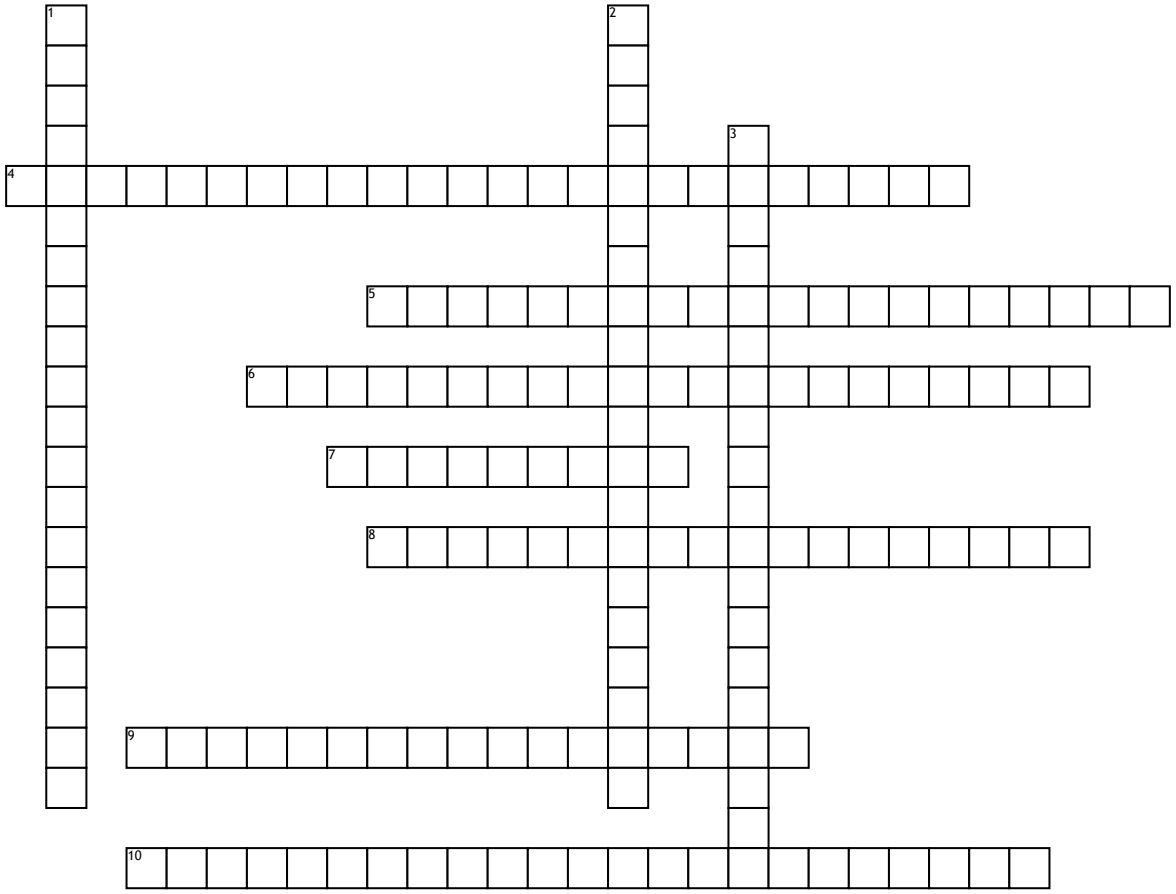
Name: _____ Date: _____

OWASP 2017 (Web)



Across

4. 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.

5. Development teams using third party libraries to speed the development process are unaware of the vulnerabilities within the third party code.

6. Improper protection of sensitive information such as financial, healthcare, and PII.

7. Occurs when untrusted data is sent to an interpreter as part of a command or query.

8. Client-side code injection attack

9. Allows an attacker to interfere with an application's processing of XML data.

10. Malicious serialized data objects are sent as input to vulnerable deserialization methods in a production environment.

Down

1. Allows attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

2. When important events are not logged or logs of applications and APIs are not monitored for suspicious activities.

3. When an application uses unverified data in a SQL call that is access account information.