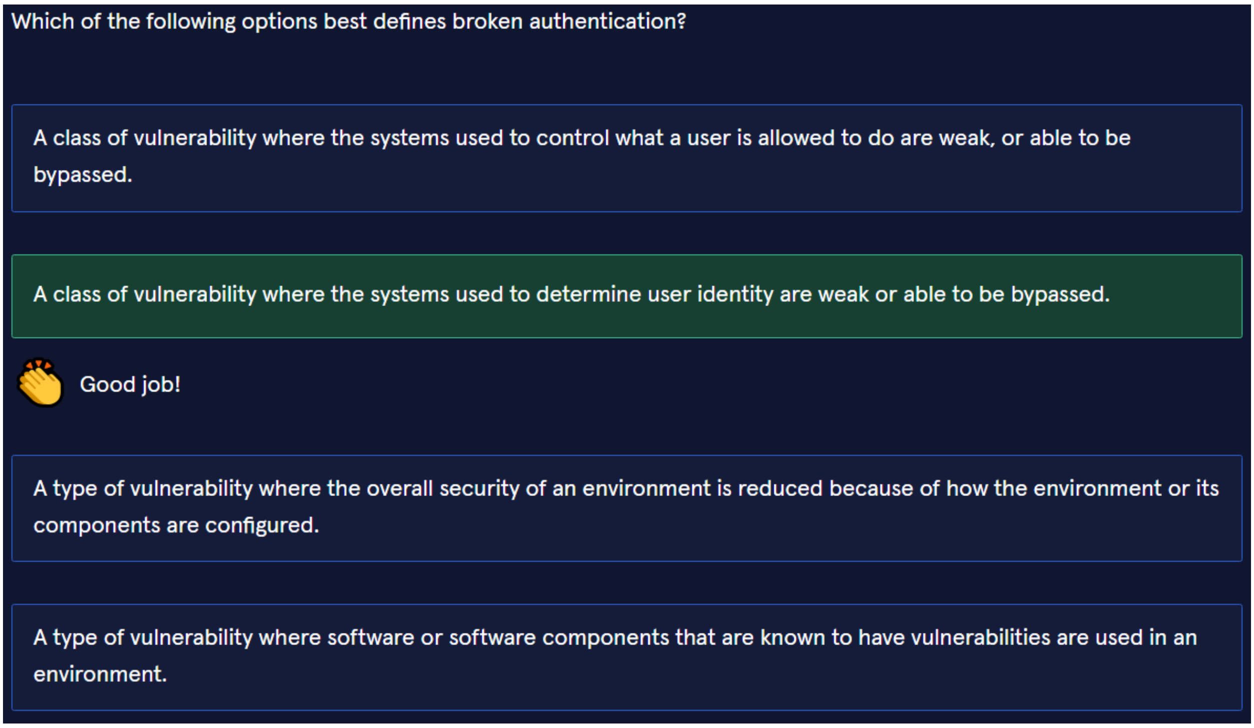
QUIZ



Which of the following options best defines broken authentication?

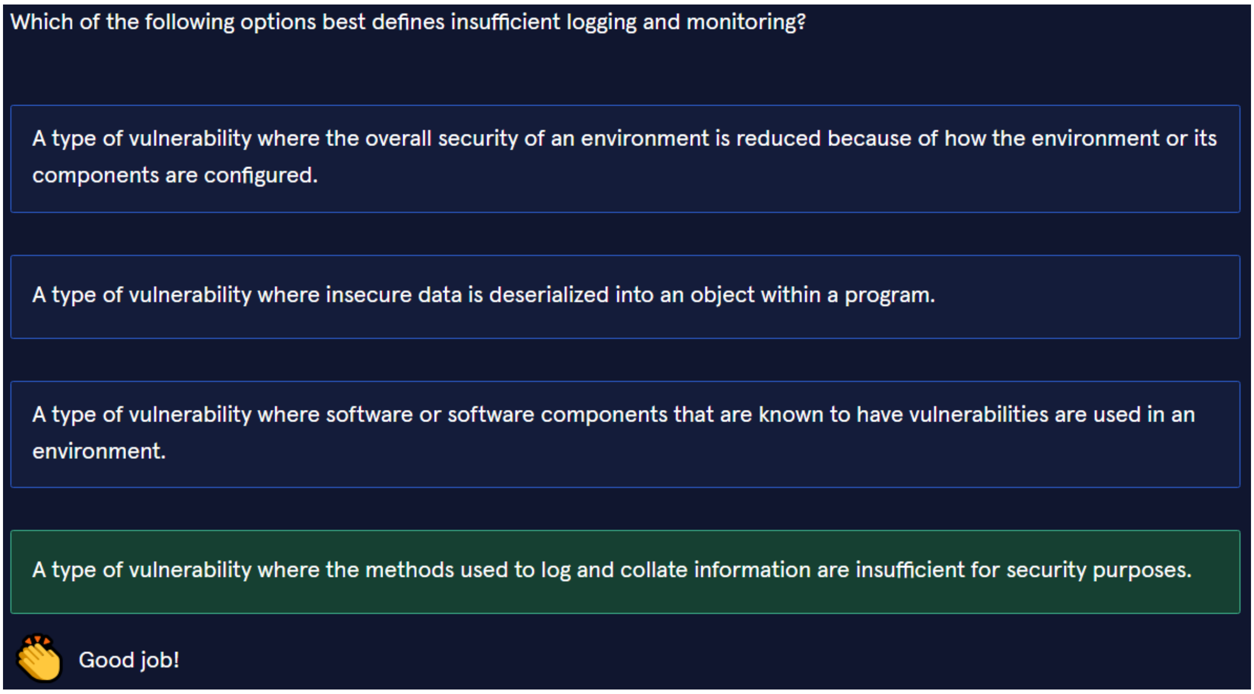
A class of vulnerability where the systems used to control what a user is allowed to do are weak, or able to be bypassed.

A class of vulnerability where the systems used to determine user identity are weak or able to be bypassed.

👏 Good job!

A type of vulnerability where the overall security of an environment is reduced because of how the environment or its components are configured.

A type of vulnerability where software or software components that are known to have vulnerabilities are used in an environment.



Which of the following options best defines insufficient logging and monitoring?

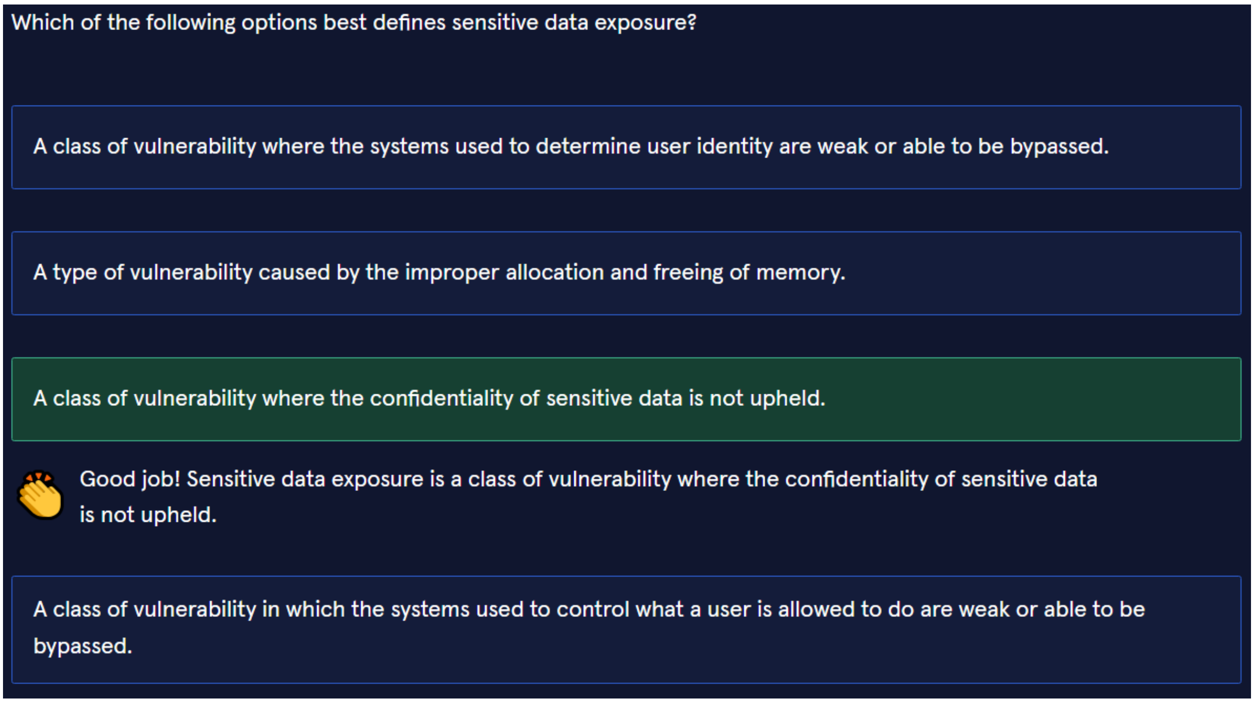
A type of vulnerability where the overall security of an environment is reduced because of how the environment or its components are configured.

A type of vulnerability where insecure data is deserialized into an object within a program.

A type of vulnerability where software or software components that are known to have vulnerabilities are used in an environment.

A type of vulnerability where the methods used to log and collate information are insufficient for security purposes.

👏 Good job!



Which of the following options best defines sensitive data exposure?

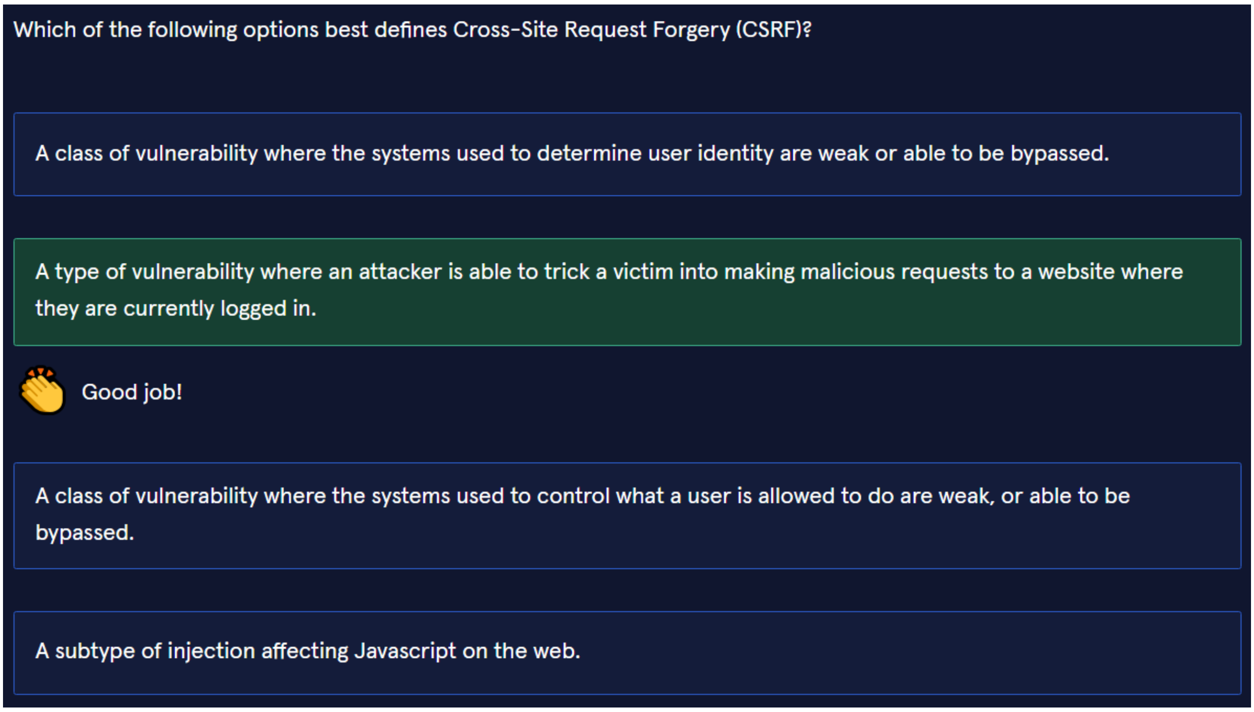
A class of vulnerability where the systems used to determine user identity are weak or able to be bypassed.

A type of vulnerability caused by the improper allocation and freeing of memory.

A class of vulnerability where the confidentiality of sensitive data is not upheld.

👏 Good job! Sensitive data exposure is a class of vulnerability where the confidentiality of sensitive data is not upheld.

A class of vulnerability in which the systems used to control what a user is allowed to do are weak or able to be bypassed.



Which of the following options best defines Cross-Site Request Forgery (CSRF)?

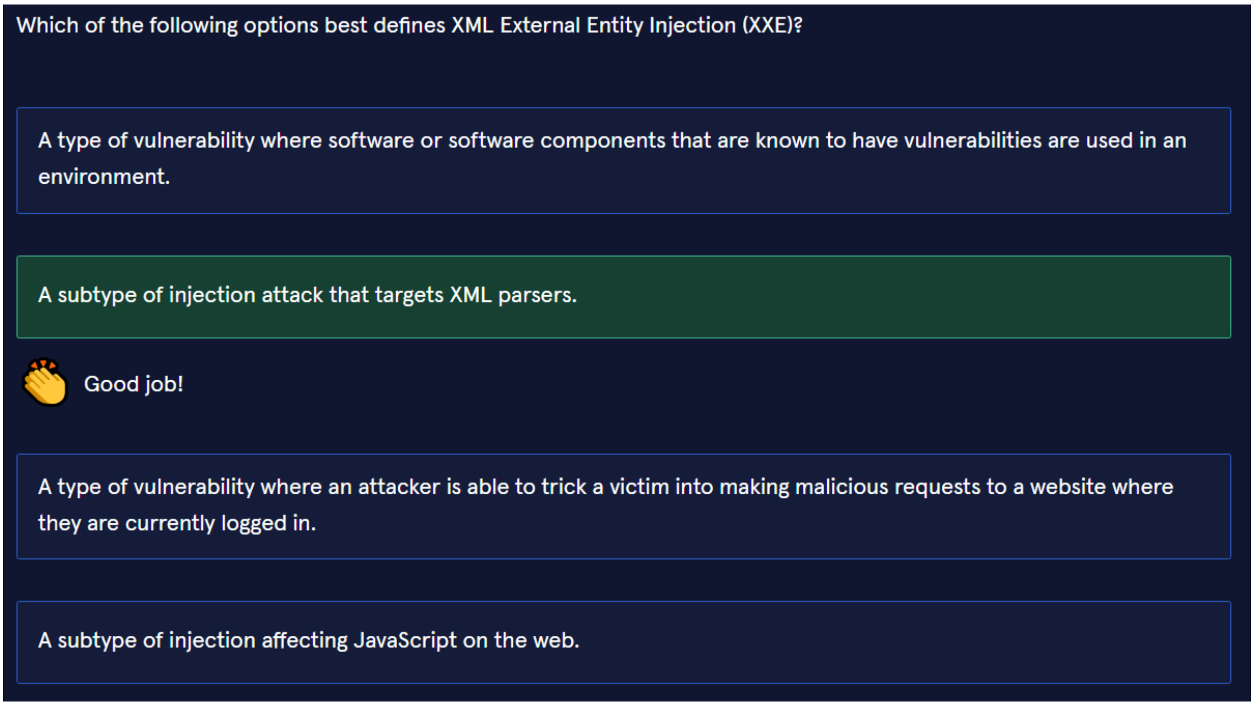
A class of vulnerability where the systems used to determine user identity are weak or able to be bypassed.

A type of vulnerability where an attacker is able to trick a victim into making malicious requests to a website where they are currently logged in.

👏 Good job!

A class of vulnerability where the systems used to control what a user is allowed to do are weak, or able to be bypassed.

A subtype of injection affecting Javascript on the web.



Which of the following options best defines XML External Entity Injection (XXE)?

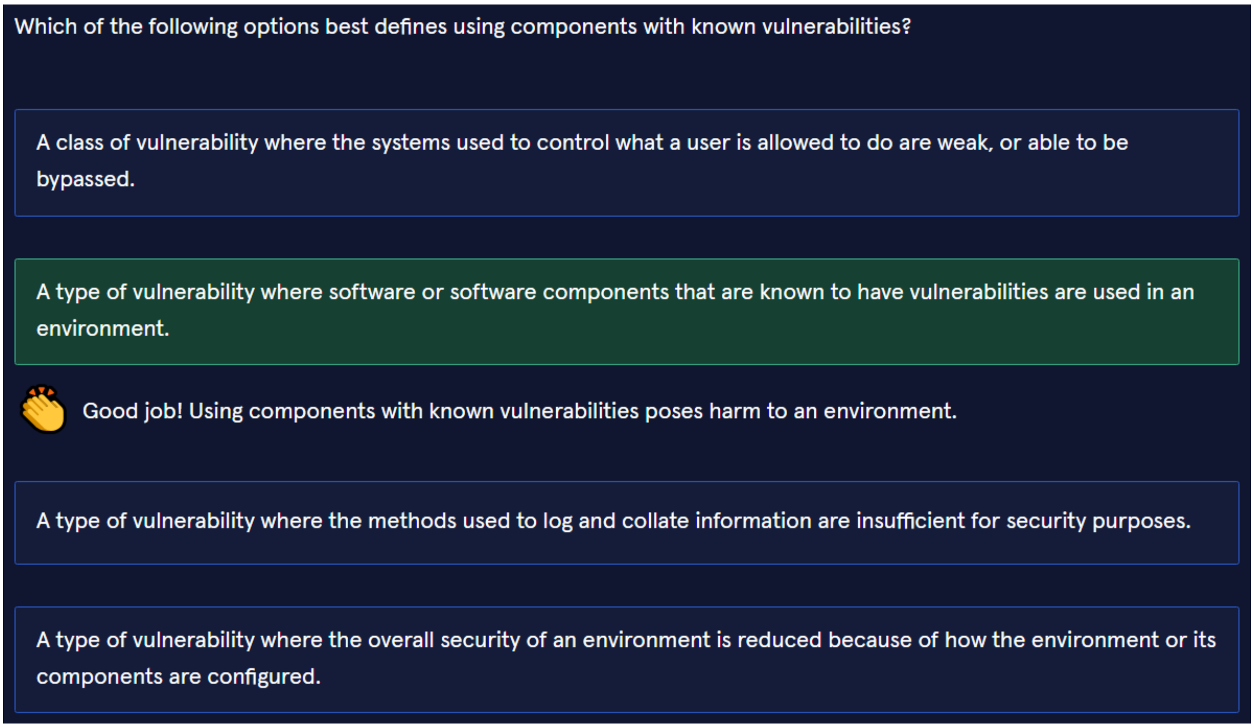
A type of vulnerability where software or software components that are known to have vulnerabilities are used in an environment.

A subtype of injection attack that targets XML parsers.

👏 Good job!

A type of vulnerability where an attacker is able to trick a victim into making malicious requests to a website where they are currently logged in.

A subtype of injection affecting JavaScript on the web.



Which of the following options best defines using components with known vulnerabilities?

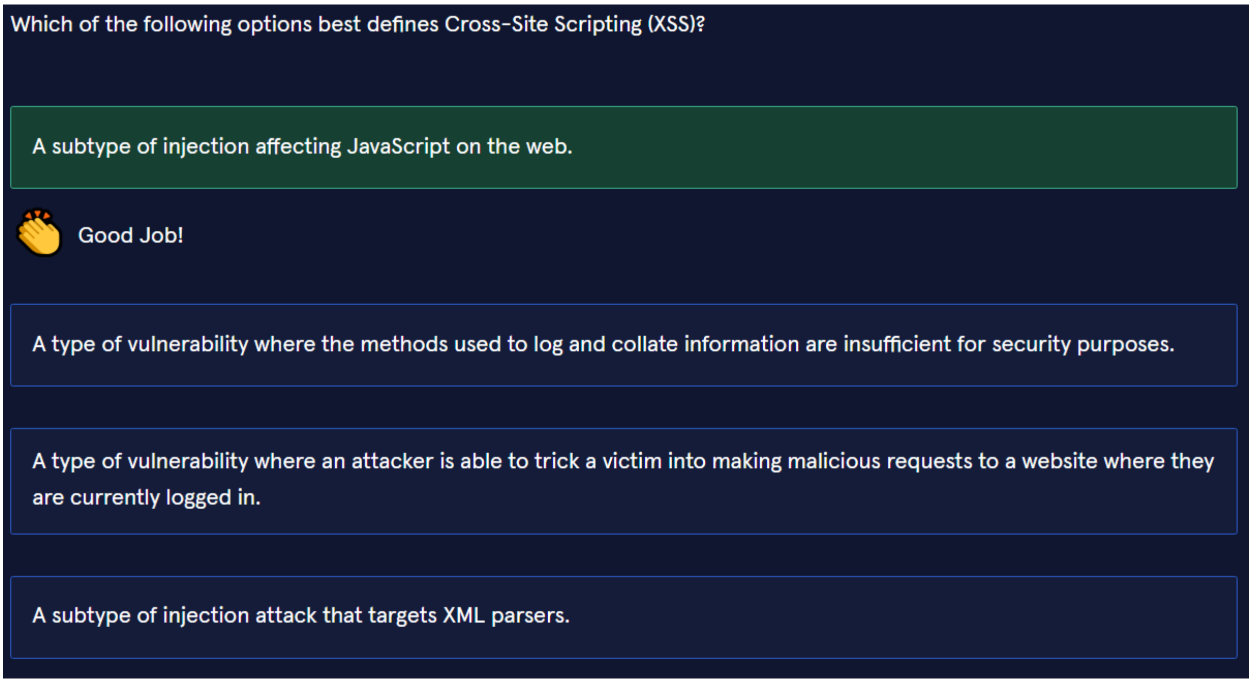
A class of vulnerability where the systems used to control what a user is allowed to do are weak, or able to be bypassed.

A type of vulnerability where software or software components that are known to have vulnerabilities are used in an environment.

👏 Good job! Using components with known vulnerabilities poses harm to an environment.

A type of vulnerability where the methods used to log and collate information are insufficient for security purposes.

A type of vulnerability where the overall security of an environment is reduced because of how the environment or its components are configured.



Which of the following options best defines Cross-Site Scripting (XSS)?

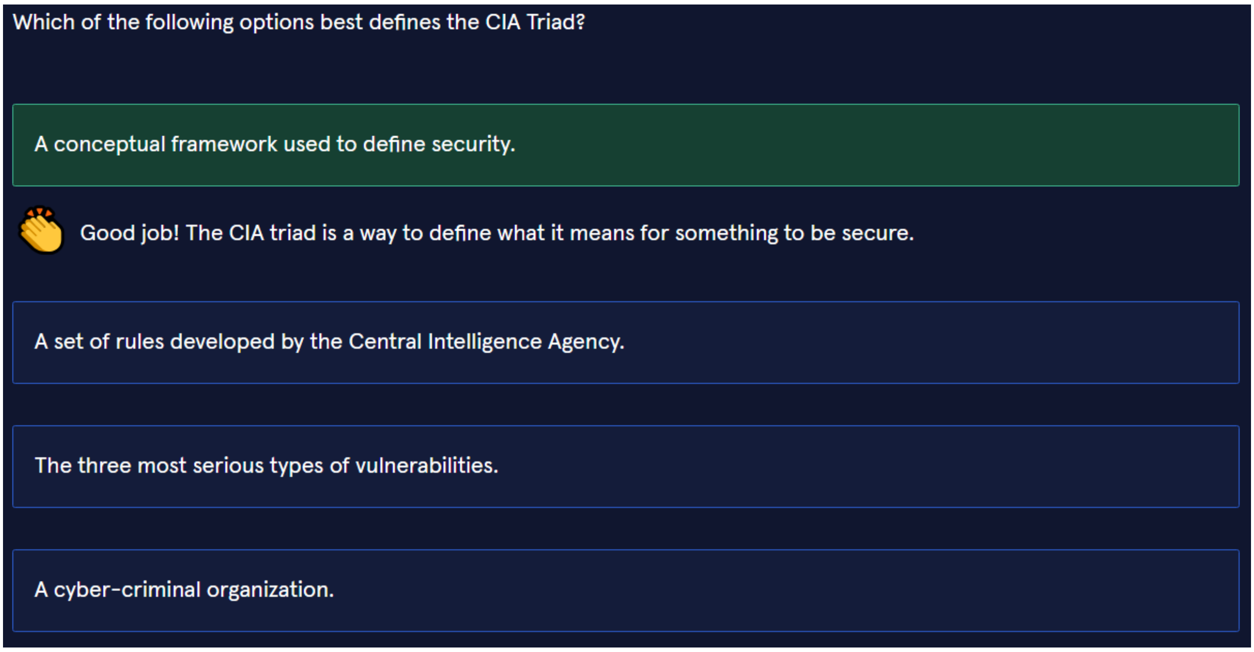
[✓ A subtype of injection affecting JavaScript on the web.]

👏 Good Job!

A type of vulnerability where the methods used to log and collate information are insufficient for security purposes.

A type of vulnerability where an attacker is able to trick a victim into making malicious requests to a website where they are currently logged in.

A subtype of injection attack that targets XML parsers.



Which of the following options best defines the CIA Triad?

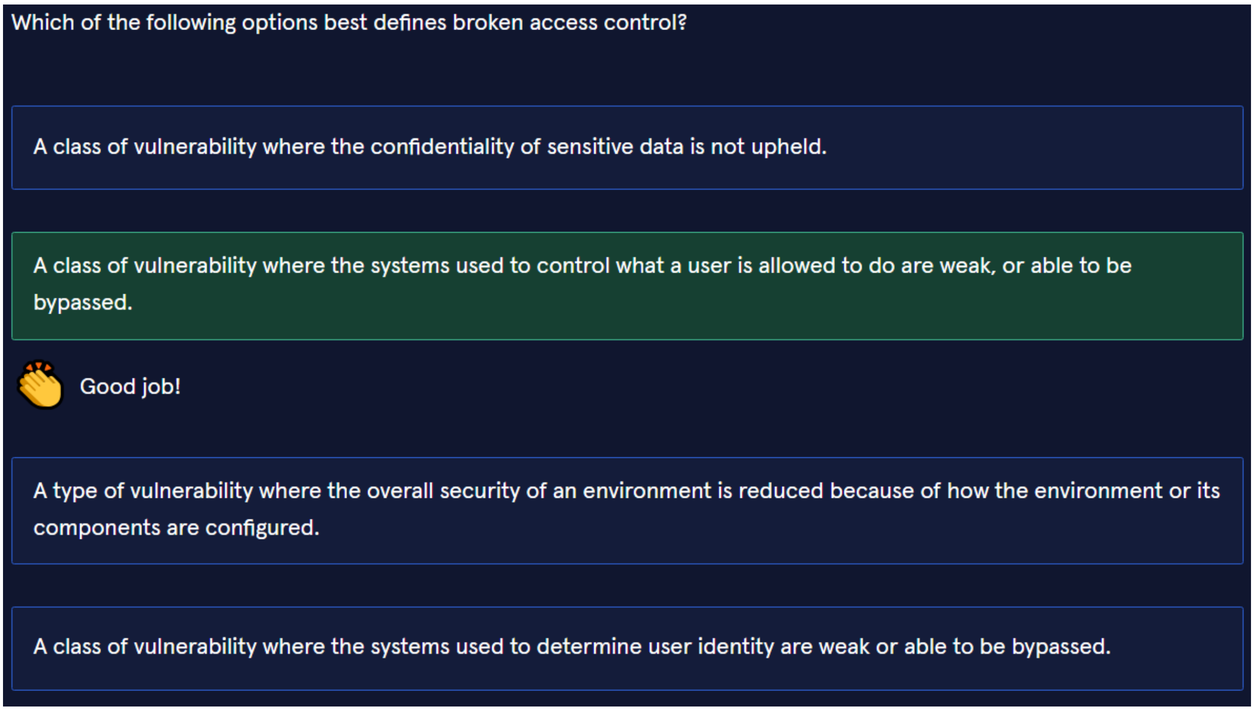
[✓ A conceptual framework used to define security.]

👏 Good job! The CIA triad is a way to define what it means for something to be secure.

A set of rules developed by the Central Intelligence Agency.

The three most serious types of vulnerabilities.

A cyber-criminal organization.



Which of the following options best defines broken access control?

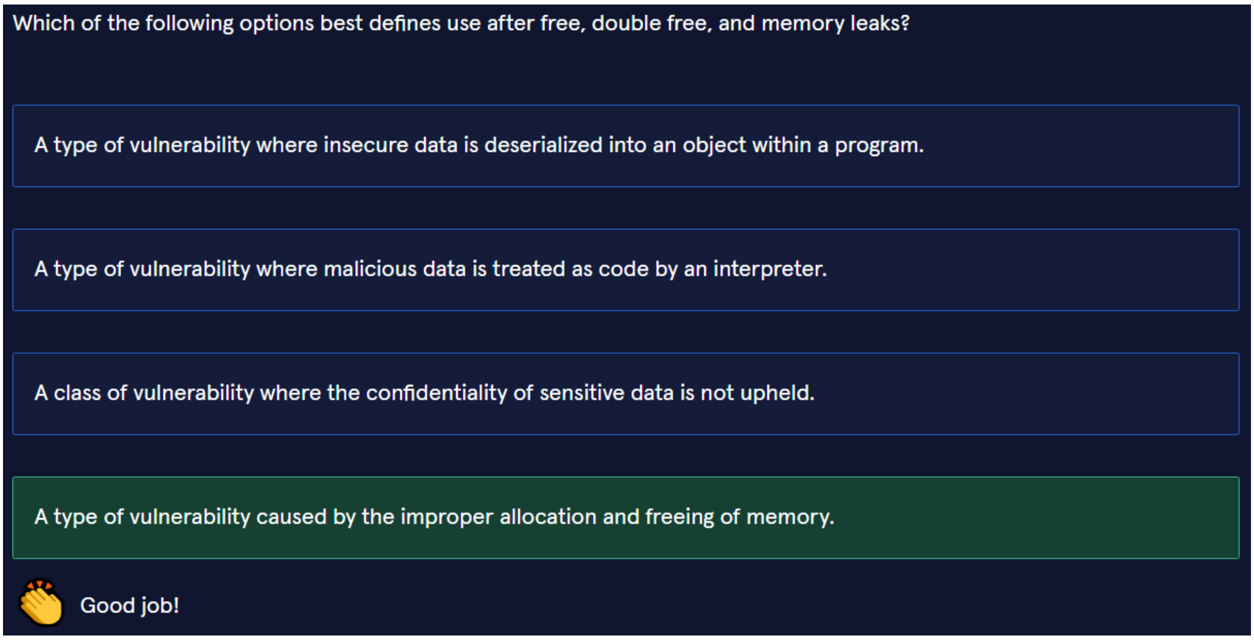
A class of vulnerability where the confidentiality of sensitive data is not upheld.

[✓ A class of vulnerability where the systems used to control what a user is allowed to do are weak, or able to be bypassed.]

👏 Good job!

A type of vulnerability where the overall security of an environment is reduced because of how the environment or its components are configured.

A class of vulnerability where the systems used to determine user identity are weak or able to be bypassed.



Which of the following options best defines use after free, double free, and memory leaks?

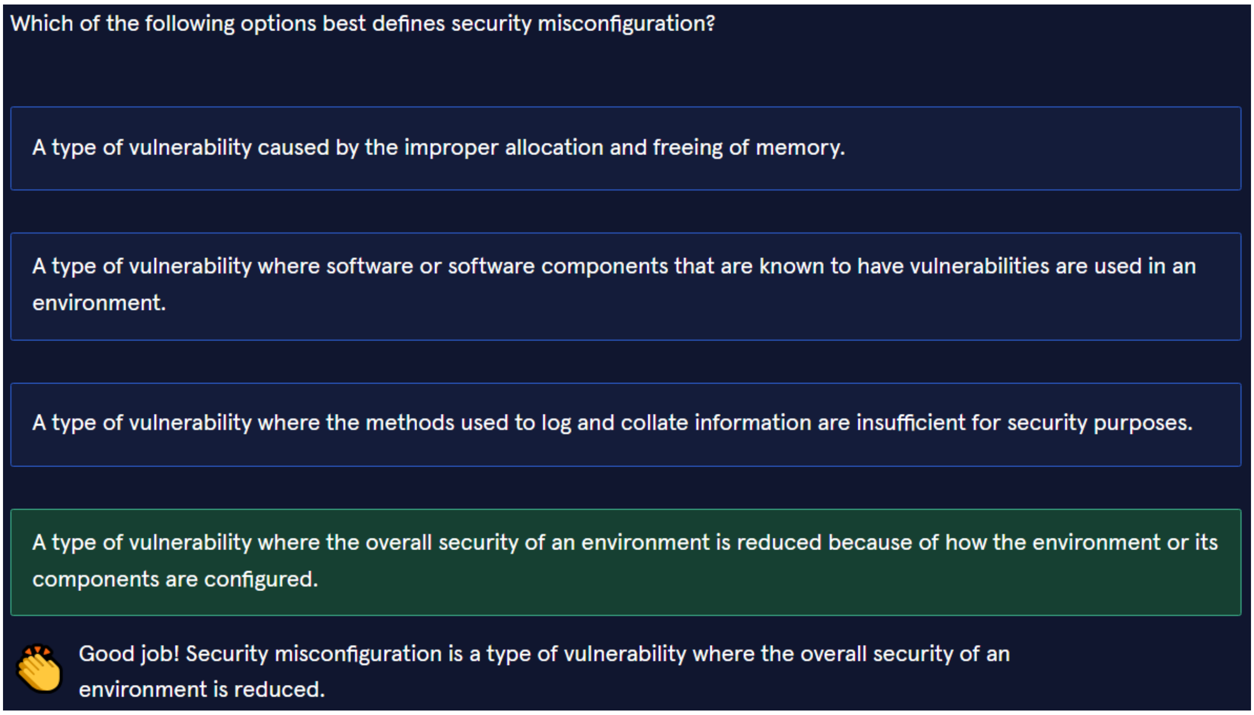
A type of vulnerability where insecure data is deserialized into an object within a program.

A type of vulnerability where malicious data is treated as code by an interpreter.

A class of vulnerability where the confidentiality of sensitive data is not upheld.

[✓ A type of vulnerability caused by the improper allocation and freeing of memory.]

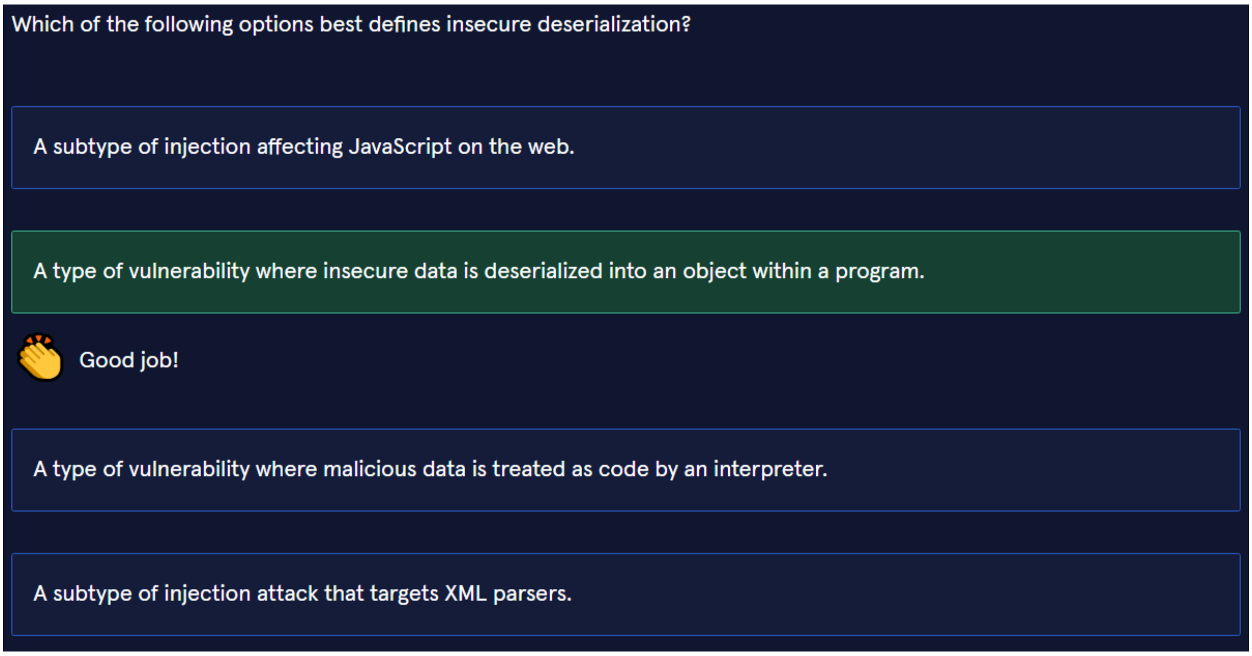
👏 Good job!



Which of the following options best defines security misconfiguration?

- A type of vulnerability caused by the improper allocation and freeing of memory.
- A type of vulnerability where software or software components that are known to have vulnerabilities are used in an environment.
- A type of vulnerability where the methods used to log and collate information are insufficient for security purposes.
- [✓ A type of vulnerability where the overall security of an environment is reduced because of how the environment or its components are configured.]

👏 Good job! Security misconfiguration is a type of vulnerability where the overall security of an environment is reduced.

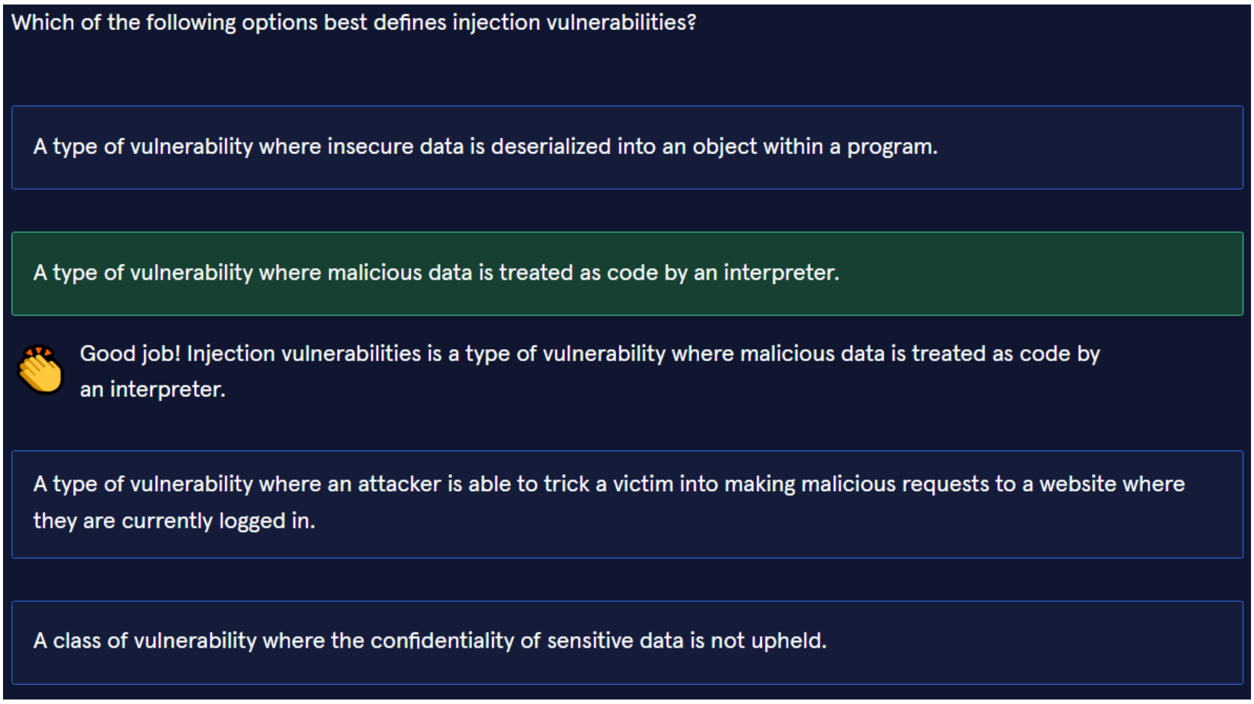


Which of the following options best defines insecure deserialization?

- A subtype of injection affecting JavaScript on the web.
- [✓ A type of vulnerability where insecure data is deserialized into an object within a program.]

👏 Good job!

- A type of vulnerability where malicious data is treated as code by an interpreter.
- A subtype of injection attack that targets XML parsers.



Which of the following options best defines injection vulnerabilities?

A type of vulnerability where insecure data is deserialized into an object within a program.

[✓ A type of vulnerability where malicious data is treated as code by an interpreter.]

👏 Good job! Injection vulnerabilities is a type of vulnerability where malicious data is treated as code by an interpreter.

A type of vulnerability where an attacker is able to trick a victim into making malicious requests to a website where they are currently logged in.

A class of vulnerability where the confidentiality of sensitive data is not upheld.