API PENETRATION TEST CHECKLIST

Prepared by HANIM EKEN

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

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

   Yes No N/A

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

   Yes No N/A

3. **Are critical APIs, such as those handling sensitive data and authentication, being targeted in the API penetration test?**

   Yes No N/A

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

   Yes No N/A

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

   Yes No N/A

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

   Yes No N/A

7. **Is the strength of API authentication mechanisms, including token management and API key usage, being assessed?**

   Yes No N/A

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

   Yes No N/A

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

   Yes No N/A

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

    Yes No N/A

11. **Are security misconfigurations in the API, server, or database being identified and addressed during the penetration test?**

    Yes No N/A

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

    Yes No N/A

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

    Yes No N/A

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

    Yes No N/A

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

    Yes No N/A

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

    Yes No N/A

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

    Yes No N/A

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

    Yes No N/A

19. **Does the API penetration test assess the API's resilience against common cyber threats and attack scenarios?**

    Yes No N/A

20. **Is social engineering testing part of the API penetration test, evaluating susceptibility to phishing or other manipulation attempts?**

    Yes No N/A

Prepared by HANIM EKEN

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