WEB SECURITY AND BROKEN ACCESS CONTROL: AN ANALYSIS

Nurfitri Fatiha Balqis Bin Zairudin (CI230096)

Nurdhia Dalili Iezazi Binti Mohamad Fuad Halmi (CI230097)

Farah Nur Ain Binti Arzhar (CI230080)

Muhammad Aiman Bin Sufian (CI230136)

Muhammad Aiman Firdaus Bin Shahrul Nizam (DI220009)

Cik Feresa

**1.0 Abstract**

Rendering secureness online is of utmost significance for preventing undesired events. Most websites are readily capable of being attacked and the application of OWASP (Open Web Application Security Project) can serve as a tool to identify widespread security issues in web applications. One of the major issues in the OWASP Top 10 list is the Broken Access Controls (A01:2021) which happens when a system does not have any proper restriction on a user's access. This enables hackers to do something like taking people's private information or doing things that they are not supposed to do.

In this report, we will discuss the following: Broken access controls, potential for exploitation, and preventive measures. A real-life example of the Facebook Data Breach (2019) is presented where bad access controls let 540 million user records get leaked. This incident is the evidence enough as to why guarding security should be the main concern.

**2.0 Introduction to OWASP**

OWASP (Open Web Application Security Project) international non-profit group was founded to help improve software security worldwide. Experts can collaborate openly to uncover vulnerabilities, and apply coding practices to writing programs. The community spreads the message about security threats and provides solutions for reducing potential cyber risks. Some of the most significant contributions from the OWASP's part come from the OWASP Top 10, which is a list of the ten most important security threats in online applications. The OWASP Top 10 is a reference for the developers & the security professionals so as to be able to prioritize and fix the vulnerabilities in their own applications. Real-world expertise and situations on which this list was compiled by the experts. Every three to four years, it is revised to account for the new security threats that have emerged. It saves companies from being exposed to the latest vulnerabilities by following the development-in response and utilizing the study and the real-world data to make appropriate defences.

**3.0 Broken Access Control (A01:2021)**

Broken Access Control is a vulnerability that occurs when an application fails to execute authorization correctly, which allows those who are not authorized to access the system to take actions that they should not be able to. This vulnerability can result in unauthorized access, data tampering, or even system control. This vulnerability exploit comes in different forms. When users are assigned more permissions than they need, least privilege violations occur, thereby increasing the security risk. Insecure Direct Object References (IDOR) comes into play, the code does not properly protect from manipulating internal IDs such as user IDs in order to access unauthorized areas. The vulnerable APIs are the hacker’s favourite targets, through which API security can be compromised. Metadata tampering is another type of attack where session tokens or cookies are tampered with so that the authentication bypassed, and CORS misconfiguration is when the cross-origin resource sharing has the wrong settings, thus making the applications more vulnerable to cyber threats.

Installing server-side access control mechanisms with role-based access control (RBAC) and direct access to sensitive resources can avoid vulnerable points and carrying out regular security audits can also improve security. Furthermore, monitoring and logging unauthorized access attempts help the detection and response measures.

**4.0 Case Studies: Real-World Security Breaches**

Broken Access Control is responsible for many violations in reality. First, a bug in Facebook's contact importer feature, which was later fixed, allowed the unlawful harvesting of data, thus, there were threats of the 2021 Facebook Data Breach. This has exposed the personal information of 533 million users. The intruders made a step further and gained more than access rights which resulted in the imperative to adopt strong authentication, rate limiting and improved API security.

In addition, the Muslim Pro App Data Leak (2020) is also one of the occasions when a heavily used religious app illicitly traded the user location data to the third-party intermediaries, connected with the U.S. military. The guilt of doing so rests with the privacy and ethical issues. Access failure was the factor that led to the misuse of sensitive user information by the third parties. The positive measures in such cases consist of clear data policies, encryption, and a more stringent policy for the third-party business.

The Clubhouse Data Breach (2021) yet again is another grave example of API security flaws causing 1.3 million user records to be tapped into without authorization. The chinks of the access of user data by third parties led to too great exposure of data and thus making phishing and theft easier. The first step is for a company to enforce API authentication, and put in place rate limiting and access restrictions to protect the information of its user.

**5.0 Conclusion**

One of the vectors of vulnerability in web security that is still very risky is the one for Broken Access Control. It is virtually evident from the real-world case studies that access controls that are incompletely overwritten can lead to data breaches that are as severe as identity theft, and that can even lead to public trust loss. To cope with these threats, organizations must press for strong access control mechanisms, regularly conduct security audits as well as driving hard data protection policies. Businesses can keep their user's data secure and the users can trust them by being quick to solve these vulnerabilities effectively.

**6.0 References**

* ‌Forced Browsing. (2023, January 31). Invicti. https://www.invicti.com/learn/forced-browsing/
* OWASP. (2021). A01 Broken Access Control - OWASP Top 10:2021. Owasp.org; OWASP. https://owasp.org/Top10/A01\_2021-Broken\_Access\_Control/
* ‌OWASP. (2013). Insecure Direct Object Reference Prevention · OWASP Cheat Sheet Series. Owasp.org. https://cheatsheetseries.owasp.org/cheatsheets/Insecure\_Direct\_Object\_Reference\_Prevention\_Cheat\_Sheet.html
* ‌Suryawanshi, T. (2023, April 14). Cross-Origin Resource Sharing (CORS) Vulnerability: Example and Prevention. Medium. https://medium.com/@tushar\_rs\_/cross-origin-resource-sharing-cors-vulnerability-example-and-prevention-588d299ff185
* ‌What Is Privilege Escalation? - Definition, Types, Examples | Proofpoint US. (2023, July 10). Proofpoint. https://www.proofpoint.com/us/threat-reference/privilege-escalation
* ‌What is Metadata? – Forensicon. (n.d.). https://www.forensicon.com/resources/articles/what-is-metadata/