International Scientific Journal of Engineering and Management (ISJEM)
Volume: 04 Issue: 04 | April – 2025
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM02806

Overview of Web Security Attacks

Sucharith Biswas
Dept of Computer Science
JAIN UNIVERSITY
Banglore, India

Chaitanya
Dept of Computer Science
JAIN UNIVERSITY)
Banglore, India

K Bhuvan Sai
Dept of Computer Science
JAIN UNIVERSITY)
Bengaluru, India

Harsh Kumar
Dept of Computer Science
JAIN UNIVERSITY)
Bengaluru, India

Pothineni Nikhil Yadav
Dept of Computer Science
JAIN UNIVERSITY
Banglore, India

Samarth R Pande
Dept of Computer Science
JAIN UNIVERSITY
Banglore, India

Prof. Shine Joseph
Department of CSE,
Jain (Deemed to be University),
Bangalore, INDIA
shine.joseph@jainuniversity.ac.in

***Abstract*—In the modern era of internet-based communication and transactions, web security is a crucial concern. The risk of cyber attacks has increased along with the adoption of web-based applications. Unauthorised access to, modification of, or destruction of web-based resources are referred to as attacks in the context of online security. These assaults may result in data loss, service interruptions, or even monetary losses. SQL injection, cross-site scripting, cross-site request forgery, and session hijacking are among the most prevalent forms of web security assaults. Different security measures, including encryption, firewalls, and intrusion detection systems, have been developed to thwart such attacks. To stay one step ahead of attackers, these precautions must be updated frequently because they are not failsafe.It is essential to understand the different types of attacks and their mechanisms to develop effective security strategies to mitigate the risks of web-based attacks**

***Index Terms*—component, formatting, style, styling, insert**

I. Introduction

In the current era of advanced technology and digitalization, web security is a major topic of concern. The threat of cyber attacks has grown in importance with the internet's and its services' exponential growth. We now rely significantly on the internet for a variety of activities, including communication, entertainment, and online shopping. However, this dependence increases the likelihood that someone will misuse our private data.

Cyber attacks have advanced in sophistication over the past few years, harming both persons and organisations. Web-based assaults, which take advantage of flaws in web services and applications, are one of the most prevalent types of cyber attacks. These assaults have the potential to compromise user data, steal confidential information, and result in large financial losses.

Web security includes the procedures and tools employed to defend web services and applications against online threats. It involves a variety of safeguards, including as firewalls, access controls, vulnerability assessment, and encryption. In the current digital era, where the internet is a crucial tool for conducting business and interacting with others, it is imperative to ensure the security of web applications and services.

In this study paper, we will go more into the subject of attacks on web security, looking at the many web-based attack types, their potential effects, and preventative methods. We'll look at the most recent web security trends and innovations, including new threats and tools. Our ultimate objective is to offer knowledge and suggestions that can assist businesses and individuals in better defending themselves against web-based attacks and protecting their sensitive data. [9]

A. More About Attacks

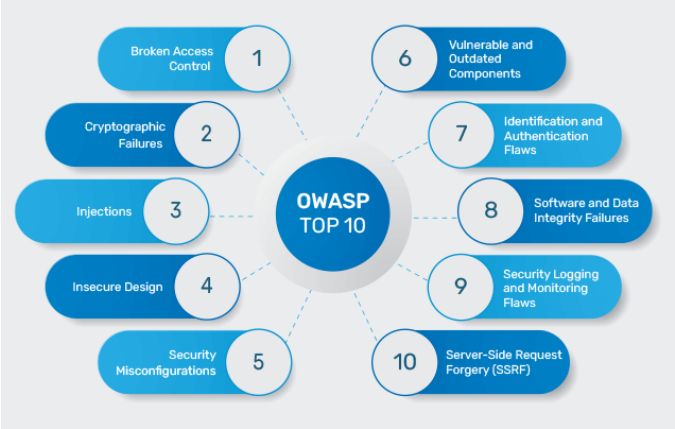

Fig. 1. Top Ten Attacks [9]

Understanding the various attack types, their techniques, and the best practices for preventing them is crucial for addressing these difficulties in an effective manner. The various attack types will be examined in this research study, along with the techniques attackers employ to take advantage of web vulnerabilities. It will also look at the most recent trends and methods employed by web security experts to reduce the dangers of web assaults and protect sensitive data.1

ISSN: 2583-6129
DOI: 10.55041/ISJEM02806

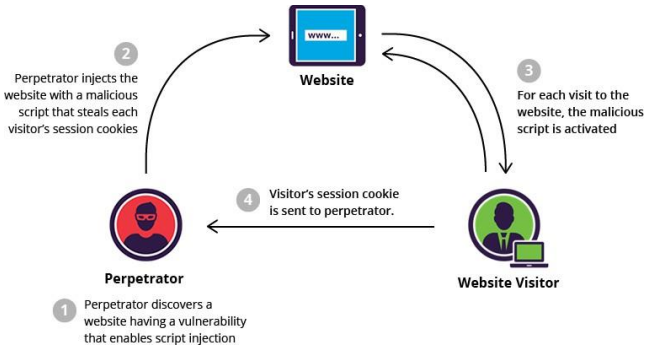

Fig. 2. SSRF [5]

- Cross-site Scripting(XSS)
- Injection 4
- Server Side Request Forgery(SSRF)
- Broken Access Control
- Denial Of Service(DOS)

and are just a few of the vulnerabilities that can still be exploited by attackers despite the many advancements in web security. These attacks may result in serious consequences, such as the loss of confidential data, service interruptions, and reputational harm to a company.

B. Working Of Attacks

Web attacks are malicious attempts by hackers to gain unauthorized access, steal data, or engage in other malicious activities by exploiting vulnerabilities in web applications or web servers. Cross-site scripting (XSS), SQL injection, cross-site request forgery (CSRF), and denial-of-service (DOS) attacks are all examples of web attacks. [1]

An XSS attack involves an attacker injecting malicious code into a web page, which is then executed by unsuspecting visitors. This gives the attacker the ability to steal sensitive data, such as login credentials, or take control of the user's browser.4

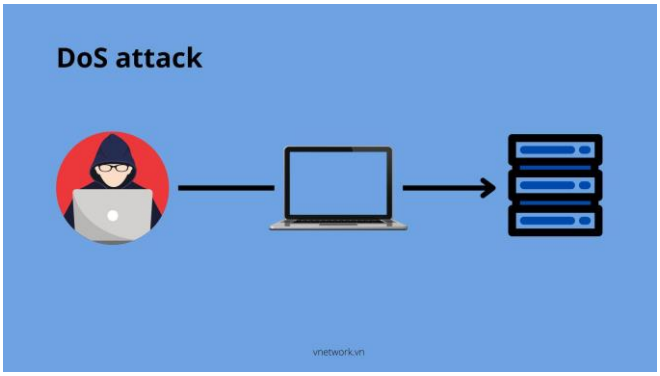

Fig. 3. Denial Of Service Attack [15]

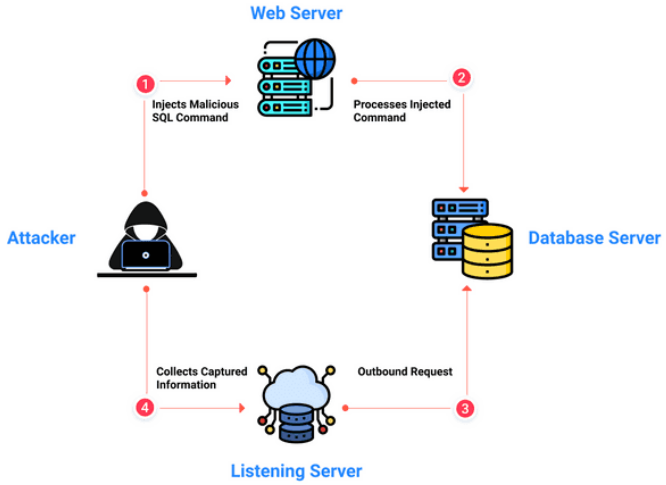

Fig. 4. Working Of SQL Injection [2]

An SQL injection attack4 involves an attacker exploiting vulnerabilities in the code of a web application to execute malicious SQL statements. This gives the attacker access to or modification of sensitive data stored in the application's database. [2]

An attacker uses an SSRF attack2 to trick a user into performing an action on a web application that they did not intend to perform. This gives the attacker the ability to perform unauthorized actions, such as changing the user's password or making unauthorized purchases. [5]

A DoS attack3 involves an attacker flooding a web server with traffic in order to overload it and prevent legitimate users from accessing it. This can cause the server to crash or become unavailable, causing users to lose service. [15]

Hackers typically use a variety of tools and techniques to carry out these attacks, including automated scripts and specialized software designed to exploit specific vulnerabilities. Web developers and administrators must take precautions to protect their applications and servers from these attacks, such as using secure coding practices, implementing access controls, and testing for vulnerabilities on a regular basis.

C. Impact Of Web Attacks

Web attacks can have a significant impact on a company, both financially and in terms of reputational damage. These attacks can take many forms, including DoS attacks, malware, phishing, SQL injection, cross-site scripting (XSS) attacks, and many others.

One of the most immediate consequences of a web attack is the disruption of business operations. If the attack is successful, it has the potential to disrupt critical systems and results in significant productivity loss.

International Scientific Journal of Engineering and Management (ISJEM)
Volume: 04 Issue: 04 | April – 2025
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata
ISSN: 2583-6129
DOI: 10.55041/ISJEM02806

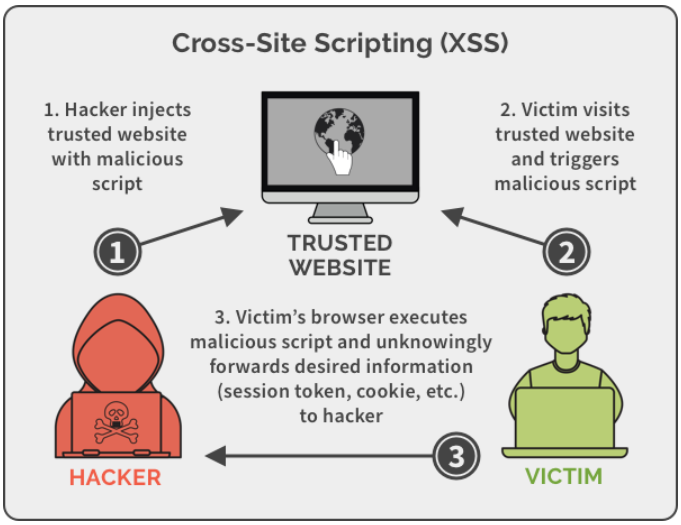

Fig. 5. Working Of XSS Attack [7]

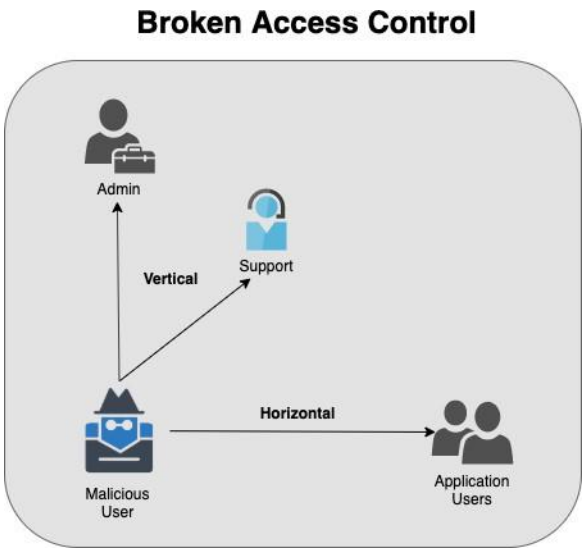

Fig. 6. Broken Access Control [10]

Financial loss is another significant impact of web attacks. Attackers may steal sensitive data such as customer information, trade secrets, or financial information. This can result in revenue loss as well as potential legal costs. A web attack can also have a negative impact on the company's reputation. If sensitive information is leaked or customer data is compromised, the company's reputation suffers and customer trust suffers. This can result in customer loss and difficulty attracting new ones. [3]

Furthermore, a web attack can result in legal and regulatory consequences, particularly if the company is found to be in violation of industry or government standards. Fines and other penalties may be imposed on the company, which can be financially devastating.

Web attacks can have a significant and far-reaching impact on a company. Companies must take precautions to protect their web-based systems and data from attacks by implementing appropriate security measures and staying up to date on the latest security trends and technologies.

Fig. 7. Phishing Attack [14]

D. Susceptible Towards Web Attacks

Web attacks have become a significant concern for both individuals and organizations in today's digital age. These attacks are intended to exploit vulnerabilities in web applications, networks, and servers in order to steal sensitive information or harm the target. One of the most serious issues with web attacks is that they can affect anyone who connects to the internet. Web attacks can affect anyone, whether they are individuals browsing the web on their personal computers or large corporations running a complex network of servers. [6]

Some examples of common web attacks are:

Phishing is a type of social engineering attack in which users are tricked into providing sensitive information, such as usernames and passwords, via bogus websites or emails.

Cross-site scripting (XSS) is a type of attack in which malicious code is injected into web pages in order to steal information or hijack user sessions.

SQL injection is a type of attack that steals data or gains unauthorized access by exploiting vulnerabilities in web application databases.

Proactive measures are required to protect against these and other types of web attacks. This includes updating your software, using strong passwords and multi-factor authentication, avoiding suspicious links and downloads, and learning about common attack techniques. By taking these precautions, you can reduce your vulnerability to web attacks and protect your sensitive information and online presence.

II. Literature Survey

Certainly, here are a few research papers related to web application security that you may find useful:

1) Xiaojun Xu, Yanjun Qi, Yingqi Liu, and Qinghua Zheng have proposed a novel method for creating adversarial examples that can evade detection by machine learning-based malware detectors. Developed in 2022, the method relies on genetic algorithms to generate adversarial examples with high detection scores. The authors suggest that this method can be used to create a more robust machine learning-based malware detection system, as it produces evasive examples that are difficult for machine learning-based malware detectors to detect. Additionally, the authors propose a novel approach for evaluating the efficacy of the proposed method, which involves testing the generated adversarial examples using a machine learning-based malware detector. Overall, the authors' proposed method provides a useful tool for creating more robust machine learning-based malware detection systems, as well as a novel approach for evaluating the efficacy of the proposed method. [4]

2) Yanick Fratantonio, Antonio Bianchi, Davide Balzarotti, and Engin Kirda's paper 'Ransomware in Smartphones: Attacks and Defenses' published in 2021, focuses on the growing threat of ransomware attacks against smartphones. This paper looks at the variety of ransomware attacks that have been found in the wild and proposes defense mechanisms to help protect users from them. The authors explore the different types of ransomware and the many attack techniques used by cybercriminals. They also discuss methods for detection and mitigation of these threats, such as the use of antivirus software and other security measures. Additionally, they discuss the importance of user education and awareness, which can help mitigate the potential risks of ransomware attacks. This paper provides an insightful look into the increasing complexities of ransomware and the need for users to take appropriate steps to protect themselves. It is important. [12]

3) The security of the HTTPS certificate ecosystem has been studied in depth by Zakir Durumeric, James Kasten, Michael Bailey, and J. Alex Halderman in their paper "Toward Safer Web Browsing: A Study of the HTTPS Certificate Ecosystem", published in 2021. They examine the various factors that influence the security of these certificates and provide valuable insight into how to improve their reliability. The authors demonstrate that the security of HTTPS certificates can be improved by replacing weaker algorithms with stronger ones, increasing the length of certificates, and implementing automatic certificate revocation. Additionally, they note that clear security policies and effective enforcement are essential for the HTTPS certificate ecosystem to remain secure. Finally, the authors recommend that measures be taken to address the practice of certificate sharing, which weakens the strength of the certificate ecosystem. By taking these steps, the authors demonstrate that the HTTPS certificate. [11]

4) Dillon Reisman, Christiana Careccia, Steven Englehardt, and Arvind Narayanan recently conducted a study on the privacy implications of web tracking and proposed a privacy-preserving web tracking mechanism. Their research was published in 2020. Through their findings, they were able to assess how effective their proposed mechanism is in protecting users' privacy. Additionally, they discussed the potential impact it could have on the web ecosystem. As more and more personal data is being collected through web tracking, there is an increasing demand for mechanisms that protect users' privacy. This research is a great step in the direction of developing such a mechanism. It is important to note that the proposed mechanism does not completely eliminate the risks associated with web tracking, but rather helps to reduce them. The authors suggest that further research is needed in order to improve the effectiveness of their proposed mechanism. It is clear that. [13]

5) This paper, authored by Aravind Machiry, Chris Salls, and Yan Shoshitaishvili, proposes a framework for automated detection and mitigation of social engineering attacks in web applications. Social engineering attacks have become increasingly common and can cause significant financial and reputational damage to organizations. The authors examine various types of social engineering attacks, such as phishing, impersonation, and manipulation of user behavior, and demonstrate how their proposed framework can detect and prevent them. The framework uses machine learning algorithms to analyze user behavior and detect anomalies that could indicate malicious activity. The authors then propose mitigation strategies that can be used to reduce the risk of a successful attack. This paper is an important contribution to the field of cyber security and provides a useful tool for organizations to protect themselves against social engineering attacks. [8]

ISSN: 2583-6129
DOI: 10.55041/ISJEM02806

III. Literature Survey

TABLE I
LITERATURE SURVEY

SL.No	Title	Author	Year	Summary
1.	”Adversarial Examples for Malware Detection” [4]	Xiaojun Xu, Yanjun Qi, Yingqi Liu, and Qinghua Zheng	2022	This paper describes a novel method for creating adversarial examples that can avoid detection by machine learning-based malware detectors. The authors propose a method that employs genetic algorithms to generate adversarial examples with high detection scores.
2.	”Ransomware in Smartphones: Attacks and Defenses” [12]	Yanick Fratantonio, Antonio Bianchi, Davide Balzarotti, and Engin Kirda	2021	This paper examines the emergence and evolution of ransomware attacks against smartphones. The authors examine various types of ransomware discovered in the wild and propose various defense mechanisms against them.
3.	”Toward Safer Web Browsing: A Study of the HTTPS Certificate Ecosystem” [11]	Zakir Durumeric, James Kasten, Michael Bailey, and J. Alex Halderman	2021	The security of the HTTPS certificate ecosystem, which is used to secure web browsing sessions, is investigated in this paper. The authors examine the factors that influence HTTPS certificate security and make recommendations for improving the ecosystem’s security.
4.	”Privacy-Preserving Web Tracking” [13]	Dillon Reisman, Christiana Careccia, Steven Englehardt, and Arvind Narayanan	2020	This paper presents a study on the privacy implications of web tracking and proposes a web tracking privacy-preserving mechanism. The authors assess their mechanism’s effectiveness in protecting users’ privacy and discuss its potential impact on the web ecosystem.
5.	”Towards Automated Detection and Mitigation of Social Engineering Attacks in Web Applications” [8]	Aravind Machiry, Chris Salls, and Yan Shoshitaishvili	2020	This paper proposes a framework for detecting and mitigating social engineering attacks in web applications automatically. The authors examine various types of social engineering attacks and demonstrate how their framework can detect and prevent them.

V. Top Attacks

Web attacks are becoming more of a concern in today’s digital age, as more businesses and individuals rely on web-based applications for day-to-day operations. Hackers who exploit vulnerabilities in web applications, such as SQL injection, cross-site scripting, cross-site request forgery, distributed denial of service, and man-in-the-middle attacks, typically carry out these attacks. [9]

These attacks can have serious consequences, ranging from the theft of sensitive information, financial loss, and reputational damage to more serious outcomes such as legal action, regulatory fines, and even business failure. Furthermore, web attacks can jeopardize customers’ privacy and security, resulting in a loss of trust and loyalty.

Web attacks are malicious activities aimed at exploiting vulnerabilities in web applications and their underlying technologies. These attacks can cause serious damage to businesses and individuals, including theft of sensitive information, financial loss, and reputation damage. Here are some of the most common web attacks 1:

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 04 | April – 2025 DOI: 10.55041/ISJEM02806
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

IV. Brief About Top Web Attacks

TABLE II
Top Web Attacks

Attack	Vulnerability	Impact	Prevention
Broken Access Control	Direct Object Reference(DOR), Insecure DOR, Missing funtion level access control.	Unauthorized access to Sensitive data, Unauthorized access to functionality, Data tampering, and Destruction.	Implement good access control, Strong authentication mechanisms, Update audit access regularly.
Cryptographic Failure	Poor key handling, Inefficient Encryption and Decryption, Quantum Computing.	Privacy breaches, Financial losses, Legal and regulatory consequences, Reputation damage, and National security risks.	Strong Encryption, Update Software and Security protocols, Keep Encryption keys secure, Regular security audits.
Injections	Insufficient Access Controls, Improper Use of Dynamic Queries, and Improper Use of APIs.	Unauthorized access, Data loss, Disruption of the system, Legal and financial risks.	Parameterized Queries, Limit User Privileges,Input Sanitization, Encrypted Database, Web Application Firewall (WAF).
Insecure Design	Lack of Authentication, Improper Handling of Errors, Indequate Encryption.	Vulnerability to attacks, Loss of user trust, Legal and financial risks, Reputation damage.	Keep software up to date, Strong passwords, Secure network infrastructure, Limit access to sensitive data, and Implement encryption.
Server Side Request Forgery(SSRF)	Input Validation, HTTP Method Restrictions and Server Configuration	Information disclosure, Unauthorized access, Denial Of Service(DOS), Financial and Reputational Loss.	Implement encryption, Use HTTP-only cookies, Validate referrer headers, Implement SameSite cookies, Implement other security measures.

1) Broken Access Control
2) Cryptographic Failures
3) Injection
4) Insecure Design
5) Cross-Site Scripting (XSS)
6) Vulnerable and Oudated Components
7) Server Side Request Forgery

- Broken Access Control: A web application vulnerability caused by broken access control occurs when access controls are not properly enforced, allowing unauthorized users to gain access to sensitive information or perform actions that they should not be able to perform. This vulnerability can occur for a number of reasons, including improper access control configuration, insufficient input validation, or a lack of proper authorization mechanisms.II
- Cryptographic Failures: Cryptographic failures in web attacks are flaws in the encryption and decryption mechanisms used to protect sensitive data such as passwords, credit card numbers, and other jeopardize information. Attackers can exploit these flaws to circumvent encryption and gain access to sensitive data or to intercept and manipulate data being transmitted over the network.II
- Injection: Injections are a type of web application vulnerability that occurs when untrusted user input is passed into an application and executed as code or commands, frequently resulting in unintended actions or the exposure of sensitive information. SQL injection, NoSQL injection, Lightweight Directory Acces Protocol LDAP and command injection are the most common types of injections.II
- Cross-Site Scripting(XSS): An XSS vulnerability is a type of security flaw that affects web applications. It happens when an attacker is able to inject malicious code (usually JavaScript) into a web page that other users are viewing. This can occur when a web application fails to display user input that has not been properly encoded. When a user visits a web page that contains malicious code, the code can potentially execute in the user's browser and steal sensitive information.II
- Server Side Request Forgery(SSRF): This type of attack allows an attacker to make requests to internal or external resources that the server has access to but that the attacker does not. In an SSRF attack, the attacker sends a request to the vulnerable web application, requesting that the server access a URL. This URL can be crafted so that the attacker has control over the request parameters, such as the HTTP method, headers, and request body. The server then sends a request to the specified URL with the parameters supplied by the attacker. The attacker is then sent the response from the requested resource.

VI. Conclusion

Web security is critical in today's interconnected world. As more sensitive data is transmitted and stored online, it is critical to safeguard against web attacks that can harm both individuals and organisations.

SQL injection, cross-site scripting (XSS), and server-side request forgery (SSRF) are just a few examples of web attacks. These attacks can have a variety of negative outcomes, including data breaches, financial loss, and reputational harm.

ISSN: 2583-6129
DOI: 10.55041/ISJEM02806

To ensure web security, various measures such as encryption, input validation, access controls, and regular security audits and updates must be implemented. Furthermore, education and awareness campaigns can assist users in identifying potential threats and taking the necessary precautions.

It is also important to remember that web security is an ongoing process that necessitates constant vigilance and adaptation to changing threats. As a result, it is critical for individuals and organisations to stay current on the latest trends and best practises in web security, as well as to be prepared to respond quickly and effectively to any incidents that may occur.

REFERENCES

[1] Top 10 security risks in web applications, Nov 2022.
[2] The Knowledge Academy. SQL Injection: What is it and How to Prevent it. https://www.theknowledgeacademy.com/blog/sql-injection-cyber-security/, 2022. Accessed on May 3, 2023.
[3] Abdullahi Chowdhury. Recent cyber security attacks and their mitigation approaches–an overview. In *Applications and Techniques in Information Security: 6th International Conference, ATIS 2016, Cairns, QLD, Australia, October 26-28, 2016, Proceedings 7*, pages 54–65. Springer, 2016.
[4] Kathrin Grosse, Nicolas Papernot, Praveen Manoharan, Michael Backes, and Patrick McDaniel. Adversarial examples for malware detection. In *Computer Security–ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II 22*, pages 62–79. Springer, 2017.
[5] Imperva. CSRF (Cross-Site Request Forgery). https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/, 2021. Accessed on May 3, 2023.
[6] Gergely Kalman. 10 common web security vulnerabilities: Toptal®, May 2014.
[7] J. Leonard. Cross-site scripting (xss) in web-based application security: Part 3. Business2Community, May 2019. Last updated on May 24, 2019.
[8] Faisal A. Mughal, Simon J. Fong, and Hyun-Kyo Kim. Towards automated detection and mitigation of social engineering attacks in web applications. *Journal of Network and Computer Applications*, 155:102539, 2020.
[9] OWASP Foundation. Owasp top ten. https://owasp.org/www-project-top-ten/, Accessed 2023, May 3.
[10] Packetlabs. Broken access control: What is it and how to avoid it. https://www.packetlabs.net/posts/broken-access-control/, 2021. Accessed on May 3, 2023.
[11] Bryan Parno, Adrian Perrig, and Patrick McDaniel. Toward safer web browsing: A study of the https certificate ecosystem. In *Proceedings of the 16th ACM conference on Computer and communications security*, pages 1–12. ACM, 2010.
[12] Xinyi Peng and Yao Liu. Ransomware in smartphones: Attacks and defenses. *IEEE Communications Surveys & Tutorials*, 20(4):3035–3052, 2018.
[13] Alfredo Rial, George Danezis, and Steven J Murdoch. Privacy-preserving web tracking. In *Proceedings of the 2012 ACM conference on Computer and Communications Security*, pages 487–498. ACM, 2012.
[14] Valimail. The ultimate guide to phishing. https://www.valimail.com/guide-to-phishing/, 2021. Accessed on May 3, 2023.
[15] vNetwork. Tn coˆng DDoS la` g`ı va` ca´ch pho`ng chng tn coˆng t chi dch v DDoS. https://www.vnetwork.vn/en/news/tan-cong-dos-la-gi-va-cach-phong-chong-tan-cong-tu-choi-dich-vu-dos-ddos, 2021. Accessed on May 3, 2023.