




RS Global  
Journals

Scholarly Publisher  
RS Global Sp. z O.O.  
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw, Poland 00-773  
Tel: +48 226 0 227 03  
Email: editorial\_office@rsglobal.pl

|                      |   |
|----------------------|---|
| <b>JOURNAL</b>       | International Journal of Innovative Technologies in Economy   |
| <b>p-ISSN</b>        | 2412-8368   |
| <b>e-ISSN</b>        | 2414-1305   |
| <b>PUBLISHER</b>     | RS Global Sp. z O.O., Poland  |
| <b>ARTICLE TITLE</b> | NEGLECTING THE FUNDAMENTALS: HOW FOCUS ON WEB APPS AND FRAMEWORKS LEAVES GAPS IN NETWORK SECURITY   |
| <b>AUTHOR(S)</b>     | Dadash Guluzade   |
| <b>ARTICLE INFO</b>  | Dadash Guluzade. (2024) Neglecting the Fundamentals: How Focus on Web Apps and Frameworks Leaves Gaps in Network Security. <i>International Journal of Innovative Technologies in Economy</i> . 3(47). doi: 10.31435/rsglobal_ijite/30092024/8210 |
| <b>DOI</b>           | <a href="https://doi.org/10.31435/rsglobal_ijite/30092024/8210">https://doi.org/10.31435/rsglobal_ijite/30092024/8210</a>   |
| <b>RECEIVED</b>      | 12 July 2024  |
| <b>ACCEPTED</b>      | 15 August 2024  |
| <b>PUBLISHED</b>     | 16 August 2024  |
| <b>LICENSE</b>       | <br>This work is licensed under a <b>Creative Commons Attribution 4.0 International License</b> .  |

© The author(s) 2024. This publication is an open access article.

# NEGLECTING THE FUNDAMENTALS: HOW FOCUS ON WEB APPS AND FRAMEWORKS LEAVES GAPS IN NETWORK SECURITY

**Dadash Guluzade**

*Master Degree, Independent Cyber Security Researcher, PhD Candidate, University of Lodz, Poland*

DOI: [https://doi.org/10.31435/rsglobal\\_ijite/30092024/8210](https://doi.org/10.31435/rsglobal_ijite/30092024/8210)

---

## ARTICLE INFO

Received 12 July 2024

Accepted 15 August 2024

Published 16 August 2024

---

## KEYWORDS

Web Apps, Frameworks,  
Network Security.

## ABSTRACT

In the contemporary digital landscape, the rapid proliferation of web applications and frameworks has captivated the focus of cybersecurity professionals. While these modern technologies are crucial for user experience and business operations, this shift in attention often comes at the expense of foundational network protocols—DNS, DHCP, and TCP/IP. These protocols form the bedrock of network security and efficiency. This paper explores the critical role of managing DNS, DHCP, and TCP/IP in maintaining a secure and efficient network infrastructure. By emphasizing the need to balance attention between cutting-edge web technologies and fundamental network protocols, this study highlights the vulnerabilities that arise from neglecting these essential components. Effective management of these protocols is likened to fortifying the basic structures of a country house, ensuring a robust defense against vulnerabilities.

---

**Citation:** Dadash Guluzade. (2024) Neglecting the Fundamentals: How Focus on Web Apps and Frameworks Leaves Gaps in Network Security. *International Journal of Innovative Technologies in Economy*. 3(47). doi: 10.31435/rsglobal\_ijite/30092024/8210

---

**Copyright:** © 2024 Dadash Guluzade. This is an open-access article distributed under the terms of the **Creative Commons Attribution License (CC BY)**. The use, distribution or reproduction in other forums is permitted, provided the original author(s) or licensor are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

---

## Introduction.

The cybersecurity landscape is in constant flux, driven by the relentless growth of web applications and frameworks. These technologies enhance user experiences and streamline business operations, but the overwhelming focus on them can inadvertently lead to the neglect of foundational network protocols. Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Transmission Control Protocol/Internet Protocol (TCP/IP) are essential for the security and efficiency of any network. Mismanagement or overlooking these protocols opens ports for cyber threat actors to exploit vulnerabilities.

This article examines the importance of DNS, DHCP, and TCP/IP in maintaining secure and efficient networks. It discusses the potential risks associated with neglecting these fundamental protocols and provides practical insights into effective management practices. The goal is to urge cybersecurity professionals to maintain a balanced approach, giving due attention to both modern web technologies and the essential network protocols that underpin them.

### **Neglecting the Fundamentals: The Risks.**

#### **1. Domain Name System (DNS)**

- **Role in Network Security:** DNS translates domain names into IP addresses, making it possible for users to access websites and online services. This process is critical for the functioning of the internet.
- **Security Risks:** DNS is susceptible to attacks such as DNS spoofing and cache poisoning, which can redirect users to malicious sites. Ensuring DNS security through measures like DNS Security Extensions (DNSSEC) is vital.
- **Literature Reference:** According to Mockapetris and Dunlap (1988), the development and security of the DNS system are paramount for maintaining the integrity of internet navigation.

#### **2. Dynamic Host Configuration Protocol (DHCP)**

- **Role in Network Efficiency:** DHCP automates the assignment of IP addresses, ensuring efficient and conflict-free IP allocation. This is especially important in large networks with numerous devices.
- **Security Risks:** Unauthorized DHCP servers can cause IP conflicts and denial-of-service attacks. Implementing security measures like DHCP snooping can prevent such issues.
- **Literature Reference:** Droms (1997) emphasizes the necessity of secure DHCP implementations to prevent network disruptions and security breaches.

#### **3. Transmission Control Protocol/Internet Protocol (TCP/IP)**

- **Role in Data Transmission:** TCP/IP is the backbone of internet communication, ensuring reliable data transmission between devices. TCP handles the reliable delivery of data packets, while IP manages addressing and routing.
- **Security Risks:** TCP/IP is vulnerable to attacks such as IP spoofing, TCP SYN flooding, and man-in-the-middle attacks. Implementing robust security measures like IPsec can protect data integrity and confidentiality.
- **Literature Reference:** Stevens (1994) details the critical nature of TCP/IP protocols and the importance of securing them against evolving threats.

### **The Office Analogy: Ensuring Comprehensive Security.**

Think of your network as a country house where DNS, DHCP, and TCP/IP protocols are the essential structures—like fences, gates, and security systems. Web applications and frameworks are akin to the decor and advanced security gadgets that add value but cannot compensate for a weak foundational structure. Cyber threat actors are like intruders who can easily bypass superficial defenses if the fundamental structures are weak. Ensuring the security of DNS, DHCP, and TCP/IP is akin to reinforcing your fences, gates, and basic security systems, providing a strong defense against any intruders.

### **Practical Management Strategies.**

#### **1. Regular Audits and Updates.**

- Conduct periodic audits of DNS and DHCP configurations to ensure they are secure and up-to-date.
- Regular updates can close security gaps and improve network performance.

#### **2. Security Configurations.**

- Apply security best practices such as DNSSEC for DNS and IP address filtering for DHCP.
- **Example:** Enhancing DNS security by enabling DNSSEC and restricting DHCP configurations to authorized devices significantly reduced the risk of unauthorized access.

#### **3. Monitoring and Logging.**

- Implement robust monitoring and logging mechanisms to track network activity and detect anomalies.
- Continuous monitoring aids in the early detection of security incidents.

- **Example:** Utilizing tools like Wireshark and network logs, I monitored traffic patterns and identified suspicious activities, ensuring prompt response to potential threats.

### **Conclusion.**

Balancing the focus between modern web applications and foundational network protocols is crucial for maintaining secure and efficient networks. DNS, DHCP, and TCP/IP management should not be overlooked in the pursuit of cutting-edge technologies. By implementing best practices and leveraging integrated management strategies, organizations can enhance their network reliability, security, and performance. This study underscores the importance of giving due attention to both contemporary web technologies and the essential protocols that form the backbone of the internet.

### **REFERENCES**

1. Mockapetris, P., & Dunlap, K. (1988). Development of the Domain Name System. *ACM SIGCOMM Computer Communication Review*, 18(4), 123-133.
2. Droms, R. (1997). Dynamic Host Configuration Protocol. RFC 2131.
3. Stevens, W. R. (1994). *TCP/IP Illustrated, Volume 1: The Protocols*. Addison-Wesley.
4. Kent, S., & Atkinson, R. (1998). Security Architecture for the Internet Protocol. RFC 2401.
5. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). DNS Security Introduction and Requirements. RFC 4033.
6. Comer, D. E. (2006). *Internetworking with TCP/IP: Principles, Protocols, and Architecture*. Prentice Hall.
7. Albitz, P., & Liu, C. (2001). *DNS and BIND*. O'Reilly Media, Inc.
8. Stellin, S., Garfinkel, S., & Spafford, G. (2003). *Practical UNIX and Internet Security*. O'Reilly Media, Inc.