Laboratoriumsübungen

Schuljahr: 2024/25		**Name**: Noah Aichhorn
Lehrgang: 2		**Klasse**: 3a APC
Übungstag: 14.11		**Gruppe**: A

1. Aufgabe

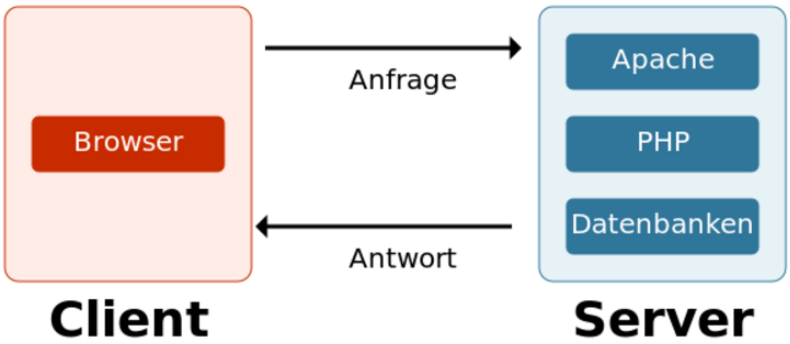
Vorlage

1. Aufgabenstellung

- Kommunikationsablauf – Webserver und Client/Browser
- Installation Entwicklungsumgebung (Webserver+PHP+MySQL/MariaDB - oder Alternative und ein Editor mit PHP Support)
- Sicherheitsrisiken von Webanwendungen (Phishing, Datendiebstahl, SQL Injections, Cross-Site-Scripting, Session-Hijacking, DoS, ...)
- Maßnahmen zum Schutz von Webanwendungen (Verschlüsselung, Multifaktor Authentifizierung, Sanitizing/Prepared Statements,...)

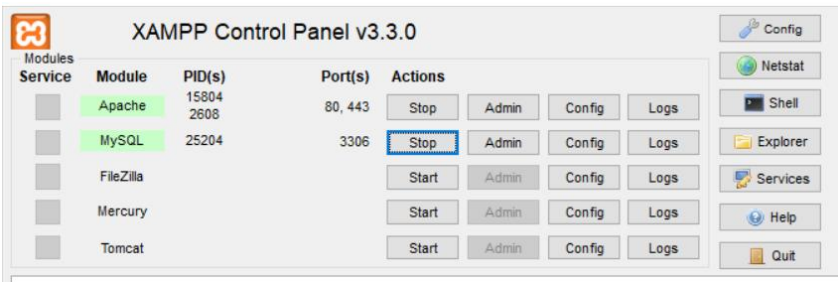
2. Lösung

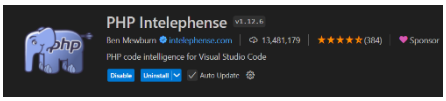
Kommunikation



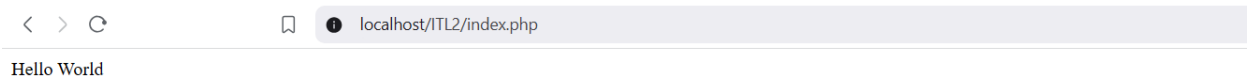
Der Code arbeitet nur, wenn es vom Client eine Anfrage gibt. Die Antwort ist dann das Ergebnis, das durch die Verarbeitung der Daten des Clients herauskommt.

Installation






```php
<?php
    echo "Hello World"
?>
```



Hello World

Xampp Server starten und erste PHP-Datei erstellt. Zum Bearbeiten der PHP-Datei verwende ich hier VS Code mit einer PHP-Extension.

Sicherheitsrisiken

Webanwendungen sind verschiedenen Sicherheitsrisiken ausgesetzt, darunter Phishing-Angriffe, bei denen Nutzer zur Preisgabe sensibler Daten verleitet werden, und Datendiebstahl, der auf die unbefugte Entnahme von Informationen abzielt. Weitere Risiken umfassen SQL-Injection- und Cross-Site-Scripting-Angriffe (XSS), die Schwachstellen in der Datenbank und im Browser ausnutzen, sowie Session-Hijacking und Denial-of-Service-Angriffe (DoS), die dazu führen können, dass Sitzungen übernommen oder der Dienst blockiert wird.

Mögliche Maßnahmen

Zum Schutz von Webanwendungen können verschiedene Maßnahmen implementiert werden, wie etwa die Verschlüsselung von Daten zur Sicherstellung der Vertraulichkeit und die Nutzung von Multifaktor-Authentifizierung zur Verbesserung der Zugangssicherheit. Zudem hilft das "Sanitizing" von Eingaben sowie die Verwendung von Prepared Statements, SQL-Injection-Angriffe abzuwehren und die Integrität der Daten zu gewährleisten.