Name: _____ Date: _____

OWASP Top Ten 2017

1. When important events are not logged or logs of applications and APIs are not monitored for suspicious activities.	A. Cross-Site Scripting
2. Occurs when untrusted data is sent to an interpreter as part of a command or query.	B. Injection
3. Allows attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.	C. Broken Access Control
4. Improper protection of sensitive information such as financial, healthcare, and PII.	D. Security Misconfiguration
5. Allows an attacker to interfere with an application's processing of XML data.	E. XML External Entity (XEE)
6. When an application uses unverified data in a SQL call that is access account information.	F. Sensitive Data Exposure
7. Vulnerabilities can appear at every layer of an application stack due to incorrect configurations, lack of patches, default accounts, etc that allow an attacker to gain access or knowledge of the system.	G. Broken Authentication
8. Malicious serialized data objects are sent as input to vulnerable deserialization methods in a production environment.	H. Insecure Deserialization
9. Development teams using third party libraries to speed the development process are unaware of the vulnerabilities within the third party code.	I. Logging & Monitoring
10. Client-side code injection attack	J. Vulnerable Components