**Assignment-1**

**Subject: Web and Mobile Security (20CST-333/ITT-333)**

**DOA: 25th August 2022**

**DOS: 2nd September 2022**

1. Apache Server Doesn't performs well for high traffic. Do you agree with this statement? If yes, then which web server is used as replacement? Explain.

ANS:-- yes, Apache Server Doesn't performs well for high traffic . we can use ngnix web server as replacement because [Nginx](https://www.nginx.com/), pronounced Engine-X, is a free, open-source software. Compared to Apache, it is a more recent web server application released in 2004.

Nginx was created to solve the so-called [c10k problem](https://programmersought.com/article/23585585099/), meaning that a web server that uses threads to handle user requests is unable to manage more than 10,000 connections at the same time.

1. Since Apache uses the thread-based structure, owners of high-traffic websites may encounter performance problems. Nginx is one of the web servers that address the c10k problem and probably the most successful one.
2. Nginx has an event-driven architecture that doesn’t create a new process for each request. Instead, it handles every incoming request in a single thread. This master process manages several worker processes that perform the actual processing of requests. The event-based model of Nginx distributes user requests among worker processes in an efficient way, therefore leading to much better scalability.
3. If you need to manage a high-traffic website, Nginx is an excellent choice, as it can do that by using minimal resources. It cannot be a coincidence that it’s used by many high-visibility websites such as Netflix, Hulu, Pinterest, and Airbnb.
4. However, for small and medium players, Apache comes with a handful of advantages over Nginx, such as its easy configuration, lots of modules, and a beginner-friendly environment.
5. Why Linux is considered to be more secure? Explain different security practices of LINUX.

Ans:- Linux systems are rarely infected by malware such as viruses, worms etc, thereby making it as a very secure OS. As a normal user, we will never come across a situation where Antivirus software is been sold for Linux. This means, Linux is inherently secure and there are many reasons associated with it. Let us look into the key reasons that describes why is linux more secure than other operating systems.

* Use Strong and Unique Passwords. ...
* Generate an SSH Key Pair. ...
* Update Your Software Regularly. ...
* Enable Automatic Updates. ...
* Avoid Unnecessary Software. ...
* Disable Booting from External Devices. ...
* Close Hidden Open Ports.

1. Differentiate between persistent and non-persistent HTTP protocol with an example.

Ans : The Hypertext Transfer Protocol (HTTP) is an application-level protocol that uses TCP as an underlying transport and typically runs on port 80. HTTP is a stateless protocol i.e. server maintains no information about past client requests.

Example

Suppose 10 images need to be downloaded from the HTTP server. The total time taken to request and download 10 images in a non-persistent and persistent connection is:

**Non-persistent**

2 RTT (Connection time) + 2 \* 10 RTT= 22 RTT22*RTT*

**Persistent**

2 RTT (Connection time) + 10 RTT= 12 RTT12*RTT*

1. How HTML injection and CSS attacks works? Take a website as example and explain.

Ans:- HTML injection attack is closely related to Cross-site Scripting (XSS). HTML injection uses HTML to deface the page. XSS, as the name implies, injects JavaScript into the page. Both attacks exploit insufficient validation of user input.[Cross-site Scripting (XSS)](https://www.invicti.com/learn/cross-site-scripting-xss/) is a client-side code [injection attack](https://www.acunetix.com/blog/articles/injection-attacks/). The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application. The actual attack occurs when the victim visits the web page or web application that executes the malicious code.

Example:- example website is Acunetix.com

[**Acunetix**](https://www.acunetix.com/plp/app-security-testing/?utm_medium=3rdparty&utm_source=softwaretestinghelp&utm_campaign=html-injection) Web Application Security Scanner has automation capabilities. It will let you schedule and prioritize full scans. It comes with built-in vulnerability management functionality that helps with managing the identified issues. It can be integrated with your current tracking system like Jira, GitHub, GitLab, etc.