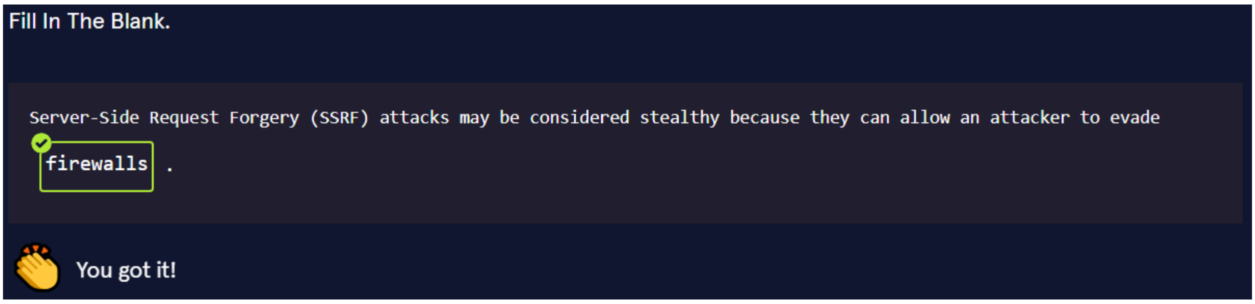
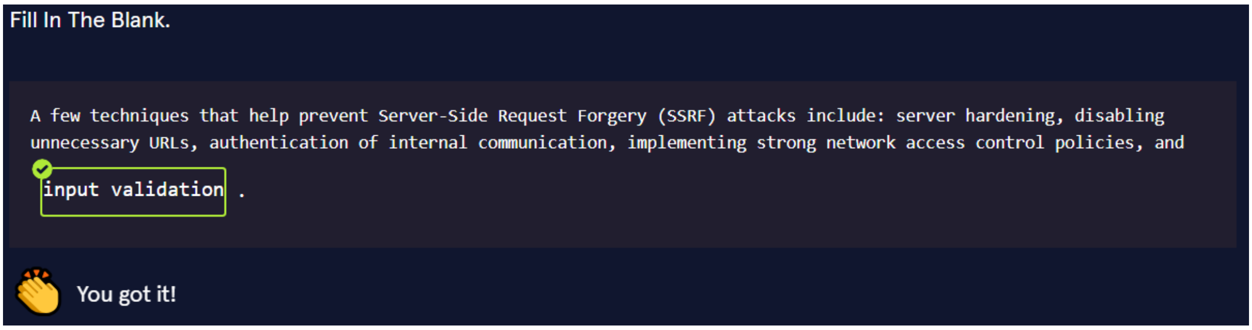
QUIZ



Fill In The Blank.

Server-Side Request Forgery (SSRF) attacks may be considered stealthy because they can allow an attacker to evade firewalls .

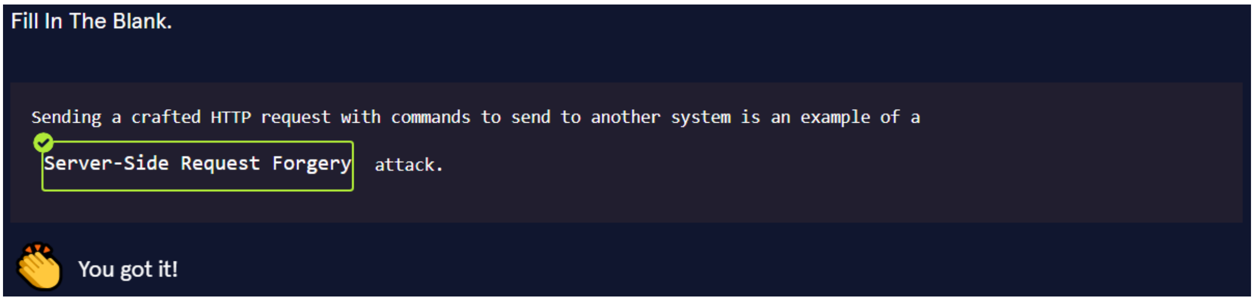
You got it!



Fill In The Blank.

A few techniques that help prevent Server-Side Request Forgery (SSRF) attacks include: server hardening, disabling unnecessary URLs, authentication of internal communication, implementing strong network access control policies, and input validation .

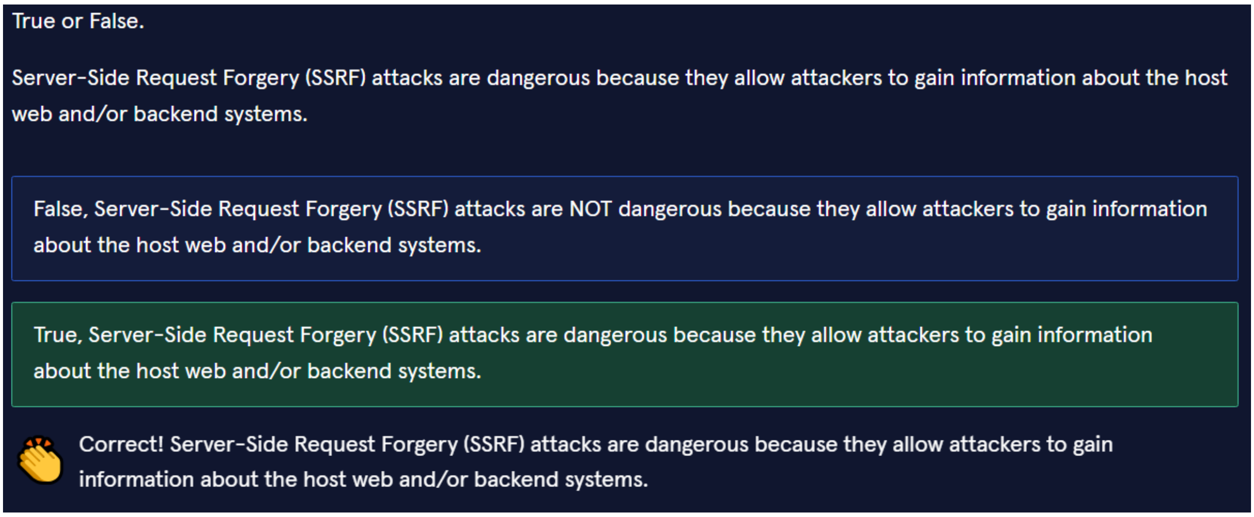
You got it!



Fill In The Blank.

Sending a crafted HTTP request with commands to send to another system is an example of a Server-Side Request Forgery attack.

You got it!



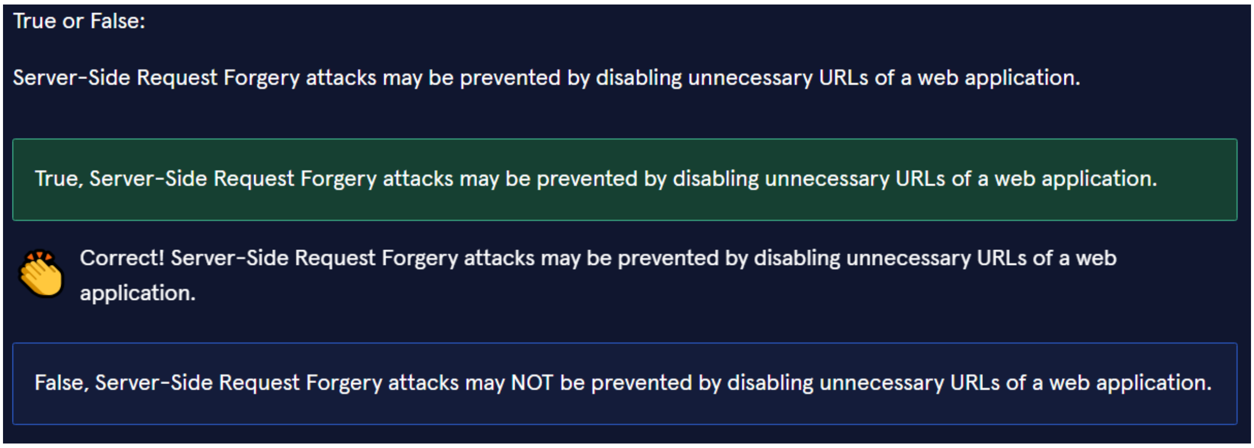
True or False.

Server-Side Request Forgery (SSRF) attacks are dangerous because they allow attackers to gain information about the host web and/or backend systems.

False, Server-Side Request Forgery (SSRF) attacks are NOT dangerous because they allow attackers to gain information about the host web and/or backend systems.

True, Server-Side Request Forgery (SSRF) attacks are dangerous because they allow attackers to gain information about the host web and/or backend systems.

Correct! Server-Side Request Forgery (SSRF) attacks are dangerous because they allow attackers to gain information about the host web and/or backend systems.



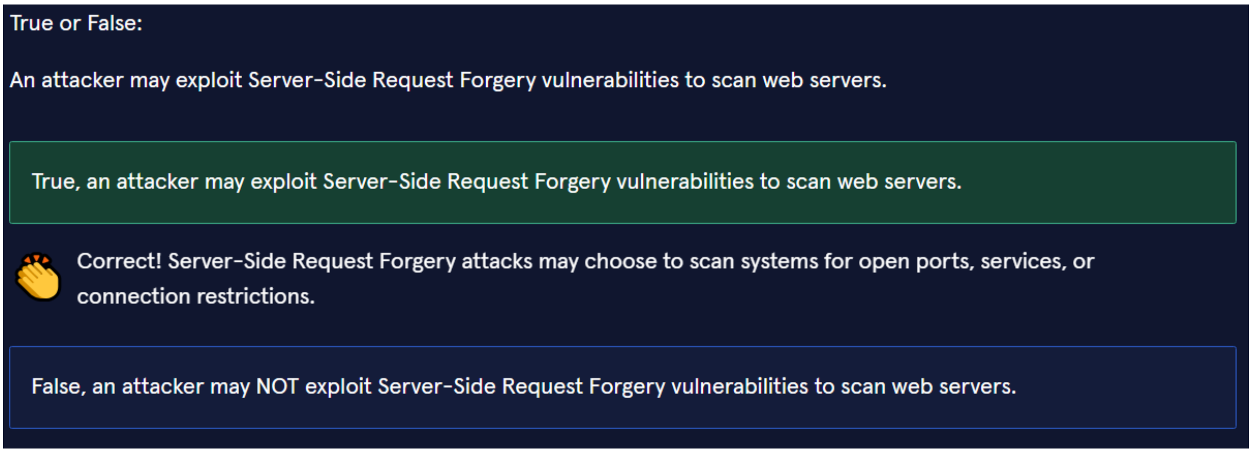
True or False:

Server-Side Request Forgery attacks may be prevented by disabling unnecessary URLs of a web application.

True, Server-Side Request Forgery attacks may be prevented by disabling unnecessary URLs of a web application.

👏 Correct! Server-Side Request Forgery attacks may be prevented by disabling unnecessary URLs of a web application.

False, Server-Side Request Forgery attacks may NOT be prevented by disabling unnecessary URLs of a web application.



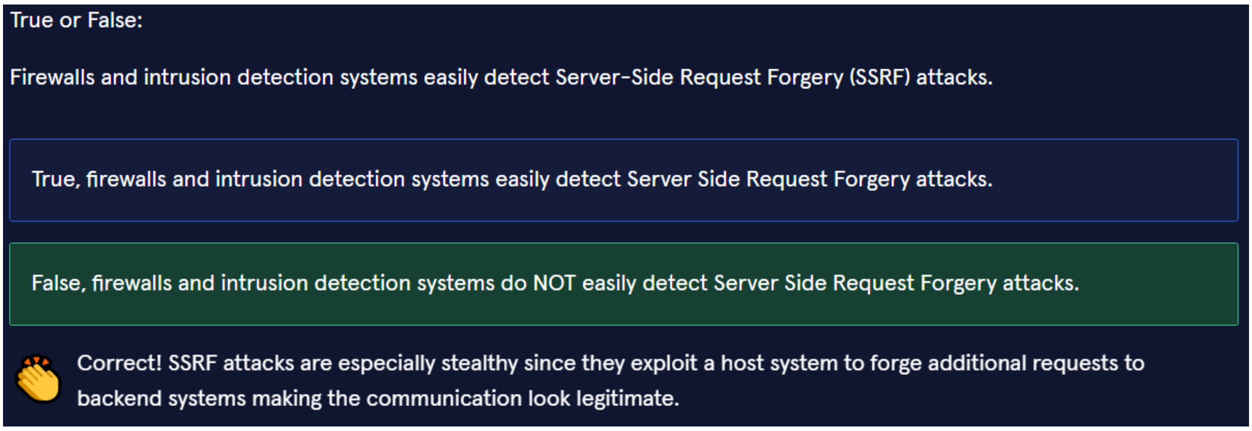
True or False:

An attacker may exploit Server-Side Request Forgery vulnerabilities to scan web servers.

True, an attacker may exploit Server-Side Request Forgery vulnerabilities to scan web servers.

👏 Correct! Server-Side Request Forgery attacks may choose to scan systems for open ports, services, or connection restrictions.

False, an attacker may NOT exploit Server-Side Request Forgery vulnerabilities to scan web servers.



True or False:

Firewalls and intrusion detection systems easily detect Server-Side Request Forgery (SSRF) attacks.

True, firewalls and intrusion detection systems easily detect Server Side Request Forgery attacks.

False, firewalls and intrusion detection systems do NOT easily detect Server Side Request Forgery attacks.

👏 Correct! SSRF attacks are especially stealthy since they exploit a host system to forge additional requests to backend systems making the communication look legitimate.