1. All websites are attacked anytime, anywhere, and website security is very important in order to deal with the threat of hackers. The 3 reasons why web application security is so important include:1.preventing the loss of sensitive data, 2.understanding that security is about more than just testing, and 3.security is required to maintain business reputation and minimize losses (the cost of a hacked business can be more than just financial).

（Timothy Chiu. (2022, March 19). *What is web application security and why is it important?* K2io. Retrieved May 5, 2022, from https://www.k2io.com/what-is-web-application-security-and-why-is-it-important/ ）

2. There are many kinds of vulnerabilities in websites, such as information disclosure vulnerabilities and command execution vulnerabilities. The Top 3 security vulnerabilities as per OWASP Top 3 are: 1.SQL Injection 2.Cross Site Scripting 3.Broken Authentication and Session Management

（Williams, L. (2022, March 5). *10 most common web security vulnerabilities*. Guru99. Retrieved May 5, 2022, from https://www.guru99.com/web-security-vulnerabilities.html#3 ）

3. There are many ways to protect a website, and the basic steps to improve the security of a website are:

1.Keep Software And Plugins Up-To-Date

2.Add HTTPS and an SSL Certificate

3.Choose a Smart Password

(Drew Hendricks. (n.d.). *10 essential steps to improve your website security*. IEEE Computer Society 10 Essential Steps To Improve Your Website Security Comments. Retrieved May 5, 2022, from <https://www.computer.org/publications/tech-news/trends/10-essential-steps-to-improve-your-website-security>)

4. A lot of hardware and software will be used in the process of protecting the website.

Hardware: content servers, web servers Software: Firewall