

Unveiling User Enumeration Attacks: Methods, Impacts and Mitigation Strategies

Venera-Elena MĂCSINOIU

Faculty of Electronics, Telecommunications, and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest,
Romania

venera.macsinoiu@stud.etti.upb.ro

Abstract

This paper examines the vulnerabilities posed by user enumeration attacks and presents effective prevention techniques to safeguard against them. The paper investigates the various approaches that hackers use to compromise unsecured web application modules, including exploiting insecure user database interactions. Additionally, the paper discusses effective countermeasures, such as two-factor authentication, rate limiting, and password policies, that can prevent enumeration attacks. The research presented in this paper contributes to the field of data protection and privacy by identifying the unique characteristics of user enumeration attacks and proposing measures to enhance the security of web applications. The paper emphasizes the importance of securing user databases and educating users on the risks of user enumeration attacks as essential measures for safeguarding sensitive information.

Index terms: data protection, privacy, web application security, prevention techniques, vulnerabilities

References

- [1]. OWASP Top Ten 2017, A2:2017-Broken Authentication, https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication
- [2]. E. Kost, What is an Enumeration Attack? How they Work + Prevention Tips, <https://www.upguard.com/blog/what-is-an-enumeration-attack>
- [3]. RiskXchange, How to prevent an enumeration attack, <https://riskxchange.co/4317/how-to-prevent-an-enumeration-attack/>
- [4]. R. Das, What enumeration attacks are and how to prevent them, <https://www.techtarget.com/searchsecurity/tip/What-enumeration-attacks-are-and-how-to-prevent-them>