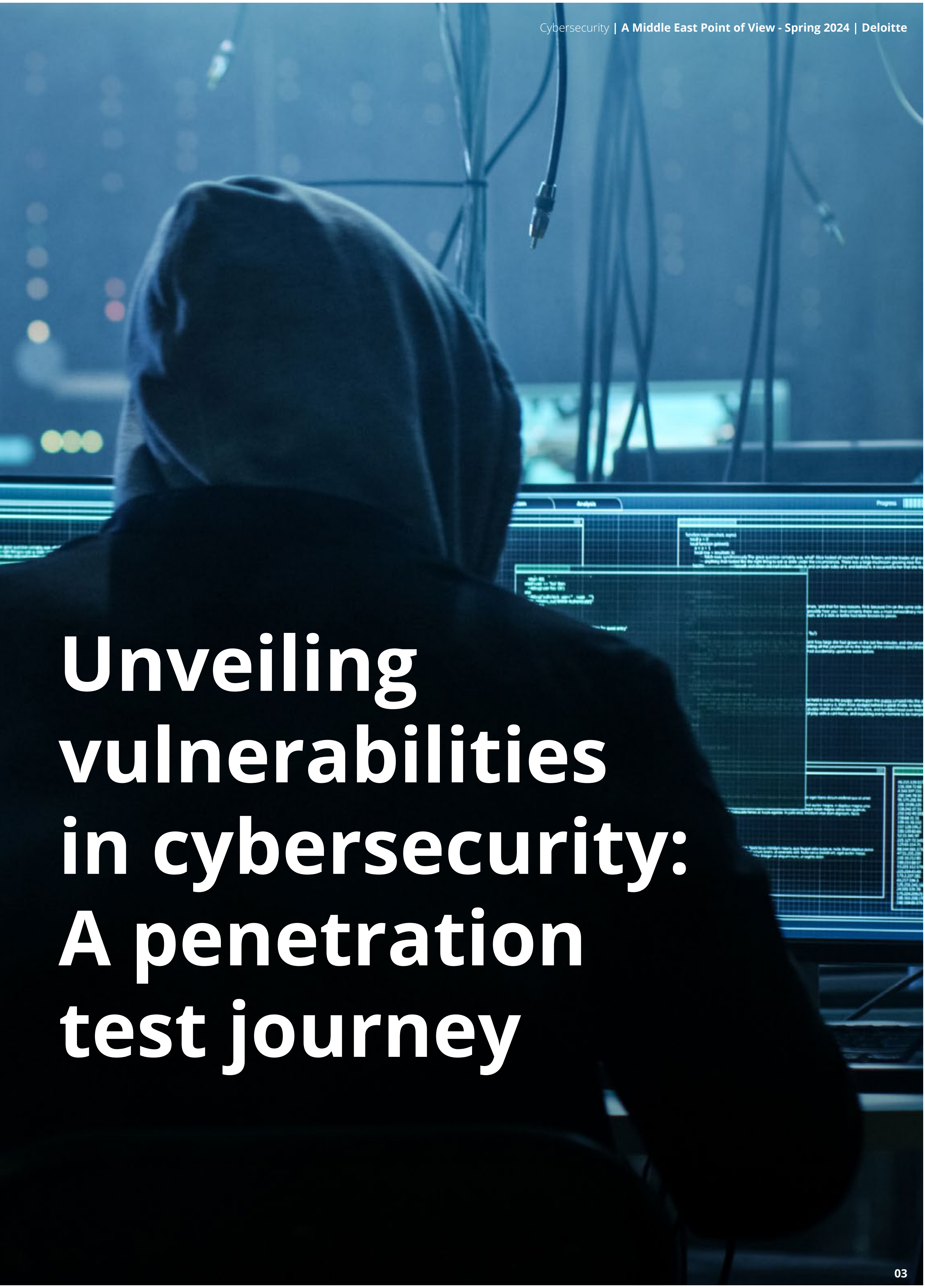

# Unveiling vulnerabilities in cybersecurity: A penetration test journey

In the realm of cybersecurity, vigilance is paramount. As technologies evolve at such a rapid pace, so too do the methods of exploitation that malicious actors can employ. In this dynamic environment, organizations must adopt proactive defense mechanisms to fortify their digital fortress against potential breaches. One such crucial defense mechanism is penetration testing, a proactive cybersecurity measure involving simulated attacks on a computer system or network to uncover vulnerabilities. This article will delve into a recent penetration test project that unveiled critical vulnerabilities, shedding light on the importance of proactive security measures in an increasingly complex digital world.

During a routine penetration test for a client, the Deloitte Middle East Cybersecurity team stumbled upon a seemingly innocuous subdomain housing a third-party application - V-QRS application from Vaales Technologies. V-QRS is a software application that lets any company create digital business cards based on Quick Response (QR) codes and Near Field Communication (NFC) systems. This system consists of a mobile app and a web-application online dashboard.

While often overlooked, such hidden corners of digital infrastructure can serve as entry points for malicious actors. Recognizing the significance of thorough examination, testing was commenced. Upon scrutinizing the subdomain, two significant vulnerabilities were discovered: Insecure Direct Object Reference (IDOR) and Structured Query Language (SQL) Injection (where malicious queries are injected into input fields, enabling attackers to manipulate the database backend). These vulnerabilities, if exploited, could grant unauthorized access to sensitive data, potentially compromising the integrity and confidentiality of the system.

In the digital landscape, IDOR (A01:2021-Broken Access Control by OWASP Top 10) remains a persistent threat. This vulnerability arises when an application fails to properly validate user access to resources. By exploiting IDOR, attackers can bypass access controls, gaining unauthorized access to restricted functionalities or data. In this case, meticulous testing revealed instances where user permissions were not adequately enforced, leaving the system susceptible to manipulation.

During our penetration test journey, we discovered a URL https://SANITIZED/user-profile/6/Da**va, where "6" serves as a sequence number, and 'Da***va' represents a full name. The link stores various details such as the individual's full name and work position (Head of Finance), phone numbers (including personal one), work email, and, although the company had opted not to publish it, a photo.

Next, the team decided to investigate the possibility of extracting additional data from the portal, specifically about its CEO. Curious, we modified the number in the request from "6" to "1." Initially, the team assumed it wouldn't work without providing the real name. However, to our surprise, the system responded positively even with a fake name, revealing information about the CEO.

Upon discovering not only an IDOR but also a misconfiguration in the application, we decided to extract data about the entire company. Using our BurpSuite setup (the application for web penetration testing), we successfully retrieved the whole company's data about employees, including their names, positions, personal phone numbers, and email addresses.

> By exploiting IDOR, attackers can bypass access controls, gaining unauthorized access to restricted functionalities or data

At first glance, it could seem innocuous as the data appeared to be "public" and intended for sharing. However, having access to such information can be exploited by black hat hackers, aka cybercriminals, for malicious purposes. This data could be used to send personalized phishing emails and phone calls, to create fake advertisements, and for overloading communication channels. Furthermore, armed with personal information, black hat hackers may attempt brute force attacks on external OWA (Outlook Web Access) and other login portals. Once inside, they could launch Active Directory login attacks, potentially causing significant harm. Further investigation revealed that the error was in 2 files. Our examination uncovered lax input validation mechanisms, paving the way for potential SQL Injection attacks.

SQL Injection (A03:2021-Injection by OWASP Top 10) stands as another formidable adversary in the cybersecurity arena. The consequences of successful exploitation range from data leakage to complete system compromise.

In our case, the previous request https://SANITIZED/user-profile/6/Da**va was quite familiar for the SQL request, where the "6" was just an ID of users table in the database, something like `SELECT * from users where id='6.'` Keeping that in mind, we attempted to put a malicious request into that field. We set up our SQLmap application and got a blind SQL injection. After a reconnaissance, we were able to extract the database username and password's hash which were used in further penetration test actions.

Armed with our findings, we swiftly reported the vulnerabilities to MITRE CVE (the organization that stores a dictionary of publicly known "cybersecurity vulnerabilities and exposures" that provides a standardized naming convention for identifying and tracking security vulnerabilities), an essential step in fostering transparency and collaboration within the cybersecurity community. Subsequently, we were provided with 2 CVE numbers: CVE-2024-24312 (SQLi) and CVE-2024-24313 (IDOR), facilitating the dissemination of critical information to stakeholders and enabling expedited remediation efforts.

The journey through this penetration test project underscored the ever-present need for proactive cybersecurity measures. By vigilantly identifying and addressing vulnerabilities, organizations can fortify their defenses against emerging threats. Collaboration, transparency, and swift action are the cornerstones of effective cybersecurity, ensuring a resilient digital ecosystem for all. ●

By **Ali Khan**, Partner, Risk Advisory and **Ivan Glinkin**, Senior Manager, Infrastructure Security, Deloitte Middle East

By vigilantly identifying and addressing vulnerabilities, organizations can fortify their defenses against emerging threats

**References**
1. https://www.cve.org/CVERecord?id=CVE-2024-24312.
2. https://www.cve.org/CVERecord?id=CVE-2024-24313.
3. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/04-Testing_for_Insecure_Direct_Object_References.
4. https://owasp.org/www-community/attacks/SQL_Injection.
5. https://v-qrs.com/.