. The CIA triad [1]**.**

- **Confidentiality:** connects with safeguarding information. Financial matters, legislative limitations, or guidelines for industry consistence figure out which information is private and which isn't. The major reason of classification is to keep hidden data private. This basically implies that keeping up with privacy includes guaranteeing that main approved individuals can get to or alter information, and the business is responsible for keeping the two its own information and its clients' information safe [27]. Both purposefully and inadvertently, through an immediate assault by a danger entertainer or through a blunder by a worker or association part, secrecy can be broken.
- **Integrity:** relates to maintaining accurate data. Data integrity ensures that the information has not been altered, deteriorated, or subjected to illegal alteration while being stored or transported, whether on purpose or accidentally [28]. Since clients depend on accurate, dependable, and up-to-date information, the trust between the company and its customers may suffer if data is maliciously or unintentionally altered.
- **Availability:** Information openness is the demonstration of keeping up with accessibility. This infers that the information should be open to approved clients at whatever point the client makes an information demand [28]. While the capacity gadget for the information might be reachable, information accessibility can't be guaranteed on the off chance that other organization components fizzle or on the other hand on the off chance that there is a blackout and no reinforcements are accessible. A framework should be strong against interferences welcomed on by cyberattacks, blackouts, equipment breakdowns, and normal disasters to show accessibility. So, organizations and applications should work as they ought to for a framework to exhibit accessibility.

The CIA trinity fills in as the foundation of all security frameworks, yet it very well may be challenging to stick to each of the three immediately [29]. One of the CIA triangle standards will outweigh the others relying upon the business needs, security targets, general industry setting, and any administrative prerequisites of an association. An online business organization, for example, will probably accentuate accessibility on the grounds that any defer brings about lost pay. A business in the monetary area will probably focus on trustworthiness in light of the fact that any likely defilements in the monetary information it stores could make grievous impacts. Lastly, an organization like the tactical that arrangements with profoundly private or characterized data will put classification first.

Tracking down the best concordance between privacy, trustworthiness, and accessibility is oftentimes an urgent step, and it helps online protection groups in laying out needs. There will be compromises somewhere else in the event that one security premise is focused on over another. Picking an answer that completely safeguards secrecy and respectability might suggest that different variables like speed and execution endure. This procedure may be compelling for organizations in a single area, similar to medical services, however not really for organizations in different areas (like online business).

These sorts of compromises are normal in business, and going with a decision requires directing a money saving advantage examination. Every business ought to in this way ponder its own specific requirements and choose how to carry out these security guidelines while likewise ensuring they can offer a consistent and secure client experience [29].

WEB Attack Methods

Forswearing of administration assaults, intelligent bombs, misuse apparatuses, busybodies, deceptions, infections, worms, send spam, and botnets are among the most critical cyberattack strategies. Figure (3) portrays the vital classifications of cyberattacks. The approved clients' admittance to the framework as well as the other way around are lost while utilizing the refusal of administration strategy. As a matter of fact, the assailant starts flooding the objective PCs with messages at one point and impeding the real progression of information. Because of this, no framework can get to the Web or communicate with different frameworks [30].

Another strategy, known as wide Refusal of administrations, includes all the while going after from many scattered frameworks instead of a solitary source. Worms are often used to attack the objective along these lines, increasing on numerous frameworks. The overall population can get to apparatuses that can find and take advantage of weaknesses in networks at different expertise levels. One more kind of assault is a rationale bomb, in which a developer embeds code into a program so that, on account of a specific situation, the product consequently participates in hurtful way of behaving [31].

Sniffer is another device that screens directed information and outputs every bundle in the information stream for determined data like passwords [32]. Regularly, a deception seems to be a helpful program that the client will run and hides dangerous code [33]. Moreover, an infection taints framework records — generally utilized programs — by bringing a duplicate of itself into those documents. These forms work and license the infection to contaminate different records by stacking tainted documents into memory.

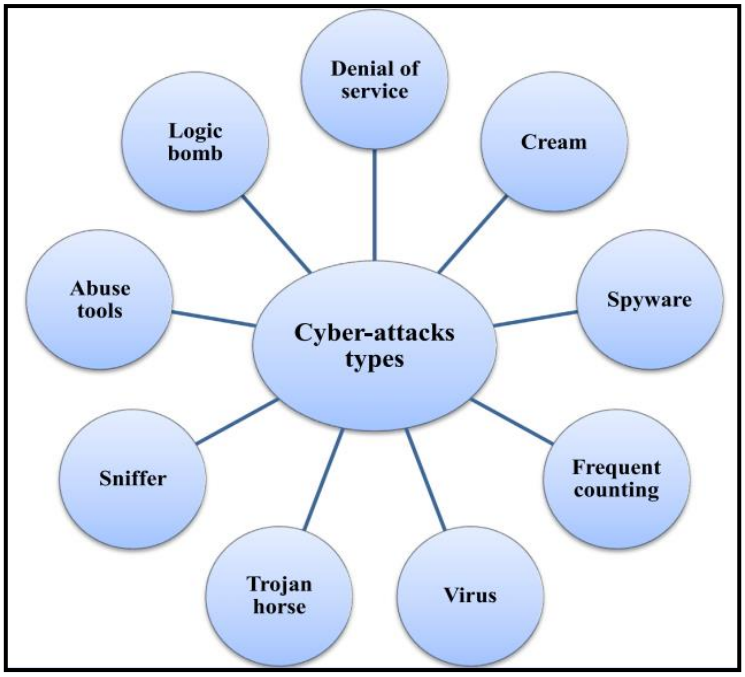

Figure 3. primary forms of cyberattacks.

WEB Attack Types.

The different types of Web attacks they are described in Table (2).

Table 2. WEB Attack Types [34]

Type	Description
Cross-site scripting (XSS) attack	The application-layer hacking procedure known as cross-website prearranging (XSS) is utilized to think twice about applications. At the point when a unique Page gets hurtful information from the assailant and executes it on the client's framework, an assault of this sort happens.
Cross-site request forgery (CSRF)	The casualty of a CSRF Web assault is forced into sending the assailant's structure information to the casualty's Internet server. The host structure is made by the assailant and shipped off the confirmed client with malignant information on it. The structure is finished up by the client and shipped off the server. The Internet server acknowledges the information since it comes from a reliable client.
SQL injection	At the point when an aggressor sends malevolent SQL code to an Internet application, a SQL infusion happens. By modifying an information base, it focuses on the information put away behind an application. Information is placed into a SQL question in this assault without being checked for legitimate designing or included get away from strings. Most applications that utilize a data set back end and don't uphold variable sorts have been known to be impacted by it.
Code injection	Like a SQL infusion assault is a code infusion assault. In this assault, the aggressor hacks the application and additions destructive code, for example, shell orders or PHP scripts, before the client sends any application to the server. The server runs the program when it gets the solicitation. This assault's principal objective is to set around or change the first application up to run erratic code, access obstructed sites or data sets, particularly those that incorporate individual data like passwords and charge card subtleties, and access confined Sites.
Command injection	Code infusion assaults are perceived by interruption recognition frameworks (IDS) and various sandbox execution conditions presented by the operating system. The dubious

	parcels' payload is shipped off the execution climate that matches the bundles' objective when the IDS distinguishes a bunch of executable guidelines in the organization traffic. The objective IP address of the showing up bundles is utilized to distinguish the suitable execution climate.
Parameter tampering	A particular sort of web attack known as boundary altering happens when an assailant alters or changes a URL's boundaries.
Cookie poisoning	Web applications use treats to store information on the clients nearby workstation, including client IDs, passwords, account numbers, and timestamps. In a treat harming assault, the aggressor changes a treat's items to take a client's very own data or stunt sites.
Buffer overflow	This attack can possibly adjust information, degenerate records, or uncover delicate data. Assailants will endeavor to over-burden back-end servers with additional solicitations to do a cushion flood assault. Then, to run erratic code and give the aggressor control of the projects, they give exceptionally planned input. Support flood issues can happen in both the Internet application and server items, what capability as one or the other static or dynamic parts of the site. Server items as often as possible experience the ill effects of support spills over, as is notable.
Cookie snooping	Treat sneaking around is the demonstration of an aggressor taking a casualty's treats and using them to sign on as the person in question, in some cases with the utilization of a nearby intermediary. This can be abstained from by utilizing safely scrambled treats and encoding the source IP address in the treat. For additional security, treat procedures can be completely connected with SSL capacity.
DMZ protocol attack	The semi trusted network zone known as the DMZ (peaceful area) isolates the organization's confided in inside network from the untrusted Web. Most of organizations confine the conventions that are allowed to go through their DMZ to further develop DMZ security and lower risk. End-client conventions like NetBIOS would essentially expand the security hazard to the DMZ's frameworks and traffic.
Zero-day attack	Zero-day assaults exploit weaknesses that were not recently unveiled, making them especially hazardous in light of the fact that it is basically impossible to avoid potential risk ahead of time. Between the time a specialist or aggressor finds a weakness and the time the seller delivers a fix, a ton of time can elapse. Sadly, it is absolutely impossible to ward against these assaults while the product is defenseless. It's essential to introduce fixes when they're free to decrease hurt.
Authentication hijacking	Most Web applications require validation, approval, and bookkeeping (AAA) administrations, which are contained for the most part of verification. Thus, the primary line of guard for affirming and observing the approved utilization of an Internet administration is confirmation.
Log tampering	Web applications keep logs to follow use examples of an application, including asset access, mistake conditions, client and head logins, and other application-explicit information. These logs are utilized for advertising examination, legal occurrence investigation, and exchange sealing. They are additionally used to fulfill legitimate record keeping commitments. At the point when nonrepudiation is important, the trustworthiness and openness of logs are especially pivotal.
Directory traversal	The capacity for an assailant to search for registries and documents beyond the extent of a typical program access is known as a registry crossing assault, likewise alluded to as a powerful perusing attack. This uncovers an application's registry structure as well as regularly the working framework and Web server that it is running on.
Cryptographic interception	By doing this, the programmer approaches a safe, scrambled channel through which to go after the web-based application. A programmer who can capture the signs that are cryptographically gotten can peruse and modify touchy material that has been encoded. A man in the center aggressor can wreck destruction on security utilizing the taken confidential keys and testaments, habitually without illuminating the gatherings in question.
URL interpretation	An assailant who mishandles the understanding of a URL by taking advantage of different text encoding methods is supposed to play out a URL translation assault. Web traffic normally enters unfiltered since it is viewed as "amicable." It is the most considered normal

	utilized sort of traffic that firewalls license. The URLs utilized for this sort of assault habitually contain extraordinary characters that call for novel language structure handling.
Impersonation attack	A pantomime assault happens when a programmer mimics a genuine client to parody Web applications. In this case, the assailant joins the meeting as a customary client through a typical port, keeping the firewall from spotting it. A server's weakness to this assault might be brought about by lacking meeting the executives coding.

Defenses of Web

As shown in Table (2), the six classes of guard components that were analyzed were Application, Gadgets, Organization, Social Designing, Strategy, and Framework.

Table 2. Defenses of Web

Defense	Description	Ref
Application	systems for applications that give safe handling.	[35][36]
Devices	Security-empowering systems for gadgets	[37][38]
Network	strategies or programming for keeping up with network effectiveness and security	[39][40]
Social Engineering	Encourage education and awareness	[39][41]
Policy	in a technique, convention, or standard, laid out rules	[42][43]
System	advances used to ensure framework security	[43][44]

- **Application:** Application security can be considered making extraordinary guard instruments that increment an item's general wellbeing. To obtain a particular result, various procedures may be picked. A security technique against timing-put together side-channel attacks with respect to the Web of Things' response time is recommended by the creators in [45]. The two pieces of this framework are security assurance and weakness testing. This proposition's exploratory result exhibits that the framework planned can precisely recognize and successfully hide side-channel spillages connected to response time. The creators of [46] propose utilizing a Blend Stowed away Markov Component (MHMM) to make danger insight that can follow and distinguish cyberattacks for Industry 4.0 frameworks. Utilizing actual power frameworks and UNSW-NB15 datasets, the procedure created exhibited its ability to totally distinguish physical and network dangers [35]. The component performed better as far as discovery rates, bogus up-sides, and handling times than five particular companion draws near. This study offers a commonsense system for assessing online protection perils in any Industry 4.0 situation. A structure is proposed in study [37] that contains a Block chain-based model conveyed across a SDN-IoT-empowered design to offer satisfactory security, which is the essential worry in Industry 4.0. The essayists ensure that all information is secure for Industry 4.0 applications by incorporating Block chain.
- **Devices:** Associations ought to guarantee that all equipment and programming is arranged securely and with controlled changes [36]. The creators of Ref. [38] portray the VulHunter structure, which expects to find novel weaknesses in the examination in light of the fix of existing weaknesses, for assessing and identifying weaknesses in IoT and Industry 4.0. The creators in [36] examine frameworks that direct character checks and information parcels, which can be utilized to guard against assaults on steering tables, to get network gadgets. The structure IoT-SI-Defender is introduced by the creators in Reference [47] to evaluate the security of delicate data spillage and abuse in each layer of IoT gadgets. The system's outcomes show that it is feasible to distinguish delicate data spillage destinations and safeguard against attacks by utilizing in-the-second hot fixes that are made to stop them. The blend of assault surface decrease, secure improvement life cycle, information assurance, secure and solidified gadget equipment and firmware, and AI might be basic in pushing ahead with a protected, cautious, and versatile Industry 4.0-empowered gadgets, as per Ref. [48]. Computer based intelligence is viewed for the purpose of danger discovery in gadgets.
- **Network:** Networks with changing security norms shouldn't speak with each other [49]. The creators in [49] propose a powerful Vehicle Layer Security (TLS)- based validation system that is impervious to MITM assaults for web applications that utilization the TLS convention to shield HTTP correspondences determined to guarantee correspondences between industry 4.0 production network accomplices. The proposed approach prevents an assailant from professing to be a genuine help to safeguard client secrecy. The creators of [39] present areas of strength for an of safeguarding a remote sensor organization, guaranteeing the honesty and credibility of information assortments, and distinguish and plan plausible weak endpoints in a modern worldview. For the situation study, the creators recognize the advances associated with Industry 4.0, as well as the safety efforts, possible dangers, countermeasures, and points of weakness related with every innovation, one of which is the Information Procurement (DAQ) gadgets and the

Correspondence Layer among DAQ and the cloud. The creators of Ref. [50] propose a product characterized network (SDN)- based guarded framework that incorporates a model for traffic the executives and peculiarity identification. The creators concentrated on the utilization of this technique for SCADA frameworks and IoT networks in light of this system [39]. It permitted the extraction of traffic examples to recognize and forestall different organization assaults like Location Goal Convention (ARP) caricaturing, replay assaults, and distinguish pernicious order sending ways of behaving.

- **Social Engineering:** Guard strategies against social designing can include preparing partners to detect requests for delicate data (telephone numbers, messages, and so on) or rerouting clients to fake sites that need to gather this data outside the organization's domain. The use of Truecaller or Dialer Programming is seen by the creators of [50] as a strategy of safeguard against phishing attacks. [38] prompts utilizing alert while utilizing messages, connections, and URLs that appear to be suspect. To bring down the gamble of assault, these connections ought to be twofold registered or physically put with the program.
- **Policy:** As indicated by the creators of Ref. [50], associations intending to send Industry 4.0 designs should initially settle on their data security approaches by using the ISO/IEC 27001 and ISO/IEC 27002 [51] norms. Subjects connected with protection, uprightness, and openness ought to be covered also, including stock of equipment and programming resources, security weakness the executives [38], reinforcements, the utilization of cryptographic controls, human asset security, and programming establishment constraints.
- **System:** As indicated by [38] states that Block chain innovation, which utilizes hash and cryptographic techniques, can likewise be used as a safeguard against different assaults on IIoT frameworks, for example, infusion assaults and malware assaults, while guaranteeing the classification and respectability of data sets and Block chain. To reinforce functional security in the battery's energy stockpiling frameworks against digital assaults, the creators of Ref. [51] additionally use Block chain, thinking about that it is decentralized, impervious to digital attacks, and can likewise be coordinated with the shrewd agreement framework.

Web attacks and defenses are two sides of the same coin, as they affect each other. Attacks on web applications and services are becoming increasingly sophisticated, as attackers use a range of techniques and tools to exploit vulnerabilities in web systems. At the same time, defenses are also evolving, with new security technologies and best practices emerging to help protect against these attacks. Web applications are vulnerable to a range of other attacks, such as denial-of-service (DoS) attacks, phishing attacks, and man-in-the-middle (MITM) attacks. Defenses against these attacks can include implementing firewalls, intrusion detection and prevention systems, and using secure communication protocols such as HTTPS.

In general, while web attacks and defenses are constantly evolving, it is clear that the best defense is proactive. Regular vulnerability assessments, penetration testing, and security awareness training can help identify and mitigate vulnerabilities in web applications and services before attackers can exploit them. In addition, organizations can benefit from investing in the latest security technologies and staying up-to-date on emerging threats to stay ahead of attackers.

Use Machine Learning in Web Defenses

Machine learning (ML) is an advanced technology that is being increasingly used in web security to improve the effectiveness of web defenses. ML algorithms can analyze large amounts of data to identify patterns, detect anomalies, and make predictions, which can be useful in identifying and preventing cyber attacks [52].

One application of ML in web security is in detecting and blocking malicious traffic. ML algorithms can analyze network traffic to identify patterns of suspicious behavior, such as repeated attempts to access restricted areas of a web application or unusual traffic spikes. By identifying and blocking this traffic in real-time, ML can help prevent attacks before they can cause damage [52].

Another application of ML is in identifying and mitigating vulnerabilities in web applications. ML algorithms can analyze code and data inputs to identify potential vulnerabilities, such as injection or cross-site scripting vulnerabilities. By identifying these weaknesses before they can be exploited, developers can proactively fix them to prevent attacks [53].

ML can also be used to enhance user authentication and access control. By analyzing user behavior and patterns, ML algorithms can detect and alert administrators to potential security breaches, such as suspicious login attempts or unauthorized access attempts. Additionally, ML can help develop more sophisticated access control policies based on user behavior, allowing for more fine-grained access control [53].

While ML is a powerful technology, it is not without its challenges. One of the key challenges is the need for large amounts of data to train ML models effectively. Additionally, ML models may be susceptible to attacks such as adversarial attacks, where attackers can manipulate the model's behavior by feeding it malicious input [54].

Related works

In 2011, ***Kallapur & Geetha*** provided an outline of the latest web-based security attacks. They likewise included a brief link to graphic assaults. Moreover, they sent messages over a period of time with data monitoring regarding the assaults. The report concludes by showing the need for such overviews and the potential for research here[55] .
In 2014, ***Bansal et. al.,*** uncovered a model extraction device that converts programs made in subsets of JavaScript and PHP into applied math consequently. Various beforehand unseen weaknesses in notable sites like Hurray and WordPress when they associate with informal organizations like Twitter and Facebook have affirmed the approach [56].
In 2016***, Kaura & Parminder*** analyze current web goes after that imperiled clients, information, or web applications. The Site Hacking Episode Data set (WHID), as well as other data security and news sites, are utilized in this paper's examination of web assaults. Furthermore, it is a work to concentrate on various attacks on huge classes of sites, which fills in as a kind of perspective for engineers to execute the legitimate protection measures proceeding. The main web not entirely set in stone, and the weakest web application types were analyzed [57].
In 2016, ***Mitropoulos et. al.,*** gave a study of several web code injection attack protection techniques. We suggest a model that identifies the main flaws that allow these attacks and offers a shared viewpoint for assessing the various countermeasures. Then, based on the traits of accuracy, performance, deployment, security, and availability, we categorise and evaluate a collection of 41 previously proposed defences. In light of the findings, which indicate that many protection mechanisms are not well evaluated, detection accuracy is particularly crucial. Additionally, it has been highlighted that several techniques can be evaded by attackers who are familiar with how they operate [58].
In 2017, ***Kong*** talked about the appropriate web security advancements, completely inspected the web application security according to three viewpoints — security dangers to the web client, security dangers to the web server, and security dangers to information transmission — and afterward explored security innovation in light of WEB applications. I'm trusting that the extension of this article will be helpful to the relevant field laborers [59].
In 2017, ***Stiawan et. al.,*** dissect digital assault techniques as well as the life structures of entrance testing to help security officials in directing a precise appraisal of the security on their organization frameworks [60].
In 2021, ***Alsharif et. al.,*** examining potential vulnerabilities and limiting risks by concentrating on how people behave in various situations, the human component can be improved. This survey demonstrated that the majority of participants lacked experience defending against cyber security risks and safeguarding their personal data. Furthermore, inadequate training and understanding of the top three human factor weaknesses in cyber security—phishing assaults, password attacks, and social engineering—are serious problems that must be handled and reduced [61].
In 2022, ***Sharma et. al.,***examined network safety and its capability in friendly penetration, how to perceive electronic robbery, and how to explore the explanations for and impacts of the flood in cybercrime. The creators finish up by giving a few down to earth protections against network safety attacks, dangers, and weaknesses. As indicated by the review, while innovation mastery assists with reducing the effect of cyberattacks, human way of behaving and mental qualities make individuals defenseless. Interests in authoritative schooling programs offer expectation that cyberattacks can be diminished,regardless of whether exploration uncovers dangers of mental weaknesses in cyberattacks [62].

Conclusion

Web security is an important aspect of protecting information online and preventing cyber attacks. Despite great efforts to secure web applications and services, there are still many vulnerabilities that attackers can exploit. Injection attacks, which occur when an attacker injects malicious code or commands into a web application, which could lead to data theft or modification. The most common types of injection attacks include SQL injection and cross-site scripting (XSS) attacks, as well as broken authentication and session management. Weak or broken authentication mechanisms can allow attackers to bypass authentication and gain unauthorized access to the application. In addition, bad session management can enable attackers to hijack authenticated sessions and impersonate legitimate users. Inadequate input validation can allow attackers to send malicious input to a web application, leading to data theft, system intrusion, or unauthorized access. . Common examples of insufficient input validation include buffer overruns, format string attacks, and integer overflows. Insecure communication over web applications that use insecure communication protocols, such as HTTP instead of HTTPS, is vulnerable to interception and eavesdropping. Attackers can intercept and modify data in transit, resulting in data theft or modification. From this it can be concluded that incorrect error handling Improper error handling can provide attackers with valuable information about application architecture, vulnerabilities, and vulnerabilities. This information can be used to plan and launch further attacks. Inadequate security controls, such as weak passwords, lack of access controls, and insecure configuration files, can make web applications vulnerable to attacks. To mitigate these vulnerabilities, it is important to implement comprehensive web security measures, such as regular vulnerability testing,

secure coding practices, and user awareness training. It is also essential to stay up-to-date with the latest security threats and trends to ensure that security controls are adapted and improved as necessary.

Acknowledgements

The researcher extends his thanks and appreciation to the University of Mosul, College of Computer Sciences and mathematics, Department of Computers, for providing support for the completion of this work.

Conflict of interest

The author has no conflict of interest.

References

1. Haaga-Helia, “Secure web development Pankaj Pant,” Haaga-Helia Univ. Appl. Sci., no. 8.5.2017, pp. 2003–2005, 2022.
2. G. YENİLMEZ KAÇAR, “the Relationship Between the Use of Social Media and Loneliness During Covid-19 Pandemic,” Atatürk İletişim Derg., no. Özel Sayı, pp. 93–110, 2021, doi: 10.32952/atauniiletisim.1034712.
3. M. M. Boke, “Web Security Vulnerability Analysis in Selected Ethiopian Governmental Offices (Using White Box and Black Box Testing),” no. June, 2022.
4. D. D. Kumar* and D. U. Sharma, “Smart Home using Visual Sensor Network and Li-Fi Technology,” Int. J. Recent Technol. Eng., vol. 8, no. 4, pp. 4791–4796, 2019, doi: 10.35940/ijrte.d7462.118419.
5. D. D. Bertoglio, G. Girotto, C. V. Neu, R. C. Lunardi, and A. F. Zorzo, “Pentest on an Internet Mobile App: A Case Study using Tramonto,” no. December, pp. 31–36, 2021, doi: 10.20533/icitst.worldcis.wcst.wcicss.2019.0004.
6. D. S. M. Apurv Yadav, Ajay Singh Paikra, “Experimental Analysis of Emission Performance Characteristics on Diesel and Diesel-Biodiesel Blends With Exhaust Gas Recirculation,” Int. Res. J. Eng. Technol., vol. 6, no. 6, pp. 1513–1519, 2019.
7. D. . V. Prajapati and D. Upadhyay, “Cyber Defence A Hybrid Approach for Information Gathering and Vulnerability Assessment of Web Application (Cyberdrone),” Int. J. Comput. Sci. Eng., vol. 7, no. 5, pp. 65–72, 2019, doi: 10.26438/ijcse/v7i5.6572.
8. A. M. Bossler and T. Berenblum, “Introduction: new directions in cybercrime research,” J. Crime Justice, vol. 42, no. 5, pp. 495–499, 2019, doi: 10.1080/0735648X.2019.1692426.
9. V. S. Alexandra Michota (ENISA), Andreas Mitrakas (ENISA), Andreas Sfakianakis, Catalin Patrascu, François Beauvois, Koen Van ImpAlexandra Michota (ENISA), Andreas Mitrakas (ENISA), Andreas Sfakianakis, Catalin Patrascu, François Beauvois, Koen Van Impe, Silvia, Roadmap on the Cooperation Between Csirts and Le Roadmap on the Cooperation Between Csirts and Le About Enisa, no. December. 2019. [Online]. Available: www.enisa.europa.eu.
10. C. Team, C. Co-cordinator, C. Editor, and P. Leader, COURSE GUIDE CSS 810 CYBERCRIME AND FORENSIC INVESTIGATION, National Open University of Nigeria,2021, ISBN: 978-978-058-313-2.
11. G. O. Teiu, “Cooperare judiciar ă interna ț ional ă în UE: EUROJUST,” no. October, pp. 0–70, 2019, doi: 10.13140/RG.2.2.25994.62405.
12. A. Alexandrou and A. Alexandrou, “Cybercrime. In M. Natarajan (Ed.), International and Transnational Crime and Justice (pp. 61-66). Cambridge: Cambridge University Press. doi:10.1017/9781108597296.010,” pp. 61–66, 2019.
13. Comisión Europea, “EU Strategy to tackle Organised Crime 2021-2025,”, EUROPEAN COMMISSION 2021, doi: 10.2837/64101.3.
14. E. Comission, “First progress report on the implementation of the EU Alcohol Strategy,” no. December, p. 61, 2009, [Online]. Available: http://ec.europa.eu/health/archive/ph_determinants/life_style/alcohol/documents/alcohol_progress.pdf
15. J. B. Barnes, “INSTRUMENTS OF THE EUROPEAN UNION IN FIGHTING ORGANIZED CRIME,” EUROPEAN COMMISSIONno. September, 2020.
16. Pursuant to The Local Authorities and Police and Crime Panels (Coronavirus) (Flexibility of Local Authority Police and Crime Panel Meetings) (England and Wales) Regulations 2020, the Norfolk Police and Crime Panel meeting on 2 February 2021 will be held using Microsoft Teams..
17. PwC, “Cyber Threats 2021: A Year in Retrospect,” pp. 1–74, 2022, [Online]. Available: https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf

18. M. G. Porcedda and D. S. Wall, “Cascade and Chain Effects in Big Data Cybercrime: Lessons from the TalkTalk hack,” Proc. - 4th IEEE Eur. Symp. Secur. Priv. Work. EUROS PW 2019, no. August 2019, pp. 443–452, 2019, doi: 10.1109/EuroSPW.2019.00056.
19. B. L. Linkomies, S. Airey, and J. Thorne, “Collective actions build against,” PRIVACY LAWS & BUSINESS UNITED KINGDOM REPORT, no. 106, 2020.
20. A. A. Hall and C. S. Wright, “Data Security: a Review of Major Security Breaches Between 2014 and 2018,” Fed. Bus. Discip. J., vol. 6, no. December 2013, pp. 50–63, 2018.
21. T. Jančárková and G. Visky, International Conference on Cyber Conflict : Keep Moving. 2022.
22. N. O. N. Classifi, “The Cyber Threat to Operational Technology”, Communications Security Establishment, 2022.
23. Cyber Arms Watch An Analysis of Stated & Perceived Offensive Cyber Capabilities, no. May. 2022.
24. PwC, “Operational resilience: How to set and test impact tolerances,” no. February, 2020.
25. W. Nwankwo and K. C. Ukaoha, “Socio-technical perspectives on cybersecurity: Nigeria’s cybercrime legislation in review,” Int. J. Sci. Technol. Res., vol. 8, no. 10, pp. 47–58, 2019.
26. A. M. Kovács, “Here there be Dragons: Evolution, Potentials and Mitigation Opportunities of Cybercrime in Nigeria A Review, Analysis, and Evaluation,” J. Cent. East. Eur. African Stud., pp. 0–1, 2021.
27. M. R. Mphatheni and W. Maluleke, “Cybersecurity as a response to combating cybercrime,” Int. J. Res. Bus. Soc. Sci. (2147-4478), vol. 11, no. 4, pp. 384–396, 2022, doi: 10.20525/ijrbs.v11i4.1714.
28. L. O. Nweke and S. D. Wolthusen, “A review of asset-centric threat modelling approaches,” Int. J. Adv. Comput. Sci. Appl., no. 2, pp. 1–6, 2020, doi: 10.14569/ijacsa.2020.0110201.
29. L. O. Nweke, “Using the CIA and AAA Models to Explain Cybersecurity Activities,” PM World J., vol. VI, no. Xii, pp. 1–3, 2017, [Online]. Available: https://pmworldlibrary.net/wp-content/uploads/2017/05/171126-Nweke-Using-CIA-and-AAA-Models-to-explain-Cybersecurity.pdf
30. D. D. Data, “A MODEL TO INVESTIGATE THE SECURITY CHALLENGES AND VULNERABILITIES OF CLOUD COMPUTING SERVICES IN,” J. Univ. Shanghai Sci. Technol., vol. 24, no. 5, pp. 105–121, 2022.
31. P. P, D. R. S. Mohana, and D. S. Kalaiselvi, “Enhancing the Cyber Security Intrusion Detection based on Generative Adversarial Network,” Ilkogr. Online - Elem. Educ. Online, vol. 20, no. 5, pp. 7401–7408, 2021, doi: 10.17051/ilkonline.2021.05.839.
32. F. Cremer et al., “Cyber risk and cybersecurity : a systematic review of data availability,” Geneva Pap. Risk Insur. - Issues Pract., vol. 47, no. 3, pp. 698–736, 2022, doi: 10.1057/s41288-022-00266-6.
33. D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, “A Survey of Deep Learning Methods for Cyber Security,” Information, 2019, doi: 10.3390/info10040122.
34. Ryan, Cooper, and Tauer, Computer Forensics Investigating Network Intrusions & Cyber Crime. 2013.
35. A. Rahman et al., “DistB-SDoIndustry : Enhancing Security in Industry 4 . 0 Services based on Distributed Blockchain through Software Defined Networking-IoT Enabled Architecture,” Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 9, pp. 674–681, 2020.
36. Pedreira, Vítor & Barros, Daniel & Pinto, Pedro. "A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0" with New Challenges on Data Sovereignty Ahead. Sensors. 21. 5189. 10.3390/s21155189. 2015.
37. Moustafa, Nour & Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set". 1-14. 10.1080/19393555.2015.1125974, 2014.
38. F. U. Xiao, L. Sha, Z. Yuan, and R. Wang, “VulHunter : A Discovery for unknown Bugs based on Analysis for known patches in Industry Internet of Things,” IEEE Trans. Emerg. Top. Comput. VulHunter, vol. 6750, no. c, 2017, doi: 10.1109/TETC.2017.2754103.
39. S. Chain, S. Mumtaz, M. A. Violas, A. M. D. E. O. Duarte, and J. Rodriguez, “Man-In-The-Middle Attacks in Industry,” IEEE Access, vol. PP, no. c, p. 1, 2019, doi: 10.1109/ACCESS.2019.2914454.
40. J. Vrchota, “applied sciences Readiness of Enterprises in Czech Republic to,” Appiles Scince, 2019.
41. A. A. Sü, “A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4 . 0 Ecosystem,” I. J. Comput. Netw. Inf. Secur., no. February, pp. 1–12, 2020, doi: 10.5815/ijcnis.2020.01.01.
42. L. Barreto, A. Amaral, A. Santana, P. Afonso, A. Zanin, and R. Wernke, “ScienceDirect ScienceDirect ScienceDirect ScienceDirect Network and information security challenges within Industry Costing models for T . capacity Pereira optimization and operational efficiency Escola Superior between Network and information security ch,” Procedia Manuf., vol. 13, pp. 1253–1260, 2017, doi: 10.1016/j.promfg.2017.09.047.
43. S. B. Elmamy, H. Mrabet, H. Gharbi, and A. Jemai, “A Survey on the Usage of Blockchain Technology for Cyber-Threats in the Context of Industry 4 . 0,” Sustainability, pp. 1–19, 2010.

44. C. Hsion, S. Lim, B. Shen, W. Pei, Q. Ng, and S. Lin, "A review of industry 4 . 0 revolution potential in a sustainable and renewable palm oil industry : HAZOP approach," Renew. Sustain. Energy Rev., vol. 135, no. August 2020, p. 110223, 2021, doi: 10.1016/j.rser.2020.110223.
45. R. T. Macedo, A. Santos, M. Nogueira, N. Prates, and A. Verg, "A Defense Mechanism for Timing-based Side-Channel Attacks on IoT Traffic," 2020.
46. J. Hu and S. Member, "A New Threat Intelligence Scheme for Safeguarding Industry 4 . 0 Systems," IEEE Access, vol. 4, no. c, pp. 1–15, 2018, doi: 10.1109/ACCESS.2018.2844794.
47. L. Sha, F. Xiao, W. Chen, and J. Sun, "IIoT-SIDefender : Detecting and defense against the sensitive information leakage in industry IoT," World Wide Web, 2017, doi: 10.1007/s11280-017-0459-8.
48. Pedreira, V.; Barros, D.; Pinto, P. A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead. Sensors 2021, 21, 5189. https://doi.org/10.3390/s21155189.
49. J. Bhamub, P. Stief, J. Dantan, A. Etienne, and A. Siadat, "Science Science Direct Direct ScienceDirect Analysis Barriers to adoption in Manufacturing Analysis of Barriers to Industry Industry Organizations : Organizations : an an ISM ISM Approach Approach A new methodology to analyze the functional and physical a," ELSEVIER, pp. 1–6, 2021, doi: 10.1016/j.procir.2021.01.010.
50. J. S. Najeem and P. Krishnan, "Advanced Defence Mechanisms for Future Network Security using SDN," Int. J. Recent Technol. Eng., vol. 3878, no. 6, pp. 686–690, 2019.
51. S. N. Michael Sony, "Key ingredients for evaluating Industry 4.0 readiness for organizations: a literature review," Benchmarking An Int. J., 2019.
52. M. S. Akhtar and T. Feng, "Malware Analysis and Detection Using Machine Learning Algorithms," Symmetry (Basel)., vol. 14, no. 11, 2022, doi: 10.3390/sym14112304.
53. A. Shaheed and M. H. D. B. Kurdy, "Web Application Firewall Using Machine Learning and Features Engineering," Secur. Commun. Networks, vol. 2022, 2022, doi: 10.1155/2022/5280158.
54. T. Thangamani, R. Prabha, M. Prasad, U. Kumari, R. KV, and S. Abidin, "WITHDRAWN: IoT Defense Machine Learning: Emerging Solutions and Future Problems," Microprocess. Microsyst., no. February, p. 104043, 2021, doi: 10.1016/j.micpro.2021.104043.
55. P. V. Kallapur and V. Geetha, "Web security: A survey of latest trends in security attacks," Lecture Notes in Electrical Engineering, vol. 121 LNEE. pp. 405–415, 2011. doi: 10.1007/978-3-642-25541-0_52.
56. C. Bansal, K. Bhargavan, and S. Maffeis, "Discovering concrete attacks on website authorization by formal analysis," Proceedings of the Computer Security Foundations Workshop. pp. 247–262, 2014. doi: 10.1109/CSF.2012.27.
57. D. Kaur and P. Kaur, "Empirical Analysis of Web Attacks," Physics Procedia, vol. 78. pp. 298–306, 2016. doi: 10.1016/j.procs.2016.02.057.
58. D. Mitropoulos, P. Louridas, M. Polychronakis, and and A. D. Keromytis, "Defending Against Web Application Attacks: Approaches, Challenges and Implications," , IEEE Trans. Dependable Secur. Comput. MITROPOULOS, pp. 1545–5971, 2017.
59. F. Kong, "Research on Security Technology based on WEB Application." pp. 367–370, 2017. doi: 10.5220/0006450603670370.
60. D. Stiawan, M. Y. Idris, A. H. Abdullah, F. Aljaber, and R. Budiarto, "Cyber-attack penetration test and vulnerability analysis," Int. J. Online Eng., vol. 13, no. 1, pp. 125–132, 2017, doi: 10.3991/ijoe.v13i01.6407.
61. M. Alsharif, S. Mishra, and and M. AlShehri, "Impact of Human Vulnerabilities on Cybersecurity," Comput. Syst. Sci. Eng., 2021.
62. D. M. Sharma and D. S. N. Jain, "Cyber Security Attacks, Threats, and Vulnerabilities," Int. J. Creat. Res. Thoughts, vol. 10, no. 5, 2022.

EDUSJ, Vol, 32, No: 2, 2023 (114-127)

اختراقات الويب والدفاعات: ورقة مراجعة

عمار عادل احمد، نجلاء بديع الدباغ

قسم علوم الحاسوب، كلية علوم الحسابات والرياضيات، جامعة الموصل، الموصل، العراق

الخلاصة

نظرًا لمحدودية البيانات التي تجمعها تطبيقات الويب من المستخدمين ، فإنها تخضع لمخاطر أمن المعلومات. الطريقة الأكثر فعالية للاحتفاظ بالبيانات في العصر الحديث هي من خلال التطبيقات عبر الإنترنت. تُعرف عملية توفير البيانات وأنظمة البيانات بضمانات أمنية إجرائية ومتطورة مناسبة بالأمن السيبراني. تتزايد التهديدات للأمن السيبراني في بعض الأحيان. يُعرف الخلل أو الضعف في نظام الكمبيوتر ، أو التكتيكات الأمنية ، أو الضوابط الداخلية ، أو التخطيط ، أو التنفيذ الذي يمكن أن يضر بالسياسة الأمنية لإطار عمل بالثغرة الأمنية على شبكة الإنترنت. يمكن أن تتعطل المجالات الاجتماعية والاقتصادية والسياسية للحكومات بسبب ضعف الإنترنت ، مما قد يكون له تأثير على الدولة. يتم بذل جهد للتعرف على العيوب ونقاط الضعف أثناء دراسة الضعف من أجل الاستفادة من نقاط الضعف هذه. الهدف من هذه المراجعة هو فهم طبيعة ونطاق الهجمات التي تستهدف تطبيقات وخدمات الويب. من خلال تحليل هجمات الويب ، بالإضافة إلى تحديد أنماط الهجوم ، يمكن أن يساعد تحليل هجمات الويب أيضًا في تحديد السبب الجذري للثغرات الأمنية التي يستغلها المهاجمون. من خلال فهم طبيعة هجمات الويب ونقاط الضعف التي يتم استغلالها بشكل شائع ، من الممكن تطوير دفاعات وإجراءات مضادة أكثر فعالية. بشكل عام ، يتمثل الهدف الشامل لهذه المراجعة في تحسين أمان الويب من خلال تحديد نقاط الضعف والتهديدات والتخفيف من حدتها.