International Journal of Engineering Trends and Applications (IJETA) – Volume 12 Issue 4, Jul-Aug 2025

RESEARCH ARTICLE OPEN ACCESS

The State Of Web Security: An Overview Of Risks And Countermeasures

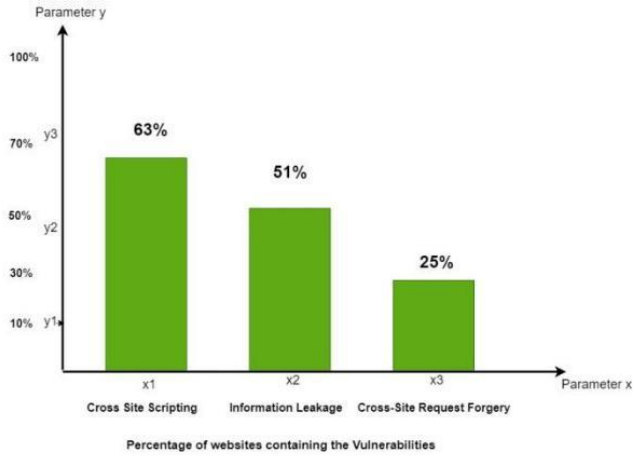
Rajpreet Kaur
*Department of Computer Science & Engineering, Global Institute of Technology, Jaipur, Rajasthan, India

Abstract:
With the volume and sophistication of cyber-attacks increasing all the time, swift efforts are needed to protect sensitive corporate and personal information, as well as national security. Thus need of cyber security has drastically increased because of the huge reliance on wireless networks and internet.
For a long time, Web Security has been one of the hottest study fields, whether it's from the standpoint of analysis or detection, and then implementing mitigation methods. Web security risks have changed significantly since their original debut, and they are becoming more sophisticated by the day. The evolution could be in the form of new attack methods or resistance to the use of simulated OS or VM environments. In addition, the aim of assaults has shifted significantly in recent years. Clients were previously disregarded while selecting targets.
Web security has become a crucial worry for both businesses and individuals due to the internet's explosive growth. The prevalence and sophistication of security vulnerabilities have increased with the use of web-based technologies. The purpose of this article is to present an overview of the main web security risks and the available mitigation strategies. We start off by outlining the typical categories of web application assaults, like injection attacks, cross-site scripting, and session hijacking. The significance of secure coding techniques, such as input validation, error management, and access control, is then covered.

Keywords: Cyber-Attacks, Web Security, Cross-Site Scripting.

1. INTRODUCTION

In modern world, the Internet is the swift-growing structure. Numerous new technologies are transubstantiating the face of humanity in today's technological terrain. Still, because of these new technologies, we're unfit to cover our particular information as effectively as we'd like, and as a result, cybercrime is on the rise. As a result, cyber security has come as a hot content. Web security is a pivotal point of every web operation. At present, cyber security is a major solicitude in the online world. It's regarded as the primary frame for the global data society. Through a web runner, web operations give a better interface for a customer. The customer's web cyber surfer executes the web runner script. The thing of website security is to keep these (and other) pitfalls at bay. The act/ practice of securing websites from unauthorized access, use, revision, destruction, or dislocation is the more formal description of website security. Effective website security necessitates design sweats across the board, including in your web operation, web garcon setup, word creation and renewal processes, and customer- side law. Cross-site scripting, cookie- session robbery, cyber surfer attack, and tone- propagating worms in web emails and websites all appear from web apps. These attacks are known as' injection attacks,' and they include the use of vicious law. For the better part of the previous decade, injection attacks are ranked at the top of web operation vulnerability rankings. SQL injection and cross-site scripting are the two most common security excrescencies in the modern world. According to a security assessment of the operation defence centre, which included over 250 e-commerce operations, online banking, and commercial websites, more than 85% of web operations are vulnerable to attacks.



2. NEED OF WEB SECURITY

The practice of defending websites, web apps, and web-based services against online dangers like hacking, data breaches, viruses, malware, phishing attacks, and other cyber-attacks is known as web security. A variety of technologies, techniques, and best practices are used in web security to protect web assets and stop unauthorized access to confidential data.

Every website requires security for four main reasons:

- Protects confidential information: Web security tools like encryption, firewalls, and secure authentication mechanisms assist in preventing unauthorized access to sensitive information like personal and financial data.
- Prevents cyber attacks: Malware, phishing, and hacking are a few examples of the increasingly sophisticated and common cyber attacks that pose a serious danger to both individuals and businesses. Antivirus software and intrusion detection systems are two web security tools that help avoid these attacks and lessen their effects.
- Maintains company image: A security breach can seriously harm a company's reputation, which could lead to a loss of clients and income. Maintaining the trust of stakeholders and customers is made easier by putting effective web security steps in place.
- Regulation compliance: To protect sensitive data, businesses are required to implement specific security measures under the rules and standards that apply to many sectors. Legal repercussions, fines, and reputational harm may come from failure to adhere to these regulations.
- Maintaining business reputation: Web security works to maintain the availability and functionality of websites and web apps, ensuring the continuity of business operations.
- Reducing legal liabilities: By preventing data breaches, unauthorized access, and other security events that may give rise to lawsuits, fines, or other legal repercussions, web security helps reduce legal liabilities.

3. CAUSES AND CONSEQUENCES OF WEB SECURITY

Web security is crucial for preventing unauthorized access, theft, and misuse of private and personal data. Web security problems can have a variety of reasons, but some typical ones are as follows:

- Software flaws: Hackers may use coding errors, bugs, or other software flaws in web apps, servers, or other software to obtain unauthorized access.
- Weak passwords: Passwords that are simple to guess or that are used on several different accounts can be quickly cracked, giving hackers quick access to user accounts.
- Malware and viruses: Malware and viruses can infect systems and carry out malicious tasks such as installing backdoors, stealing data, and more.
- Social engineering: To trick users into allowing them access to their accounts or data, hackers may use social engineering techniques. To steal login information, they

might, for instance, send phishing emails or build fake websites that mimic real ones.

- Absence of encryption: Sensitive data must be encrypted while in route. Data can be readily intercepted and stolen if it is not encrypted.
- Software that has reached its expiration date: Outdated software may contain security flaws that have not yet been fixed, making them vulnerable to exploitation.
- Third-party integrations: If they are improperly protected or contain vulnerabilities, third-party integrations can pose a security risk.

Web security problems can have serious repercussions for both people and businesses. Consequences include, among others:

- Data breaches: When private information is taken or disclosed, it can have serious negative effects on people and businesses, including financial loss, injury to their reputations, and legal repercussions.
- Identity theft: Hackers are able to steal identities and commit fraud using stolen personal information, which can have severe repercussions for victims.
- Loss of confidence: A security breach can reduce users' trust in a company, which can result in lost sales and reputational harm for the latter.
- Financial penalties: Organizations must protect user data under data protection laws that apply to many sectors. If a company doesn't follow these rules, there could be heavy fees and other consequences.

4. WEB SECURITY THREATS

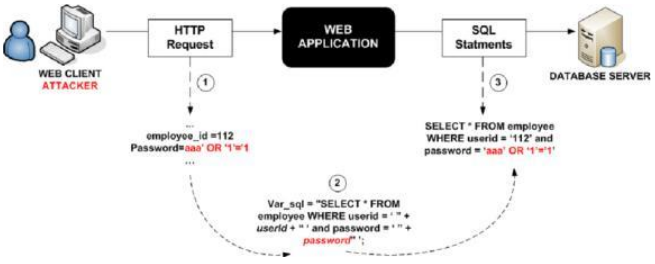
Any malicious actions or assaults targeted at compromising the confidentiality, integrity, or accessibility of websites, web applications, and web-based services are considered web security threats. These dangers can come in many different shapes and come from a variety of people, including insiders, state-sponsored players, hackvists, and cybercriminals.

Threats to web security may aim to steal confidential information, seize control of websites or servers, interrupt services, spread malware or viruses, or carry out unauthorized deeds. Malware, phishing attacks, cross-site scripting (XSS) attacks, SQL injection attacks, denial of service (DoS) attacks, and man-in-the-middle (MitM) attacks are a few examples of common online security threats.

A. SQL Injection Attack

A type of web security flaw known as SQL injection (SQLi) enables attackers to insert malicious SQL code into the database of a web service. This kind of attack is especially risky because it frequently doesn't require any authentication and can let attacker access private data or change data already present in the database.

When a web application does not correctly sanitize user input, SQL injection attacks frequently happen. An attacker could enter malicious SQL code that the database server could execute if a web application takes user input for a search box or a login form without validating or escaping special characters. By doing this, the attacker may be able to steal private information like usernames, passwords, credit card numbers, or other personal data.



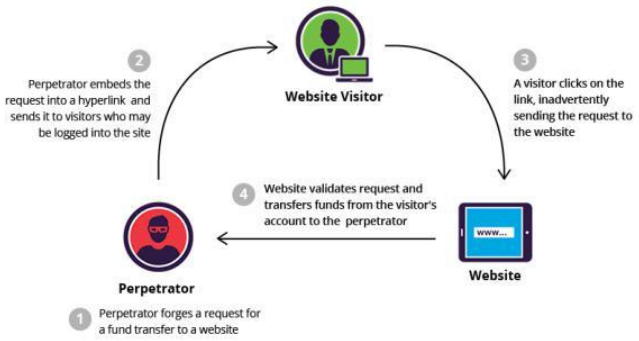
B. Cross-Site Rquest Forgery Attack (CSRF)

A form of web security flaw known as cross-site request forgery (CSRF) enables an attacker to carry out unauthorized actions on behalf of an authenticated user. In a CSRF attack, the attacker

uses the target's current session and authentication credentials to trick the victim into unintentionally sending a malicious request to a vulnerable web service.

As an illustration, consider a scenario in which a user is signed in to a web application when they click on a link to a malicious website that has a hidden form that sends a request to the vulnerable web application. The request will

be carried out if the user is currently logged in to the vulnerable web application, enabling the attacker to take unapproved actions on the user's behalf like changing their password, buying something, etc.

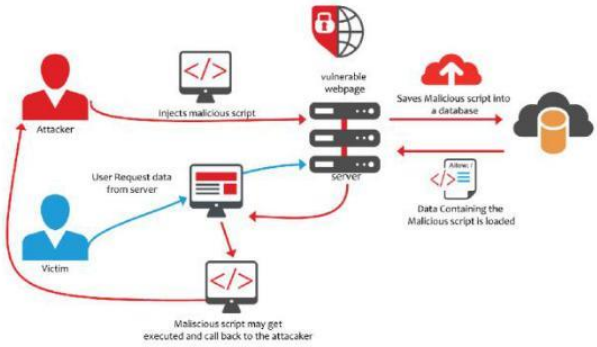


C. Cross-Site Scripting

A form of web security flaw called cross-site scripting (XSS) enables attackers to insert malicious scripts into a web page that is being viewed by other users. An XSS attack involves the injection of malicious code into a weak web application, which is then executed by users who watch the web page without thinking.

XSS assaults can be classified as either stored or reflected. When a user sees the impacted page, the malicious code from the stored XSS attack is executed on the web server. Through a weak input area, such as a search bar or a comment form, the malicious code is reflected back to the user in a reflected XSS attack.

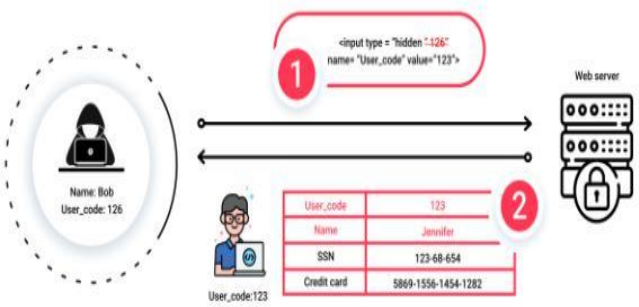
In addition to stealing private data like login credentials or credit card numbers, XSS attacks can also hijack user sessions, deface websites, spread malware, or engage in phishing attacks.



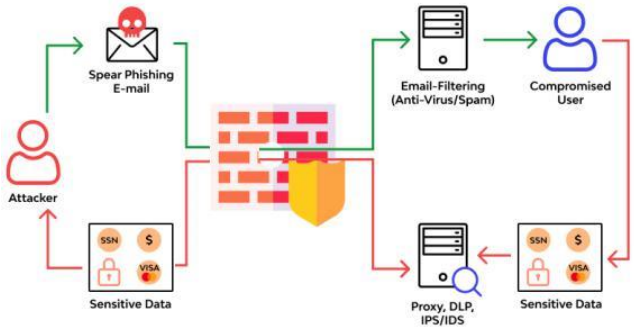
D. Broken Authentication

When an application's authentication method is incorrectly implemented or configured, it creates a type of web security vulnerability known as broken authentication. This vulnerability enables attackers to compromise authentication, bypass it, and access confidential information or functionality without authorization. Weak or readily guessable passwords, insufficient password complexity requirements, a lack of password expiration policies, session fixation, session hijacking, and other authentication-related issues are examples of broken authentication vulnerabilities.

Unauthorized access to confidential information, identity theft, data theft, and other security breaches are just a few of the negative effects of broken authentication vulnerabilities.



Attackers can take advantage of vulnerabilities that allow sensitive data exposure to pilfer sensitive information, which can then be used for a variety of nefarious activities like identity theft, financial fraud, or data breaches.

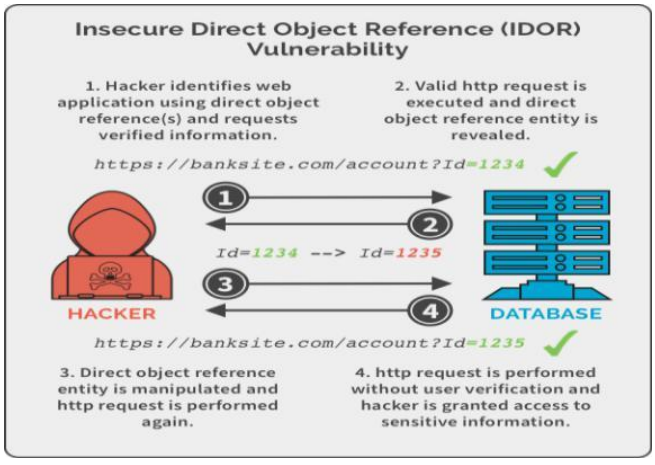


E. Insecure Direct Object References

Insecure Direct Object Reference (IDOR) is a type of web security vulnerability that occurs when an application exposes a reference to an internal implementation object, such as a file, database record, or resource, without proper authorization and validation checks.

Insecure Direct Object References vulnerability occurs when an attacker can manipulate these references, either by modifying parameters in the URL or by intercepting and modifying HTTP requests, to gain access to sensitive data or resources that they are not authorized to access.

For example, consider an e-commerce website that displays a list of orders by order number. If the website uses the order number directly as a reference to retrieve the order details, an attacker could easily modify the order number in the URL to view the details of other orders that they are not authorized to view.



F. Sensitive Data Exposure

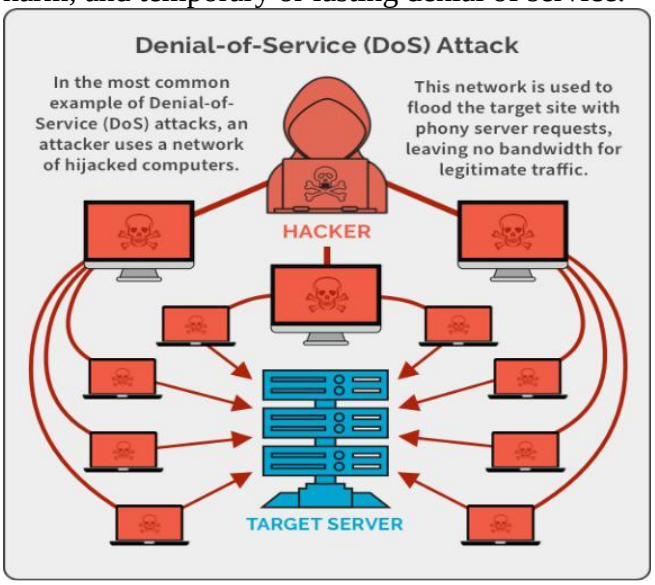
An application's failure to safeguard confidential data, such as passwords, credit card numbers, or personal information, from unauthorized access or disclosure results in sensitive data exposure, a type of web security vulnerability. Vulnerabilities for sensitive data exposure can occur for a number of reasons, including bad encryption techniques, unsafe data transfer or storage, a lack of access controls, or open communication channels.

G. Denial of Service (DoS) Attack

A type of web security attack known as a denial of service (DoS) attempts to stop a website or web application from being accessible by flooding it with traffic or requests.

DoS attacks can take many different shapes, such as network-based ones that overload the target server with data or application-based ones that use application flaws to crash servers or drain system resources.

A successful DoS assault can have serious repercussions, such as data loss, reputational harm, and temporary or lasting denial of service.



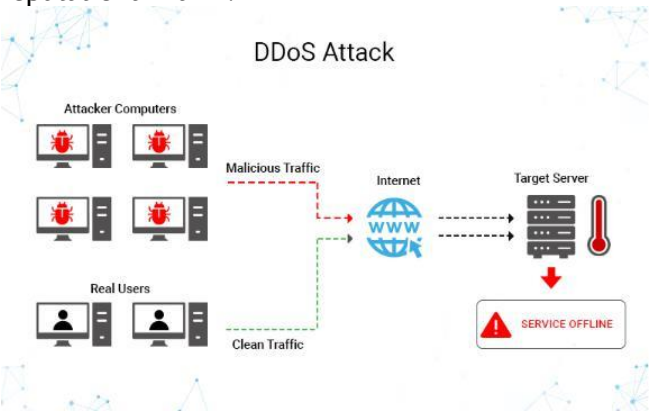
H. Distributed Denial of Service (DDoS) Attack

Similar to a DoS attack, a distributed denial of service (DDoS) attack includes a number of compromised systems, or "zombies," that are coordinated to flood a target server or network with traffic or requests.

The attacker uses the compromised systems, which are frequently part of a botnet, to create a flood of traffic or requests that overload the target server or network, rendering it unresponsive or crashing.

DDoS assaults can originate from a variety of places, such as infected computers, compromised IoT devices, and cloud-based resources. They can take many different shapes, such as UDP flood, ICMP flood, SYN flood, and HTTP flood.

A successful DDoS assault can have serious repercussions, such as temporary or permanent service interruptions, financial losses, and reputational harm.



I. Malware

Any software programme created with the malicious intent to damage a computer system or steal confidential data is referred to as malware, short for malicious software. Malware can come in a variety of shapes and sizes, including viruses, worms, Trojan horses, malware, spyware, adware, and other harmful software applications. Typical forms of viruses include:

- Virus: A computer programme called a virus has the ability to replicate itself and spread from one machine to another. Usually, it joins a trustworthy file and disseminates when the infected file is viewed or executed.
- Worm: A worm is a self-replicating programme that distributes uninhibitedly throughout computers and networks. Worms can cause extensive harm and are built to eat up system resources.
- Trojan: A Trojan is a form of malware that poses as a trustworthy programme but, once loaded, is capable of doing harm to the system or stealing data.
- Ransom ware encrypts files on the victim's machine and demands money in return for the decryption key.
- Spyware: A form of malware, spyware is intended to steal confidential data and covertly monitor the victim's activities.
- Adware: A form of malware known as adware causes unwanted advertisements to appear on the victim's device.

J. Defacement

Unauthorized alterations to a website or online page are known as defacement. It typically entails altering the website's visual design or adding new content, frequently in an effort to discredit the website's owner or organization or to disseminate a political or ideological message.

Defacement can be carried out by taking advantage of flaws in content management systems or web sites, or by using stolen login information. After a website has been defaced, the attackers may add new offensive or bad-mouthing content or substitute the original content with their own messages or images.

The owner of the defaced website may suffer severe repercussions, including diminished sales, reputational harm, and legal liabilities. Users of the website may also be impacted by being exposed to malware or other security hazards.

5. METHODS AND TECHNOLOGIES FOR WEB SECURITY

For web security, a variety of techniques and technologies are used to guard against different threats and vulnerabilities. Typical techniques and tools include:

- Authentication is the procedure of confirming a user's or system's identity. It is a crucial step in online security and can be carried out using a variety of tools, including passwords, biometrics, and multi-factor authentication.
- Encryption: Encryption is a method for encrypting data so that only authorized individuals can decipher it. Both data at rest and data in motion are protected by encryption.
- Firewalls: Network security tools called firewalls watch and regulate both incoming and outgoing network traffic. They are employed to stop unauthorized entry to a network and can be hardware- or software-based.
- Systems for detecting and preventing intrusions (IDPS): An IDPS system scans network data for indications of an attack. By blocking attacks or warning admins, it can identify and stop them.
- Transport Layer Security (TLS) and Secure Sockets Layer (SSL): A protocol called SSL/TLS is used to secure data as it travels between a client and a server. It is frequently employed for safe online conversation.
- Vulnerability Scanning: A technique for locating possible vulnerabilities in a system or application is vulnerability scanning. It is carried out using automated tools that search for recognized flaws and notify the administrator of them.
- Web Application Firewalls: Firewalls that are particularly designed to protect web applications are known as web application firewalls. They can stop attacks like SQL injection and cross-site scripting by keeping an eye on both incoming and outgoing data.

6. BEST PRACTICES FOR WEB SECURITY

For your website and its users' safety and privacy, you must protect against online security threats. Here are some practical precautions you can take to safeguard against threats to online security:

- Update software: To patch known vulnerabilities that attackers can use, keep your website's software, plugins, and other apps up to date.
- Use secure protocols: To prevent hackers from intercepting and stealing confidential information, use secure protocols like HTTPS to encrypt all data sent between your website and its users.
- Use firewalls to prevent unauthorised access to your website and regulate the volume of data that can reach it.
- Use secure passwords: Make sure that all user profiles on your website have secure passwords, and advise visitors to create a different password for each website they visit.
- Use Anti-Malware Software: Anti-malware software should be used to frequently scan your website for malware and eliminate any infections that are discovered.
- Educate Users: Users should be made aware of the value of online security, and

you should give them advice on how to avoid falling for common threats like phishing.

- Maintain regular backups: Maintain regular backups of the data on your website to ensure that you can recoup from any potential security incidents.
- Test for vulnerabilities: Conduct frequent penetration tests and vulnerability assessments to find and fix any security flaws in your website.
- Implement access controls: Implement access controls to make sure that only authorized users can access confidential information and features on your website.
- Using Content Delivery Network (CDN): Use a content delivery network (CDN) to distribute the content of your website across several servers and lessen the likelihood of DDoS attacks.

We can lessen the risk of web security threats by taking the measures outlined here to help ensure the safety and privacy of your website and its users.

7. LEGAL AND ETHICAL CONSIDERATIONS

Web security is not just a technological issue; there are also moral and legal considerations that must be made. Some of the ethical and legal issues surrounding web security are listed below:

- Regulations: Websites collecting and storing sensitive data, such as financial or personal information, must abide by rules like the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR).
- Privacy protection for users: Websites must make sure that users' privacy is respected and that no personal information is sold or shared without the user's permission.
- Ethical data handling: Websites must make sure that the data they gather is handled ethically and that it isn't put to use for things for which the user hasn't given their consent.
- Responsibility for Data Breaches: Websites must assume responsibility for data breaches and take action to lessen its effects on users in the event that one occurs.
- Ethical Hacking: Penetration testing, commonly referred to as ethical hacking, is the process of finding flaws in a system or application. Websites must make sure that ethical hacking is done with users' permission and that the proprietors of the website are informed of the results.
- Accountability: Websites must be responsible for the security of their systems and applications and take the necessary precautions to avoid security breaches.

8. CONCLUSION

In conclusion, maintaining the privacy and security of sensitive data and systems requires strong online security. Web security problems can be caused by a number of things, including third-party integrations, malware, viruses, weak passwords, obsolete software, and web application vulnerabilities. Numerous techniques and technologies, including as authentication, encryption, firewalls, IDPS, SSL/TLS, vulnerability scanning, and web application firewalls, are used to counteract these threats and weaknesses.

Web security, however, is not just a technical issue; there are also moral and legal implications. Regulations must be followed, user privacy must be protected, data must be handled ethically, data breaches must be addressed, ethical hacking must be done with user consent, and websites must be responsible for the security of their systems and apps.

To maintain the safety and privacy of sensitive data and systems, it is crucial to keep up with the most recent security trends and technologies. In general, web security is a field that is always growing. It is crucial to take proactive steps to limit these risks and defend against possible

security breaches as new security threats and vulnerabilities may arise as technology develops.

REFERENCES

[1] Anderson, R., & Moore, T. (2009). The economics of information security. Science, 314(5799), 610-613.

[2] Bhunia, S., & Ray, S. (2017). Web security: A survey of approaches and trends. ACM Computing Surveys (CSUR), 50(3), 1-45.

[3] Cert.org. (2021). Common web application vulnerabilities. Retrieved from https://www.cert.org/secure-coding/tools/common-web-application-vulnerabilities.cfm

[4] Doupé, A., Kirda, E., Kruegel, C., & Vigna, G. (2010). A look back at "Know your enemy: Web application threats". IEEE Security & Privacy, 8(5), 60-65.

[6] OWASP. (2021). Top 10 web application security risks. Retrieved from https://owasp.org/Top10/

[7] Tajpour Atefeh, Maslin Masrom, Mohammad Zaman Heydari and Suhaimi Ibrahim, "SQL injection detection and prevention tools assessment", Computer Science andInformation Technology (ICCSIT) 2010 3rd IEEE International Conference, vol. 9, pp. 518-522, 2010.

[8] S. Ali, S.K. Shahzad and H. Javed, "SQLIPA: An Authentication Mechanism Against SQL Injection", European Journal of Scientific Research, vol. 38, no. 4, pp. 604-611, 2009.

[9] Stallings, W. (2017). Cryptography and network security: Principles and practice. Pearson.

[10] The Open Web Application Security Project (OWASP). (2021). Home page. Retrieved from https://owasp.org/

[11] Shostack, A. (2014). Threat modeling: designing for security. John Wiley & Sons.

[12] Zhang, Z., & Wang, X. (2016). A survey on web application security testing. International Journal of Security and Its Applications, 10(4), 33-44.

[13] Zittrain, J. (2008). The future of the internet--and how to stop it. Yale University Press.

[14] L. S. Shar, H. B. K. Tan and L. C. Briand, "Mining SQL injection and cross site scripting vulnerabilities using hybrid program analysis", Proc. of Int. Conf. on Software Engineering (ICSE '13), pp. 642-651, 2013.

[15] Y. Li, Z. Wang and T. Guo, "Reflected XSS Vulnerability Analysis", International Research Journal of Computer Science and Information Systems (IRJCSIS), vol. 2, pp. 25-33, 2013.

[16] H. Kaushik, H. Arora, R. Joshi, K. Sharma, M. Mehra and P. K. Sharma, "Digital Image Security using Hybrid Model of Steganography and Cryptography," 2025 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2025, pp. 1009-1012,

[17] L. K. Shar and H. B. K. Tan, "Automated removal of cross site scripting vulnerabilities in web applications", Inf. Softw. Technol., vol. 54, pp. 467-478, 2012.

[18] Yang Haixia and Nan Zhihong, "A Database Security Testing Scheme Of Web Application", 4th International Conference On Computer Science And Education, pp. 953-955, 2009.

[19] V. Prokhorenko, K. -K. R. Choo and H. Ashman, "Web application protection techniques: a taxonomy", Journal of Network and Computer Applications, vol. 60, pp. 95-112, 2016.

[20] Soni, G.K., Arora, H., Jain, B. (2020). A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm. International Conference on Artificial Intelligence: Advances and Applications 2019. Algorithms for Intelligent Systems. Springer, Singapore.

[21] K. Elshazly, Y. Fouad, M. Saleh and A. Sewisy, "A survey of SQL injection attack detection and prevention", Journal of Computer and Communications, vol. 2, no. 8, pp. 1-9, 2014.

[22] H. Arora, G. K. Soni, R. K. Kushwaha and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," 2021 6th International Conference on Communication and Electronics Systems (ICCES), 2021, pp. 1153-1157,

[23] S. A. Saiyed, N. Sharma, H. Kaushik, P. Jain, G. K. Soni and R. Joshi, "Transforming portfolio management with AI and ML: shaping investor perceptions and the future of the Indian investment sector," Parul University International Conference on Engineering and Technology 2025 (PiCET 2025), Hybrid Conference, 2025, pp. 1108-1114.

[24] A. Agarwal, R. Joshi, H. Arora and R. Kaushik, "Privacy and Security of Healthcare Data in Cloud based on the Blockchain Technology," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), 2023, pp. 87-92.

[25] P. Upadhyay, K. K. Sharma, R. Dwivedi and P. Jha, "A Statistical Machine Learning Approach to Optimize Workload in Cloud Data Centre," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), 2023, pp. 276-280.

[26] P. Jha, R. Baranwal, Monika and N. K. Tiwari, "Protection of User's Data in IOT," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2022, pp. 1292-1297.

[27] P. Jha, M. Mathur, A. Purohit, A. Joshi, A. Johari and S. Mathur, "Enhancing Real Estate Market Predictions: A Machine Learning Approach to House Valuation," 2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), 2025, pp. 1930-1934.

[28] A. Maheshwari, R. Ajmera, and D. K. Dharamdasani, "Unmasking Embedded Text: A Deep Dive into Scene Image Analysis," in 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), 2023, pp. 1403–1408.