1. Some applications blindly trust other frameworks which makes the SQL calls vulnerable.
2. Broken Authentication
3. Sensitive Data Exposure
4. Injection
5. None of the Above

Answer: C

1. It occurs when data is used to abuse the logic of an application and this data are untrusted one.
2. Insecure Deserialization
3. Injection
4. Insufficient logging and monitoring
5. Security Misonfiguration

Answer: a

1. A student went to a computer shop and visited every single social media site he has. He was having a great time until he realizes that it was 5 minutes before his next class starts. Scared of having his class card dropped, he closed his browser without logging out his social media accounts. An hour later, another person rented the same PC, opened the browser and had seen the social media accounts of the student. Hopefully that this random person is good to logout all of the accounts.
2. Security Misconfiguration
3. Broken Access Control
4. Injection
5. Broken Authentication

Answer: d.

1. This occurs when the Security setting was defined, implemented, and retained as defaults. Attackers will easily exploits the website in this case
2. Security Misconfiguration
3. Cross-Site Scripting
4. XML External Entities
5. None of the above

Answer: a

1. It is a kind of hacking particularly in websites by doing injection attack which the attackers exploits the vulnerability of the site to attack the visitors of the site.

a. Injection

b. Broken Authentication

c. Using components with unknown vulnerabilities

d.None if the above

Answer:d

1. These components are largely used by a companies such as Google Analytics, jQuery, kiosked, dojo,nojo and other third party components that present an increased security risk that needs to be understood and managed.
2. Using components with vulnerabilities
3. Insecure Deserialization
4. Security Misconfiguration
5. None of the above

Answer: a

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  is a vulnerability that occurs whenever a web application does not properly protect sensitive information from being revealed to illegitimate users.

a. Injection

b. Sensitive Data Exposure

c. Security Misconfiguration

d.Broken Authentication

Answer: b

1. An open source project forum software run by a small team was hacked using a flaw in its software. The attackers managed to wipe out the internal source code repository containing the next version, and all of the forum contents.
2. Insufficient Logging and Monitoring
3. XML External Entities
4. Injection
5. None of the Above

Answer: a

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks
2. Cross-Site Scripting
3. XML external entities
4. Injection
5. None of the above

Answer:b

1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_is useful in businesses and inother organizaion,like it is easier to maintain a proper communication channel between potential customers and the business organization
2. Programming Language
3. Android
4. Web Application
5. Desktop Application

Answer: d