Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 08, August-2024

Exposing Insecure Direct Object Reference (IDOR) Vulnerabilities in Academic Publication Platforms: A Case Study)

Ellis Amissah
Faculty of Computing and Information Systems
Ghana Communication Technology University
Accra, Ghana

Felix Bentil
Department of Computer Applications
Lovely Professional University, LPU
Phagwara, India

***Abstract*— This article uncovers a significant security flaw known as Insecure Direct Object Reference (IDOR) found in an online academic publishing platform. The flaw allows unauthorized access to sensitive information, including the status of submitted documents, acceptance letters, payment details and author certificates. Through a detailed case study, we examine the discovery of this vulnerability, its potential consequences, and ethical considerations associated with its disclosure. We also provide recommendations for improving the security of academic and other online platforms to prevent similar issues.**

***Keywords*—Insecure Object Reference (IDOR); audit logs; responsible disclosure; Role-based access control (RBAC) ; randomized identifiers**

I. INTRODUCTION (BACKGROUND)

The evolution of scholarly publishing through digital transformation has resulted in various benefits and improved the efficiency and accessibility of the submission, review, and publication process. However, this change has also brought with it new hurdles, particularly in the area of cybersecurity. Ensuring the security of academic publishing platforms is crucial due to the processing and storage of sensitive data on the Internet.

In web applications, Insecure Direct Object Reference (IDOR) is a common security threat that occurs when an application grants direct access to objects without validating the user supplied input. If the system does not have sufficient access controls, unauthorized access to sensitive data may occur. IDOR vulnerabilities are of particular concern in situations where maintaining confidentiality and ensuring data integrity are critical, such as scientific publications.

II. CASE STUDY

A. Discovery of the Vulnerability

When attempting to publish a paper in an online academic journal, we were assigned a unique identifier (ID) “XXXXXX” to track the status of my submission. The ID was prominently displayed on the platform's interface and we were instructed to use it for future reference on the status of my submission.

Out of curiosity, we experimented by changing the ID number slightly. Increasing or decreasing the ID by a single digit gave us unexpected access to other authors' submission statuses. This simple change, which required no technical expertise, revealed sensitive details related to the contributions of other researchers using the platform.

B. Details of the Exploitable Information

The IDOR vulnerability allowed me to access a variety of sensitive information, including:

- Acceptance Letters: These documents contained important details such as reviewers' comments, a link to the publication fee payment portal, and the titles of the papers. The acceptance letters provided insight into reviewers' feedback, which is generally confidential.
- Documentation and Publication Status: We were able to view the status of all documentation required for publication, including whether all required documents had been submitted. This also included checking whether an author had completed the submission process or not.
- Payment status: The platform also revealed whether the publishing fee has been paid. In cases where the fee was paid, we were able to download the author certificates, which are official documents certifying the author's contribution to the published work and acknowledgment letter. This letter contained confidential information such as the author's name, registration ID, paper ID, published URL, and the signature of the editor-in-chief of the journal. This document is crucial for authors as it serves as proof of their publication.
- Multiple Authors: In cases where an article had multiple authors, the platform displayed the names of all co-authors. We could also download the certificates for each author, revealing their personal information without their consent.

The impact of this vulnerability was far-reaching. By simply changing the ID in the URL, we were able to access sensitive information that should be restricted to the original authors. The potential for misuse of this data is significant and raises concerns about privacy, academic integrity and the overall security of the platform.

C. Ethical Considerations

When we discovered this vulnerability, we recognized the ethical implications of my findings. The information I accessed was extremely confidential and any further investigation could have resulted in unintentional harm. We decided not to manipulate the ID any further and immediately thought about the appropriate course of action.

From an ethical perspective, it is essential to report such vulnerabilities to those responsible to ensure that they can take the necessary steps to protect their users' data. However, responsible disclosure must be handled carefully to avoid panicking or allowing malicious actors to exploit the vulnerability before it is fixed. In this case, we decided to report the issue directly to the platform administrators and provide them with detailed information about the vulnerability and its potential impact.

III. DISCUSSION

A. Security Implications

The IDOR vulnerability discovered in this case presents several significant security risks:

- Privacy Breach: A major violation of privacy occurs when someone gains unauthorized access to author certificates, acceptance letters, and payment statuses. Writers entrust these platforms with their personal and academic data, expecting it to be handled securely. A betrayal of this confidence may result in a decline in user trust in the platform and possibly even legal action.
- Academic Integrity: The ability to access and potentially alter submission statuses, reviewer comments, and acceptance letters undermines the integrity of the academic publishing process. Malicious actors could manipulate this information to falsify acceptance letters, interfere with the review process, or gain unfair advantages in publication.
- Financial Risks: Access to payment statuses and links to payment portals could be exploited for financial gain. Unauthorized individuals could interfere with the payment process or steal payment details, leading to financial losses for the affected authors.
- Forgery and Fraud: The availability of published paper confirmation letters, complete with the Editor-in-Chief's signature, opens the door to forgery and academic fraud. Malicious actors could create counterfeit documents, posing as legitimate authors or fabricating publications to enhance their academic credentials.

B. Broader Impact on Online Systems

While this case study focuses on an academic publication platform, the implications of IDOR vulnerabilities extend far beyond this context. IDOR is a common vulnerability in web applications that handle sensitive or personal information, such as healthcare systems, financial services, and e-commerce platforms. The consequences of an IDOR exploit in these contexts could be even more severe, leading to large-scale data breaches, financial losses, and damage to an organization's reputation.

C. Ethical Responsibilities in Vulnerability Disclosure

As cybersecurity professionals or researchers, it is crucial to approach vulnerability disclosure with a strong ethical framework. Responsible disclosure involves notifying the affected organization in a manner that allows them to address the issue before it becomes widely known. It also involves respecting the privacy and confidentiality of any data that may have been accessed during the discovery process.

In this case, the decision to report the vulnerability directly to the platform administrators was guided by ethical considerations. By providing detailed information about the vulnerability and its potential impact, I aimed to assist the platform in rectifying the issue while minimizing the risk of harm to its users.

IV. RECOMMENDATIONS

A. Immediate Mitigation Measures

The following steps should be taken immediately to address the identified IDOR vulnerability:

1) Disable Sequential IDs: The platform should disable the functionality that allows users to access records based on sequential IDs. Instead, unique identifiers should be randomly generated and difficult to guess, reducing the likelihood of unauthorized access.

2) Implement Access Controls: Robust access controls must be put in place to ensure that only authorized users can access sensitive information. This could include verifying user credentials before granting access to specific resources.

3) Audit Logs: The platform should maintain detailed audit logs that track access to sensitive information. This would allow administrators to monitor for unauthorized access and take corrective action if necessary.

B. Long-Term Solutions

To prevent similar vulnerabilities in the future, the following best practices should be adopted:

1) Use Non-Sequential, Randomized Identifiers: Randomizing IDs makes it significantly more difficult for attackers to guess and access other users' data. This approach should be standard practice in any application handling sensitive information.

2) Access Control Mechanisms: Robust Implement strict access control mechanisms that verify user permissions before granting access to any resource. Role-based access control (RBAC) can be particularly effective in ensuring that users only have access to the information necessary for their role.

3) Regular Security Audits: Finding and fixing possible vulnerabilities before they can be exploited requires routine security audits and penetration tests. Tests for widespread vulnerabilities such as IDOR ought to be part of these audits.

4) Data Encryption: Sensitive data should be encrypted both in transit and at rest. Encryption adds an additional layer of security, ensuring that even if data is accessed by unauthorized users, it remains protected.

5) User Education: Educating users on the importance of security and safe practices can help reduce the risk of vulnerabilities being exploited. This includes training users to recognize potential security issues and report them appropriately.

CONCLUSION

The discovery of this IDOR vulnerability underscores the critical need for robust security measures in online academic publishing platforms. As the academic community increasingly relies on digital tools, safeguarding these platforms against vulnerabilities is essential to maintaining the trust and integrity of the publication process.

Addressing this vulnerability requires immediate action from the platform administrators, as well as a long-term commitment to security best practices. By implementing the recommended measures, academic publishers can protect their users' data, ensure the integrity of the publication process, and mitigate the risks posed by similar vulnerabilities in the future.

REFERENCES

[1] OWASP Foundation. (2021). OWASP Top Ten 2021: The Ten Most Critical Web Application Security Risks, [Online]. Available: https://owasp.org/Top10/

[2] OWASP Foundation. (2020). Insecure Direct Object Reference (IDOR) – OWASP Cheat Sheet Series. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Cheat_Sheet.html

[3] OWASP Foundation. (2021). Access Control Cheat Sheet – OWASP Cheat Sheet Series. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Access_Control_Cheat_Sheet.html

[4] ISO/IEC 27001:2022. (2022). Information security management systems – Requirements. International Organization for Standardization. [Online]. Available: https://www.iso.org/standard/82102.html

[5] Bertino, E., & Sandhu, R. S. (2005). Role-Based Access Control: A Multi-Dimensional Overview. IEEE Computer Society. [Online]. Available: https://ieeexplore.ieee.org/document/1411274

[6] Kennesaw State University. (2023). The Importance of Data Encryption. [Online]. Available: https://www.kennesaw.edu/computer-science/data-encryption

[7] CERT/CC. (2022). The Importance of Regular Security Audits. [Online]. Available: https://www.cert.org/incident-management/regular-security-audits/

[8] NIST. (2018). Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[9] Briney, A. (2021). Ethical Hacking: The Ethical Responsibilities of Vulnerability Disclosure. [Online]. Available: https://www.techrepublic.com/article/ethical-hacking-responsibilities/

[10] SANS Institute. (2020). Penetration Testing and Vulnerability Assessment: Best Practices. [Online]. Available: https://www.sans.org/white-papers/42378/