Multi-server web platforms: information security strategies

Ussatova Olga Alexandrovna\(^1\),
Bekmukhan Aigerim Serikbolkyzy\(^2\)

\(^1\) PhD, Acting Associate Professor; Institute of Information and Computing Technologies; Republic of Kazakhstan; Al-Farabi Kazakh National University; Republic of Kazakhstan

\(^2\) Master's student of the II course; Al-Farabi Kazakh National University; Republic of Kazakhstan

Abstract.
Exploring information security strategies specifically tailored for multi-server web platforms, this topic delves into the critical realm of safeguarding sensitive data and ensuring uninterrupted service availability. Multi-server web platforms often involve complex infrastructures, distributed systems, and diverse components, presenting unique challenges for security.

Keywords:
Multi-server web platforms, information security strategies, safeguarding, complex infrastructures, security challenges, network segmentation, load balancing, access controls, encryption, compliance, regulations
Networking technology and information technologies are integral to the modern world. A crucial part of this process is played by multi-server web systems, which integrate several servers and components. They are utilized in a wide range of industries, from online business to the delivery of services in the health and education sectors. However, the risk of information security breaches also rises with the popularity and sophistication of such systems.

Since data leaks, hacking, and other security-related occurrences can seriously harm both the business and end users, information protection is becoming a crucial component of the operation of multi-server online systems. Due to the fact that multiprocessor web systems process a significant quantity of sensitive data, such as private information and trade secrets, they are frequently targeted by hackers and intruders.

Therefore, it is impossible to overstate the significance of the topic "Information Security Risk Management of Multi-Server Web Systems". To ensure trustworthy data protection and the efficient operation of the system, this issue necessitates special consideration and the development of appropriate techniques and procedures. The primary information security threats that multiprocessor web systems confront, as well as strategies and tactics for reducing these risks, will be discussed in this article.

A software vulnerability is a weak point or a mistake in the code that can be used by attackers to gain access without authorization, escalate their privileges, compromise the privacy of user data, carry out harmful acts, and much more. Web systems are not an exception to the rule that vulnerabilities can exist in both the operating system and application software.

Assets, hazards, and vulnerabilities identification

Asset Identification: List every asset that the web system needs to safeguard. This comprises computers, databases, software, data, network hardware, and personnel.

Finding vulnerabilities: Identify weak points in the system that an attacker could exploit. These could include gaps in procedures, software defects, configuration mistakes, or other areas.
Assessment of potential consequences

Financial consequences: Assess the potential financial losses that may arise if the risk is realized. This may include the costs of restoring the system, lost profits, fines and legal costs.

Data Loss: Assess which data may be lost or compromised. This may be sensitive corporate data, personal data of users and other confidential information assets.

Risk assessment is a key stage in the development of an information security strategy. It allows you to identify priorities and resources that are necessary to reduce risks and protect the web system from potential threats.

<table>
<thead>
<tr>
<th>Threat/Vulnerability</th>
<th>Description</th>
<th>Probability</th>
<th>Potential consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Injection</td>
<td>An attack in which an attacker inserts SQL code into a web page, which can lead to the execution of unauthorized requests.</td>
<td>High</td>
<td>Access to the database, leakage of confidential data and violation of data integrity.</td>
</tr>
<tr>
<td>Cross-site Scripting (XSS)</td>
<td>An attack in which an attacker inserts a malicious script into a web page that is executed on the client side.</td>
<td>Average</td>
<td>Introduction of malicious scripts on web pages, theft of session data, phishing.</td>
</tr>
<tr>
<td>Cross-site Request Forgery</td>
<td>An attack in which an attacker sends fake requests on behalf of a user.</td>
<td>Average</td>
<td>Performing unauthorized actions on behalf of the user in the system.</td>
</tr>
<tr>
<td>Session Attacks and Authorization Management (CSRF)</td>
<td>Attacks aimed at hijacking or changing the user's session data without his knowledge.</td>
<td>Average</td>
<td>Fake actions on behalf of the user, malicious operations.</td>
</tr>
</tbody>
</table>

Table 1
In a world where information technology plays a key role in business and society, ensuring the security of multi-server web systems is becoming a matter of paramount importance. In this article, we have considered several main aspects of effective information security risk management in such systems.

Regular security audits and penetration testing provide organizations with tools to identify vulnerabilities and weaknesses, as well as to adjust actions and increase the level of protection.

As a result, effective information security risk management in multi-server web systems is not a one-time event, but an ongoing process that requires attention and participation from all levels of the organization. Security is a contribution to the future that ensures long-term

<table>
<thead>
<tr>
<th>Vulnerabilities in the access level</th>
<th>Vulnerabilities that can be exploited by attackers to bypass authentication mechanisms.</th>
<th>Average</th>
<th>Unauthorized access, leakage of confidential data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disadvantages in session management</td>
<td>Disadvantages in managing and storing session data.</td>
<td>Average</td>
<td>Compromise of sessions, authentication data, violation of confidentiality.</td>
</tr>
<tr>
<td>Shortcomings in monitoring and incident detection</td>
<td>Absence or inefficiency of incident monitoring and detection systems.</td>
<td>Average</td>
<td>Difficulty in detecting and responding to incidents, increased reaction time.</td>
</tr>
<tr>
<td>Attacks on applications</td>
<td>Attacks on applications, including exploits and vulnerabilities in the code, which can lead to remote attacks.</td>
<td>High</td>
<td>Introduction of malicious codes, denial of service, data leakage.</td>
</tr>
</tbody>
</table>

This work is distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (https://creativecommons.org/licenses/by-sa/4.0/).
sustainability and protects both business and data privacy.

In conclusion, the topic of "Multi-server Web Platforms: Information Security Strategies" underscores the critical importance of implementing robust security measures in complex, distributed environments. Safeguarding sensitive data and ensuring uninterrupted service availability are paramount considerations for organizations operating multi-server web platforms.

The exploration of security challenges and strategies, including network segmentation, load balancing, access controls, encryption, and intrusion detection systems, highlights the multifaceted nature of safeguarding these platforms. Additionally, the recognition of the need for a well-defined incident response plan and adherence to industry-specific compliance requirements underscores the comprehensive approach required for effective information security.

As technology continues to advance and threats evolve, staying abreast of emerging security strategies and best practices remains imperative for organizations seeking to protect their multi-server web platforms. Ultimately, the proactive implementation of these strategies is essential to maintain trust, integrity, and resilience in an increasingly interconnected digital landscape.

References: