1. Restrictions on what validated clients are permitted to do are regularly not legitimately authorized. – Ans. a
2. Broken Access Control
3. Injection
4. Security misconfiguration
5. It is a prevention which enables the content security policy (CSP) is a resistance. – Ans. c
6. Injection
7. Insufficient Logging & Monitoring
8. Cross-Site Scripting
9. It can be utilized to perform an attack including a replay, infusion and benefit escalation attack. – Ans. c
10. Broken Authentication
11. XML External Entities
12. Insecure Deserialization
13. Automated scanners are highly needed for identifying these defects. – Ans. B
14. Insufficient Logging & Monitoring
15. Security Misconfiguration
16. Injection
17. Example of prevention that removes unused conditions, superfluous highlights, segments, records and documentations. – Ans. A
18. Components with Known Vulnerabilities
19. XML External Entities
20. Insecure Deserialization
21. TRUE OR FALSE – F

XSS stands for Extreme-Site Scripting.

1. TRUE OR FALSE – T

Example of broken authentication – It implements the feeble secret work check

1. TRUE OR FALSE – T

Injection defect are NoSQL, OS, LDAP and SQL

1. TRUE OR FALSE – F

XML External Entities has numerous XML processors assess outside elements

1. TRUE OR FALSE – F

Broken access control disables web client registry posting and guarantee document metadata