MOORE

AUGUST 2023

MOORE NEWSLETTER

Protect Your Business From Cyber Threats – How Does Penetration Testing Help?

In recent years, data breaches have become more common and sophisticated, affecting organisations of all sizes and industries. Cybercriminals are constantly evolving their tactics and techniques, making it challenging for organisations to keep up with the ever-changing threat landscape. Among different methods, penetration testing provides one of the most real-world and effective approaches to protect a company from cyber threats.

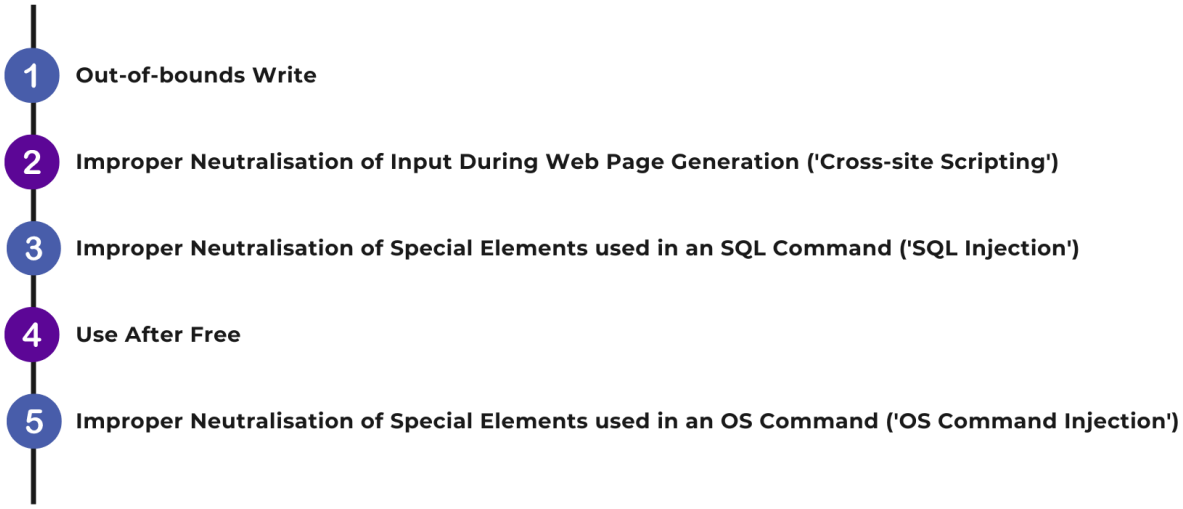
Penetration testing, or pentesting for short, simulates real-world attacks against a network, applications, or infrastructure to identify security weaknesses that could be exploited by malicious actors. The **OWASP Top 10**, **CWE Top 25**, and **CVE** are some of the most famous security frameworks that help pentesters identify potential security weaknesses and validate their existence. In the following sections, we will delve further into each of these security frameworks and how pentesters utilise them in penetration testing.

The OWASP Top 10 is a list of the most critical web application security risks. It is maintained by the Open Web Application Security Project (OWASP), a non-profit organisation dedicated to improving web application security. It provides pentesters with insights into potential vulnerabilities during penetration testing. The OWASP Top 10 for 2023 includes:

In a practical penetration testing scenario, the OWASP Top 10 is often one of the most common scopes of testing. Pentesters consider the OWASP Top 10 to identify potential risks relevant to the target application. They assess whether the application might be vulnerable to any of the listed issues. Testing methodologies and strategies are then employed to assess the presence of vulnerabilities identified in the OWASP Top 10. For example, pentesters might use manual code review, automated scanning tools, or a combination of both to identify vulnerabilities like injection flaws, broken authentication, or insecure direct object references.

CWE (Common Weakness Enumeration) is a community-developed list of the most common software and hardware security weaknesses. Unlike the OWASP Top 10, which focuses on web applications, CWE provides a standardised way to identify and categorise weaknesses in software applications and systems. CWE entries typically include a unique identifier, a description of the weakness, and information about how to address the weakness. The top 5 of the 2023 CWE Top 25 Most Dangerous Software Weaknesses are:

The top 5 of the 2023 CWE Top 25 Most Dangerous Software Weaknesses



Similar to the OWASP Top 10, the CWE Top 25 is often used as a scope of testing. Pentesters map the weaknesses identified in the CWE Top 25 to possible testing scenarios, design test cases and methodologies based on the weaknesses listed in the CWE Top 25. They create specific tests or use appropriate tools to identify vulnerabilities associated with the weaknesses, such as input validation flaws, insecure storage, or privilege escalation. After exploitation and verification, the CWE can also be used in the reporting stage. The CWE list provides detailed explanations of the weaknesses, their potential impact, and recommended mitigation strategies. Pentesters can provide recommendations and assist clients in prioritising security improvements and implementing appropriate remediation measures.

Last but not least, CVE stands for Common Vulnerabilities and Exposures. CVE and CWE are both maintained by MITRE Corporation, a non-profit organisation that operates federally funded research and development centers, but they serve different purposes. In short, CVE is a database of vulnerabilities that can be viewed by the public. When a new vulnerability is discovered, it is assigned a CVE ID and added to the CVE database. This allows security researchers and vendors to reference the vulnerability by its CVE ID, making it easier to track and manage vulnerabilities across different products and versions.

In vulnerability scanning, a pentester may manually or automatically inspect the currently installed version of every software component and check if it matches any known vulnerabilities listed in the CVE database. For example, if a system is running a version of a web server that is known to have a remote code execution vulnerability (CVE-2023-1234), the pentester can verify if the vulnerability is present by attempting to exploit it or by using proof-of-concept (PoC) code provided by the security community.

By leveraging the information provided by the OWASP Top 10, CWE Top 25, and CVE, pentesters can conduct thorough and comprehensive assessments of an organisation's security posture. These frameworks serve as valuable references for identifying and validating potential vulnerabilities, weaknesses, and exposures. Pentesters can then provide actionable recommendations to improve security and mitigate risks.

It is important to note that the security landscape is constantly evolving, and new vulnerabilities and weaknesses are continuously being discovered. Staying up to date with the latest versions of these frameworks and regularly monitoring security advisories and updates is crucial to ensure the effectiveness of penetration testing efforts and the overall security of an organisation.

Moore IT & Cybersecurity Services

Why work with us?

We are a global advisory network, with offices and member firms across the globe. Backed by our international network, we provide clients with comprehensive cybersecurity solutions and expertise from security vulnerability assessment to system penetration testing to protect them from modern cyber threats.

Our team is composed of professionals with practical and solid knowledge and experience. They are certified holders or members of professional bodies such as CISA, CISM, CRISC, CISSP, CIPP(A), CEH, OSCP and GPEN.

Our clients range from SME to listed companies from wide variety of industry, and public sector including government bureau and authorities. Through our extensive sector knowledge, we provide comprehensive advice to suit each client's goals.

Our IT & Cybersecurity Service Team

PATRICK ROZARIO
Managing Director

T +852 2738 7769
E patrickrozario@moore.hk

KEVIN LAU
Principal

T +852 2738 4631
E kevinlau@moore.hk

Follow us on social media @moorehongkong

MOORE

www.moore.hk