APPLICATION PENETRATION TEST CHECKLIST

Prepared by HANIM EKEN

https://ie.linkedin.com/in/hanimeken

1. **Is the objective of the penetration test to identify vulnerabilities in the application's security controls?**

   Yes No N/A

2. **Has the scope of the penetration test been clearly defined, specifying the applications and components to be tested?**

   Yes No N/A

3. **Is a systematic and structured methodology, such as OWASP Testing Guide, being followed during the penetration test?**

   Yes No N/A

4. **Does the penetration test include various testing types, such as black-box, white-box, and gray-box testing?**

   Yes No N/A

5. **Are critical assets, such as sensitive data, authentication mechanisms, and key functionalities, being targeted in the penetration test?**

   Yes No N/A

6. **Are both automated and manual testing tools, including scanners, fuzzers, and ethical hacking techniques, being used?**

   Yes No N/A

7. **Is vulnerability scanning part of the penetration test, aiming to identify common vulnerabilities like SQL injection and XSS?**

   Yes No N/A

8. **Does the penetration test include manual testing to identify complex vulnerabilities that automated tools may overlook?**

   Yes No N/A

9. **Is the strength of authentication mechanisms, including password policies and multi-factor authentication, being assessed?**

   Yes No N/A

10. **Is the effectiveness of access controls and authorization mechanisms being evaluated during the penetration test?**

    Yes No N/A

11. **Is there an assessment of proper input validation to prevent injection attacks and ensure data is sanitized effectively?**

    Yes No N/A

12. **Is the security of session handling, including token management and session hijacking prevention, being assessed?**

    Yes No N/A

13. **Are security misconfigurations in the application, server, or database being identified and addressed?**

    Yes No N/A

14. **Is the use of cryptographic controls, including algorithms and key management, being reviewed during the penetration test?**

    Yes No N/A

15. **Is the error handling of the application being evaluated to ensure it does not reveal sensitive information?**

    Yes No N/A

16. **Are APIs being assessed for security, including proper authentication, authorization, and protection against common API-specific vulnerabilities?**

    Yes No N/A

17. **Will the penetration test generate a comprehensive report outlining identified vulnerabilities, their severity, and recommendations for remediation?**

    Yes No N/A

18. **Is there a plan to provide guidance and support to development teams for addressing identified vulnerabilities and improving overall security?**

    Yes No N/A

19. **Will follow-up tests be conducted to verify the effectiveness of remediation efforts and ensure that identified issues are resolved?**

    Yes No N/A

20. **Is the application being checked for compliance with relevant security standards, industry best practices, and regulatory requirements?**

    Yes No N/A

Prepared by HANIM EKEN

https://ie.linkedin.com/in/hanimeken