issue 02

Case Study

IDOR IN HEALTHCARE APPLICATION

arcusec.com

Client Overview

Arcus was engaged from a leading healthcare company to conduct an application pen test. The scope of the engagement covered the platform’s web application and API.

OBJECTIVE

The primary objective of the engagement was to identify and assess the security vulnerabilities within the organization's web application and deliver recommendations to protect against potential threats and to ensure the integrity, confidentiality, and availability of its customer data and systems.

ATTACK VECTOR

During the penetration testing process, Arcus' assessment team identified an insecure direct object reference (IDOR) within the client's web application. Leveraging the discovered finding, an attacker could register in the application and manipulate the user parameter, therefore, accessing the medical records and PII of other users by only incrementing the user identifier.

This flaw effectively provided unauthorized access to the sensitive information of all users within the healthcare institution's system. The impact was severe, as it compromised the confidentiality of patient data and violated privacy regulations.

IMPACT

Financial Cost

An institution may face significant expenses related to the immediate breach response, if an attacker got unauthorised access to such data. Legal fees and fines for violating privacy laws like HIPAA (in the U.S.) or GDPR (in the EU) can be substantial.

Reputational Damage

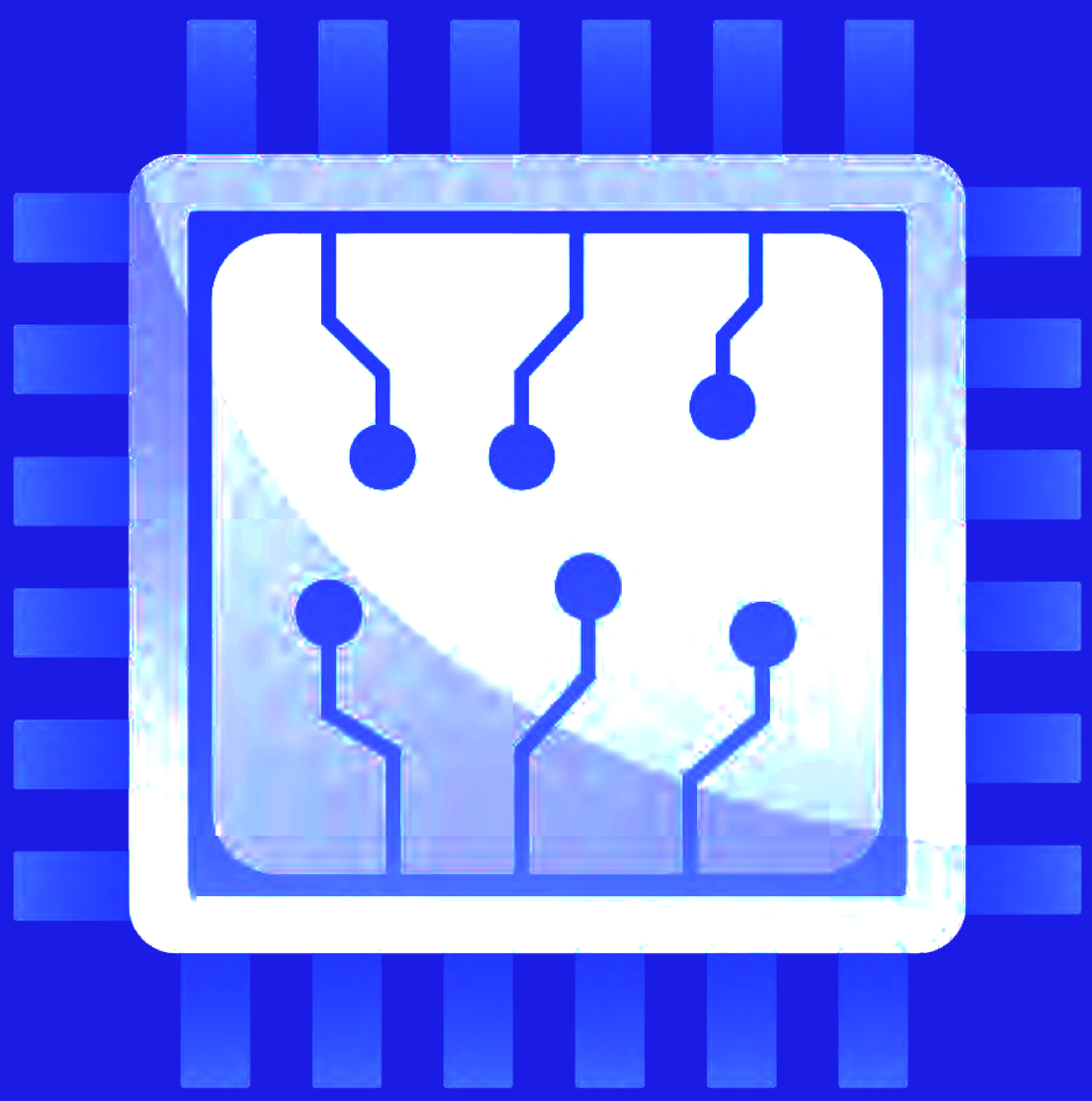
A breach can severely erode trust among patients and the public, leading to a potential decrease in patient numbers. Rebuilding the institution's reputation could take years and involve significant investment in marketing and customer service improvements.

Operational Disruption

Responding to the vulnerability and its aftermath can divert resources from everyday operations, leading to delays in patient care and possibly impacting the quality of services. This can strain resources and affect the institution’s ability to function efficiently.

Regulatory Scrutiny and Compliance Implications

Beyond immediate fines, an institution may face increased scrutiny from regulatory bodies, leading to stricter compliance requirements. This includes more frequent audits, mandatory implementation of additional security measures, and ongoing compliance costs. Non-compliance with regulations can lead to ongoing legal challenges and further financial penalties.



CONCLUSION

The average cost of a data breach in 2023 was USD **$4.45 million**. Hiring Arcus to perform penetration testing helps in proactively identifying and remediating vulnerabilities, significantly reducing the risk associated with such breaches.