Hello Class, a good Security testing tool for applications is Zed Attack Proxy also known as ZAP. ZAP is made by Open Web Application Security Project (OWASP). ZAP is used for finding vulnerable spots in a web application. Written in Java, Zap is used as a scanner, and can also detect proxies. It is automatic scanning, and also multi-platform, and analysis the system from attacks from hackers. When the analysis is completed, it gives you a detailed review showing the risk and vulnerabilities. To download ZAP, you can go to its main website “zaproxy.org”.

OWASP ZAP – Getting Started. (2022). Retrieved 13 August 2022, from <https://www.zaproxy.org/getting-started/>

Hello Class, IIS (Internet Information Services) is already packaged in Windows and Apache is free, and IIS only runs on Windows Operating Systems, but Apache can run on different types of Operating Systems. ISS frequently patches and update to be less vulnerable to hackers and new way to exploit. IIS is also a safer option than Apache. IIS uses staff for most problems, while Apache uses the community, which means no assistance to face problems from the company. With my number one thing being safe and security I would go with IIS.

Nginx is gaining server marketing shares probably because of all the abilities it has and can do like “web serving, reverse proxying, caching, load balancing, media streaming, and more.” ("What is NGINX?", 2022) Ngnix was also made to make the fastest web server, which is important for users.

Cooper, S. (2018). IIS vs Apache - which server platform is best for you?. Retrieved 13 August 2022, from <https://www.comparitech.com/net-admin/iis-vs-apache/>

What is NGINX?. (2022). Retrieved 13 August 2022, from https://www.nginx.com/resources/glossary/nginx/

Administration

A Windows container is an operating system that is separates apps and services from others that are used by the same container host and require network connectivity, this helps the network environment run fast, with isolated apps on a single system. Windows containers share a kernel with the host, and because of this the Windows container need the same configuration. It will attach to the host network by using a network mode or driver. Windows containers are similar to Virtual machines (VMs). You can use Windows containers to deploy a Hyper-V host which is connected to a virtual network adapter, and with that you can make multiple VMs, and inside those, containers are made. Windows Containers also use “Docker as the management surface, and Windows Host Network Service (HNS) as a servicing layer to create the network “plumbing” underneath”, communicating through HNS.

Hello class, you can manage Windows container through PowerShell by running a Get-Command to see what cmdlets you can use to manage containers, typing in the command “Get-Command -Module Containers”, which displays a list off all the containers. “Start-Container”, which starts a stopped container.” "Stop-Container”, which stops a running container. “Enter- ContainerSession” or “Attach-Container”, which connects a session on a running container. “ConvertTo-ContainerImage” or “Commit-Container”, which creates a new image. “Remove-Container”, which removes a container.