Quantitative Assessment on Remote Code Execution Vulnerability in Web Apps

***Md. Maruf Hassan 1, Umam Mustain 1, Sabira Khatun 2, Mohamad Shaiful Abdul Karim 2, Nazia Nishat 1, Mostafijur Rahman 1**

1 Department of Software Engineering, Daffodil International University, Dhaka, Bangladesh
2 Faculty of Electrical and Electronics Engineering, University Malaysia Pahang, Malaysia
Email: maruf.swe@diu.edu.bd

Abstract:
With the exponential increasing use of online tools, applications that are being made for day to day purpose by small and large industries, the threat of exploitation is also increasing. Remote Code Execution (RCE) is one of the top most critical and serious web applications vulnerability of this era and one of the major concerns among cyber threats ,which can exploit web servers through their functionalities and using their scripts/files. RCE is an application layer vulnerability caused by careless coding practice which leads to a huge security breach that may bring unwanted resource loss or damages. Attacker may execute malicious code and take complete control of the targeted system with the privileges of an authentic user with this vulnerability. Attackers can attempt to advance their privileges after gaining access to the system. Remote Code Execution can lead to a full compromise of the vulnerable web application as well as the web server. This chapter highlights the concern and risk needed to put under consideration caused by RCE vulnerability of a system. Moreover, this study and its findings will help application developers and its stakeholders to understand the risk of data compromise and unauthorized access of the system. Around 1011 web applications were taken under consideration and experiment was done by following manual double blinded penetration testing strategy. The experiments shows that more than 12% web application were found vulnerable with RCE. This study also explicitly listed down the critical factors of Remote Code Execution vulnerability and improper input handling. The experimental results are promising to motivate developers to focus on security enhancement through proper and safe input handling.

Keywords : Web Application Vulnerabilities; Remote Code Execution (RCE); Input Validation; Data Breach.

Acknowledgments

The authors want to acknowledge and credit Cyber Security Centre of Daffodil International University for the help in conducting this study. Also want to show gratitude to the authorities of the organizations who have given permission to examine their web applications. This research work is supported by Fundamental Research Grant Scheme (FRGS), RDU190140 funded by Ministry of Higher Education (MOHE). The authors would also like to thank the Faculty of Electrical & Electronics Engineering, Universiti Malaysia Pahang (http://www.ump.edu.my/) for financial support.