SQL injection attacks inject a SQL query into the application's client-side input data. SQL injection attacks can read and manipulate sensitive data stored in databases. SQL injection attacks involve introducing SQL commands into data in order to disrupt the execution of predefined SQL commands. (Mishra, N.D.)

A cross-site scripting attack injects data into a web application via a web request from an untrusted source. Typically, the attackers obtain private data such as cookies and session information. Redirecting the victim's attention to harmful web content. (Kingthorin, N.D.)

Traditional firewalls can't withstand many advanced cyber-attacks. Because it protects a multi-tier web application poorly. A perimeter firewall allows access to hosted sites via ports 80 and 443. Hackers use the same ports to access apps. A typical firewall can't block SQL injection or DDOS. A security solution for applications must do more than just open and close ports. (Anon,2019)

Web Application Firewall is an improved version of a regular firewall that placed in front of a web applications. It identifies suspicious network traffic and filters it. It works using a set of security rules. People think IDS heavily supports firewalls. However, they can only monitor incoming network data and cannot decode HTTP content. A WAF intercepts and analyses every HTTP request before it reaches the web app. It protects web applications from the threats. (Anon,2019)

Reference:

1. Kingthorin., (N.D), SQL Injection. available from: https://owasp.org/www-community/attacks/SQL_Injection [Accessed 8 Apr 2022]
2. Dhiraj, M., (N.D), SQL injection bypassing WAF. available from : https://owasp.org/www-community/attacks/SQL_Injection_Bypassing_WAF [Accessed 8 Apr 2022]
3. Anon., (2019) Benefits of using Web Application Firewall. Available from: https://www.inspirisys.com/blog-details/Benefits_of_using_Web_Application_Firewall/32 [Accessed 8 Apr 2022]