iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78777

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Cybersecurity Threats in Web Applications

Tashveen Kaur[1], Ipshita Arora[2], Shreya Arora[3], YogitaThareja[4]
Vivekananda Institute of Professional Studies – Technical Campus

Abstract: ***With the rapid growth of internet-based services, web applications have become essential for businesses, educational institutions, and governments.***
However, the increasing dependence on web platforms has also resulted in a rise in cybersecurity threats. This research paper examines common cybersecurity threats affecting web applications, including SQL Injection, Cross-Site Scripting (XSS), phishing attacks, malware, and Denial-of-Service (DoS) attacks.
These threats exploit vulnerabilities in poorly designed or insecure web applications and can lead to data theft, service disruption, and financial loss.
The study also discusses preventive security measures such as secure coding practices, authentication mechanisms, encryption techniques, web application firewalls, and regular security testing.
Keywords: Cybersecurity, Web Applications, SQL Injection, Cross-Site Scripting, Web Security, OWASP

I. INTRODUCTION

Web applications are widely used across the world for services such as online banking, shopping, education, and communication. These applications often store sensitive user information including personal data, financial details, and login credentials. Due to the valuable nature of this information, web applications have become common targets for cybercriminals.
Cybersecurity threats arise due to vulnerabilities in software design, weak authentication systems, poor coding practices, and lack of proper security measures. Attackers exploit these weaknesses to gain unauthorized access, steal confidential data, or disrupt services.

II. RESEARCH OBJECTIVES

1) To identify major cybersecurity threats affecting web applications.
2) To analyze common vulnerabilities exploited by attackers.
3) To study security techniques used to protect web systems.
4) To understand the impact of cyber attacks on organizations and users.

III. LITERATURE REVIEW

Several studies have identified major security vulnerabilities in modern web applications. The OWASP Top 10 report highlights critical web security risks such as SQL injection and cross-site scripting which often occur due to improper input validation.
According to Stallings (2017), weak authentication systems and lack of security testing increase the possibility of cyber attacks. Security frameworks such as the NIST Cybersecurity Framework recommend secure coding practices and regular vulnerability assessments.

IV. RESEARCH METHODOLOGY

This research is based on qualitative analysis of cybersecurity threats affecting web applications. Information was collected from academic journals, cybersecurity reports, books, and trusted technology websites.
The collected information was analyzed to identify patterns of cyber attacks and common vulnerabilities exploited by attackers.

V. COMMON CYBERSECURITY THREATS IN WEB APPLICATIONS

Figure 1: Common Cybersecurity Threats in Web Applications

1) SQL Injection: SQL injection occurs when attackers insert malicious SQL queries into input fields. This allows attackers to access or manipulate database information.
2) Cross-Site Scripting (XSS): Cross-site scripting occurs when malicious scripts are injected into web pages and executed in a user's browser.
3) Phishing: Phishing attacks trick users into revealing sensitive information such as usernames, passwords, or credit card details.
4) Malware: Malware is malicious software designed to damage systems or steal data.
5) Denial of Service (DoS): A denial-of-service attack overwhelms a server with traffic making the web application unavailable.

VI. PREVENTIVE SECURITY MEASURES

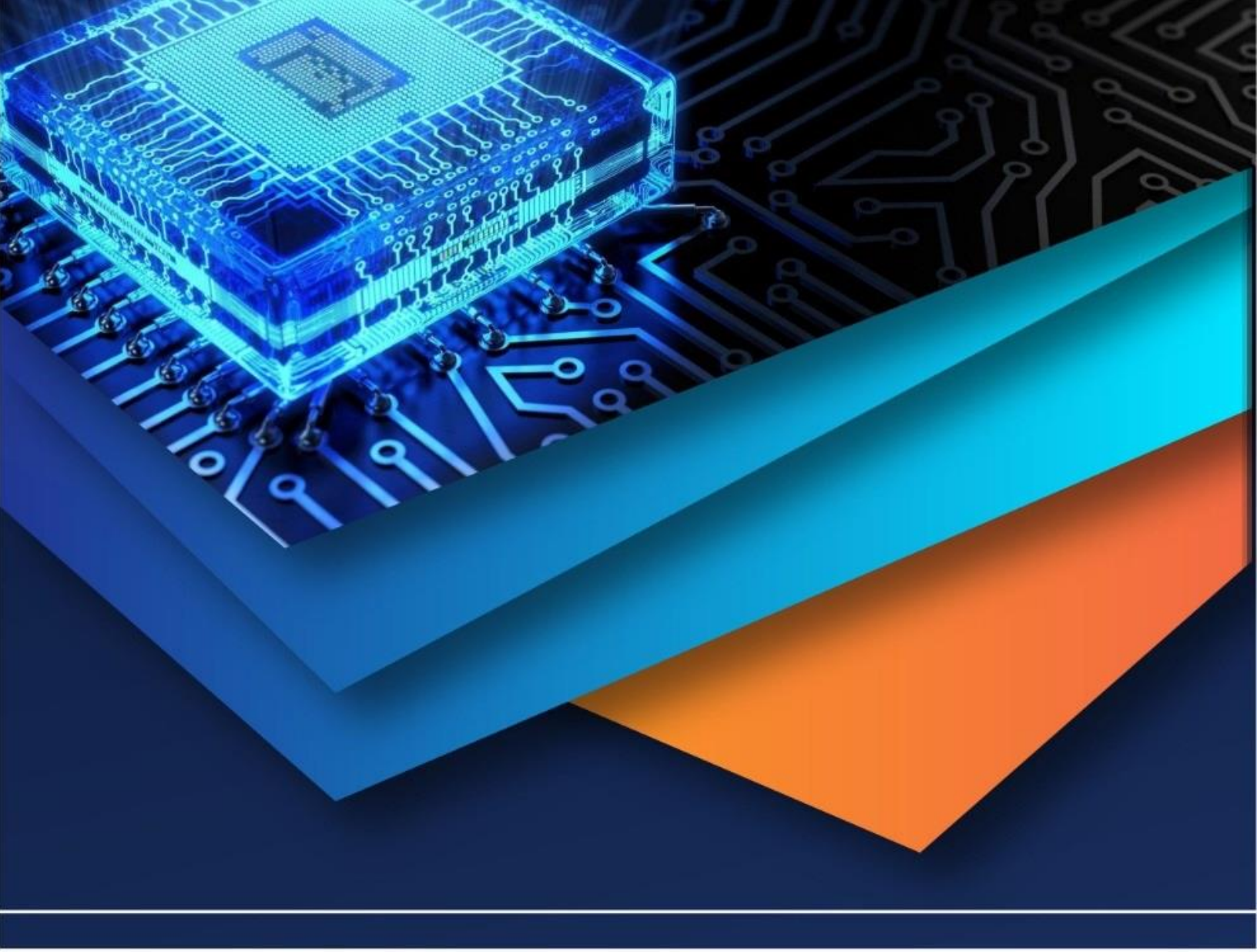
1) Secure coding practices
2) Multi-factor authentication
3) Web Application Firewalls (WAF)
4) Regular vulnerability scanning
5) Penetration testing
6) Regular security updates

VII. CONCLUSION

Cybersecurity threats in web applications continue to grow as digital technologies evolve. SQL injection, cross-site scripting, phishing, malware, and denial-of-service attacks remain major risks. Implementing strong security practices can significantly improve the security of modern web applications.

REFERENCES

[1] OWASP Foundation. (2021). OWASP Top 10 Web Application Security Risks.
[2] Stallings, W. (2017). Network Security Essentials.
[3] NIST Cybersecurity Framework (2018).
[4] Cisco Cybersecurity Report (2022).
[5] OWASP Web Security Testing Guide.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY