201P Computer Network, Winter 2020

SQL Injection Attack: Web server, LAMP, PHP, SQL, SQL Injection

28 February 2020

Aftab Hussain
University of California, Irvine

Web Server

INTRO

A **web server** is server software, or hardware dedicated to running this software.

Satisfies client requests on the World Wide Web.

Can contain one or more websites.

Processes incoming network requests over HTTP and several other related protocols.

The primary function of a web server is to store, process and deliver web pages to clients.[1]

Pages delivered are most frequently HTML documents, which may include images, style sheets and scripts in addition to the text content.

A user agent, commonly a web browser or web crawler, initiates communication by making a request for a specific resource using HTTP

The server responds with the content of that resource or an error message if unable to do so.

Web Server

What is it?

A **web server** is server software, or hardware dedicated to running this software.

Satisfies client requests on the World Wide Web.

Can contain one or more websites.

Processes incoming network requests over HTTP and several other related protocols.

The primary function of a web server is to store, process and deliver web pages to clients.[1]

Pages delivered are most frequently HTML documents, which may include images, style sheets and scripts in addition to the text content.

A user agent, commonly a web browser or web crawler, initiates communication by making a request for a specific resource using HTTP

The server responds with the content of that resource or an error message if unable to do so.

Web Server

Functionalities

A **web server** is server software, or hardware dedicated to running this software.

Satisfies client requests on the World Wide Web.

Can contain one or more websites.

Processes incoming network requests over **HTTP** and several other related protocols.

The primary function of a web server is to store, process and deliver web pages to clients.

Pages delivered are most frequently HTML documents, which may include images, style sheets and scripts in addition to the text content.

A user agent, commonly a web browser or web crawler, initiates communication by making a request for a specific resource using HTTP

The server responds with the content of that resource or an error message if unable to do so.

Web Server

About what it returns

A **web server** is server software, or hardware dedicated to running this software.

Satisfies client requests on the World Wide Web.

Can contain one or more websites.

Processes incoming network requests over HTTP and several other related protocols.

The primary function of a web server is to store, process and deliver web pages to clients.[1]

Pages delivered are most frequently **HTML** documents, which may include images, style sheets and scripts in addition to the text content.

A user agent, commonly a web browser or web crawler, initiates communication by making a request for a specific resource using HTTP

The server responds with the content of that resource or an error message if unable to do so.

Web Server

How we talk to it

A **web server** is server software, or hardware dedicated to running this software.

Satisfies client requests on the World Wide Web.

Can contain one or more websites.

Processes incoming network requests over HTTP and several other related protocols.

The primary function of a web server is to store, process and deliver web pages to clients.[1]

Pages delivered are most frequently HTML documents, which may include images, style sheets and scripts in addition to the text content.

A user agent, commonly a web browser or web crawler, initiates communication by making a request for a specific resource using HTTP

The server responds with the content of that resource or an error message if unable to do so.

Web Server

A special type

If the server provides database applications, we typically call it a **database server**, where,

- It **connects** to a database via a database management system (e.g. MySQL),
- the database may or may not be in the same machine as the server software, and also,
- the database may exist in a **distributed** manner, across several machines

A database server can thus produce information dynamically, as per the requests of the client. (The most common functionality of servers is to return .html pages which can be generated statically).

Web Server

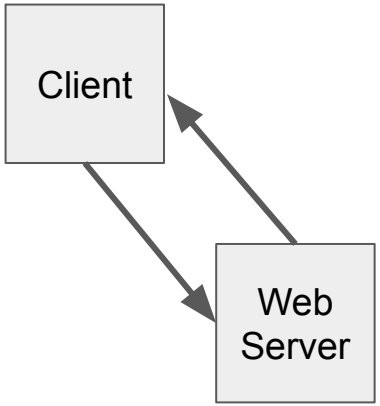
A special type

If the server provides database applications, we typically call it a **database server**, where,

- It connects to a database via a database management system (e.g. MySQL),
- the database may or may not be in the same machine as the server software, and also,
- the database may exist in a distributed manner, across several machines

A database server can thus produce information **dynamically**, as per the requests of the client. (The most common functionality of servers is to return .html pages which can be generated statically).

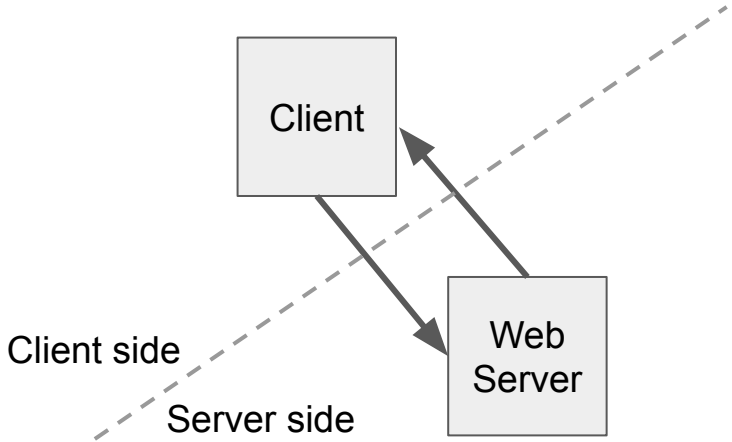
Putting together components of a Web Application



A **client** (e.g. browser) requests the web server for information (pages, data, etc.) or requests some action.

The web server returns the info (or performs the requested actions).

Putting together components of a Web Application

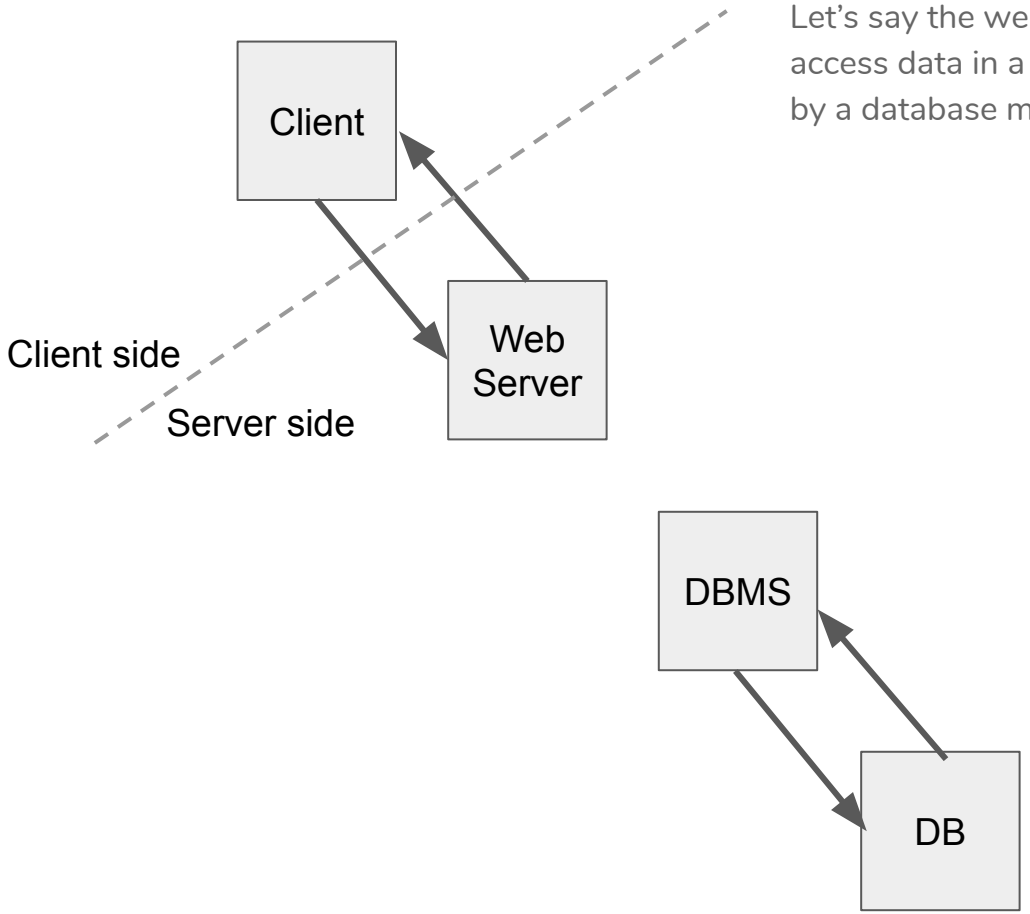


The web server does a number of things to process the client's request.

All this happens on the server side.

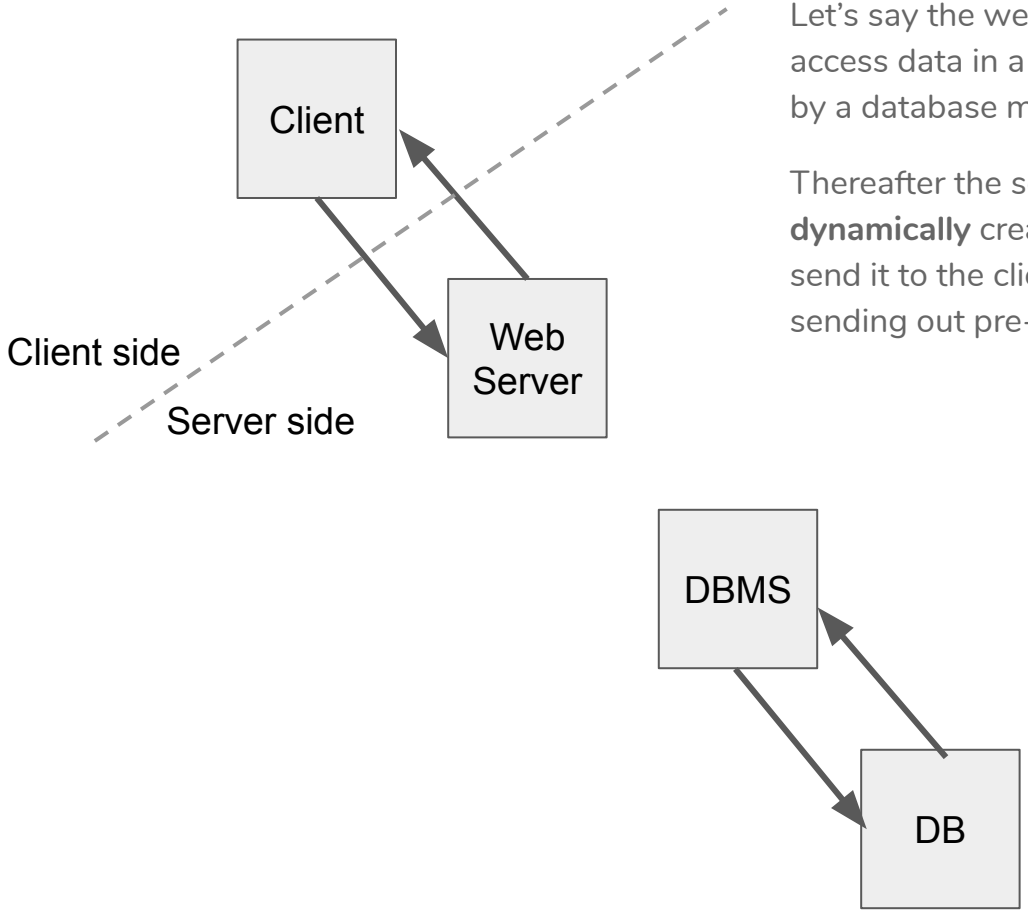
(This is our first glimpse of the **client-server architecture**.)

Putting together components of a Web Application



Let's say the web server needs to access data in a database managed by a database management system.

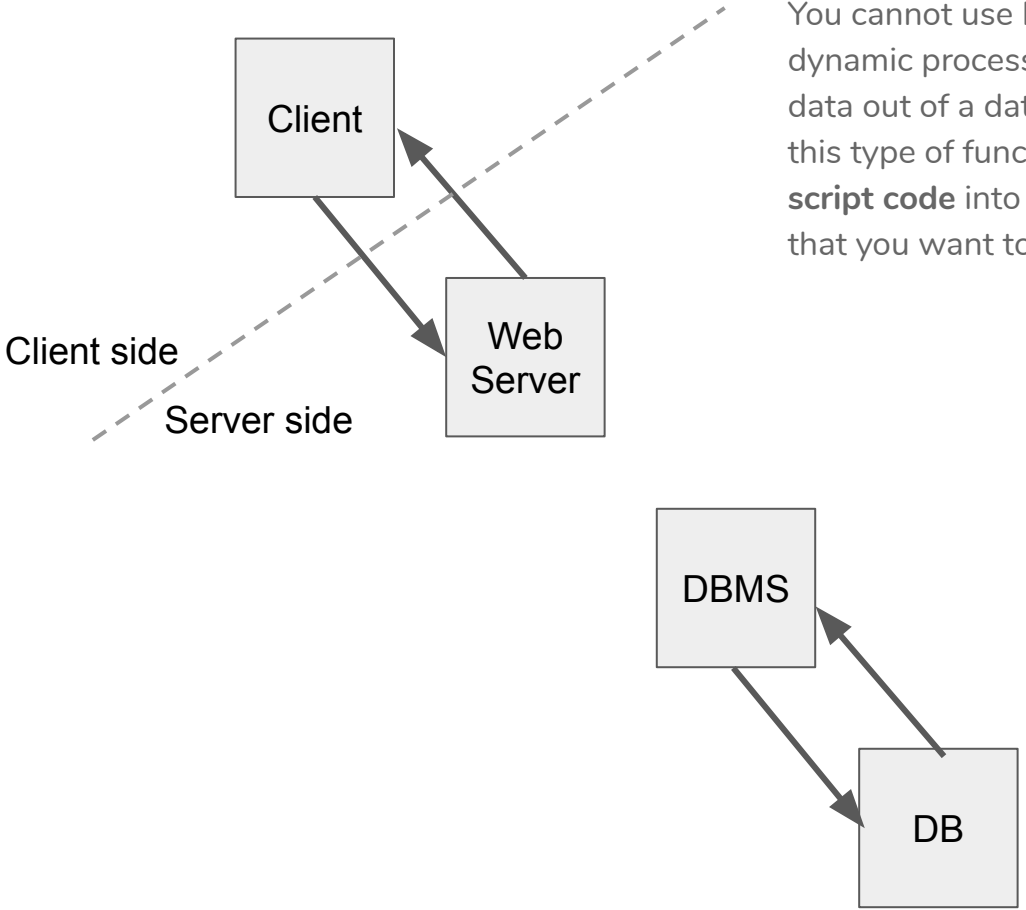
Putting together components of a Web Application



Let's say the web server needs to access data in a database managed by a database management system.

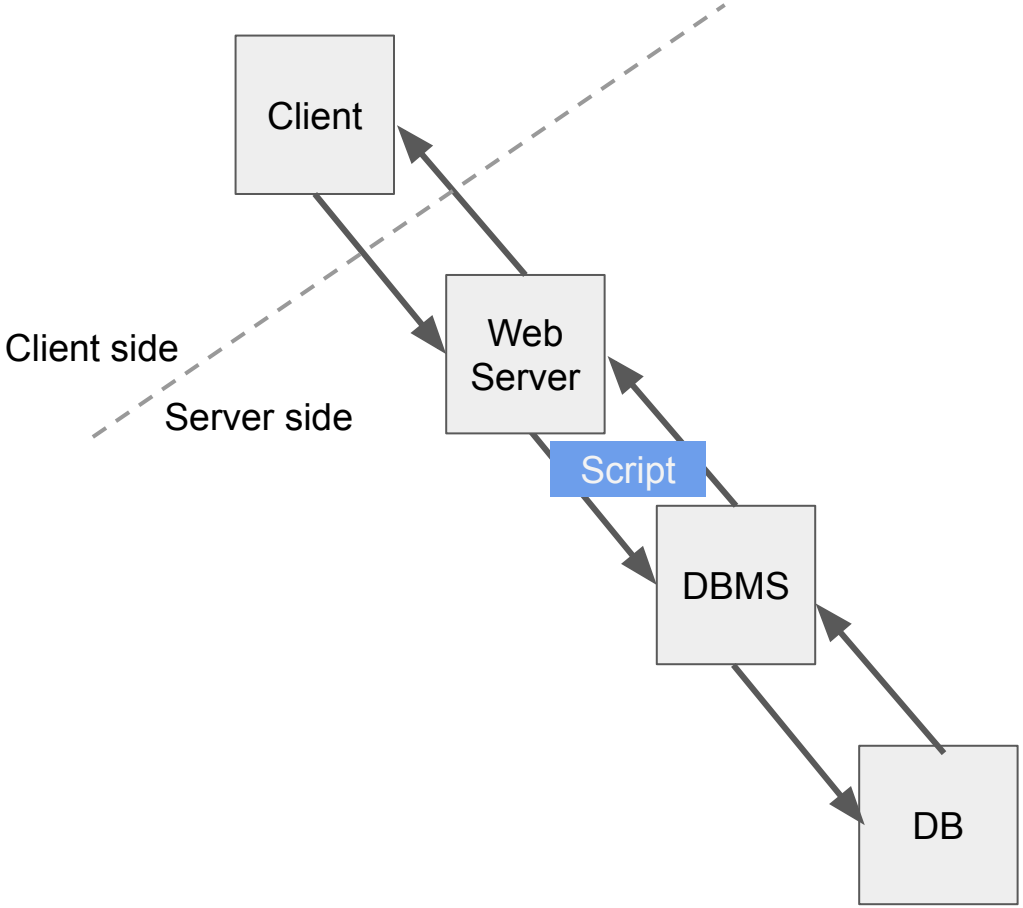
Thereafter the server would need to **dynamically** create content, and send it to the client, rather that sending out pre-built static pages.

Putting together components of a Web Application



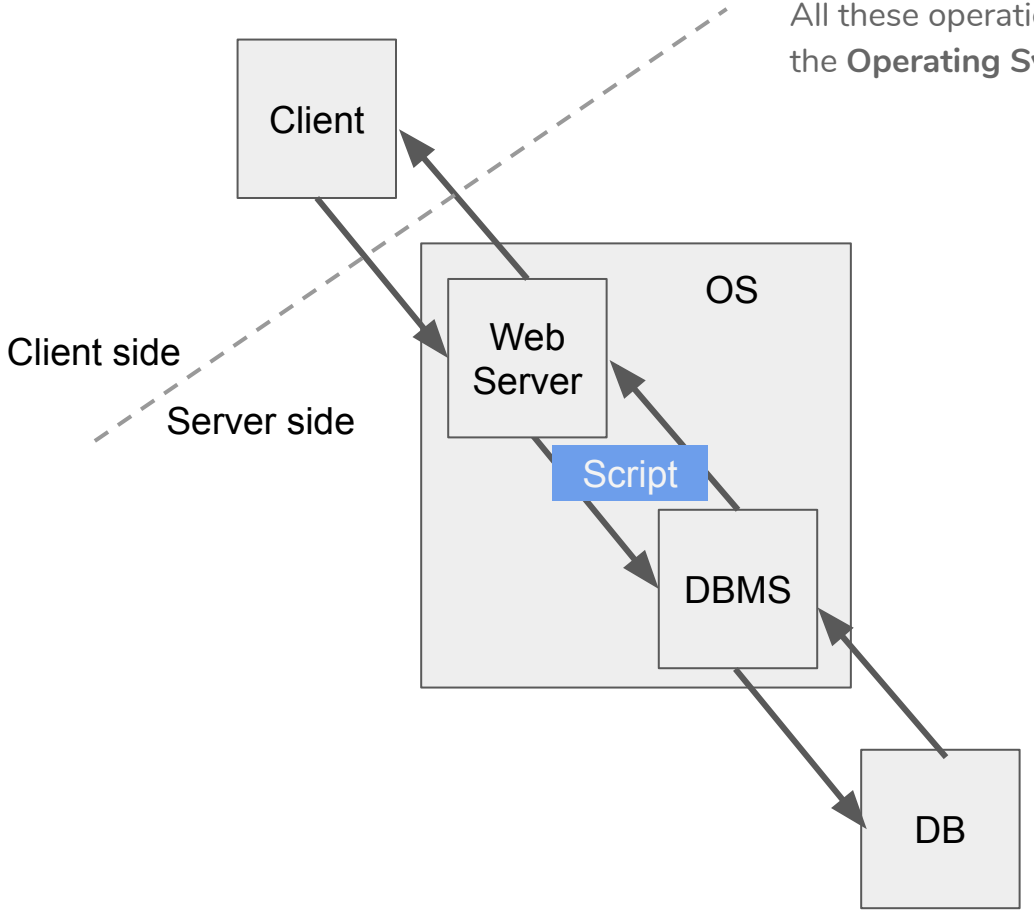
You cannot use HTML to perform dynamic processes such as pulling data out of a database. To provide this type of functionality, you put **script code** into the parts of a page that you want to be dynamic. [ref]

Putting together components of a Web Application

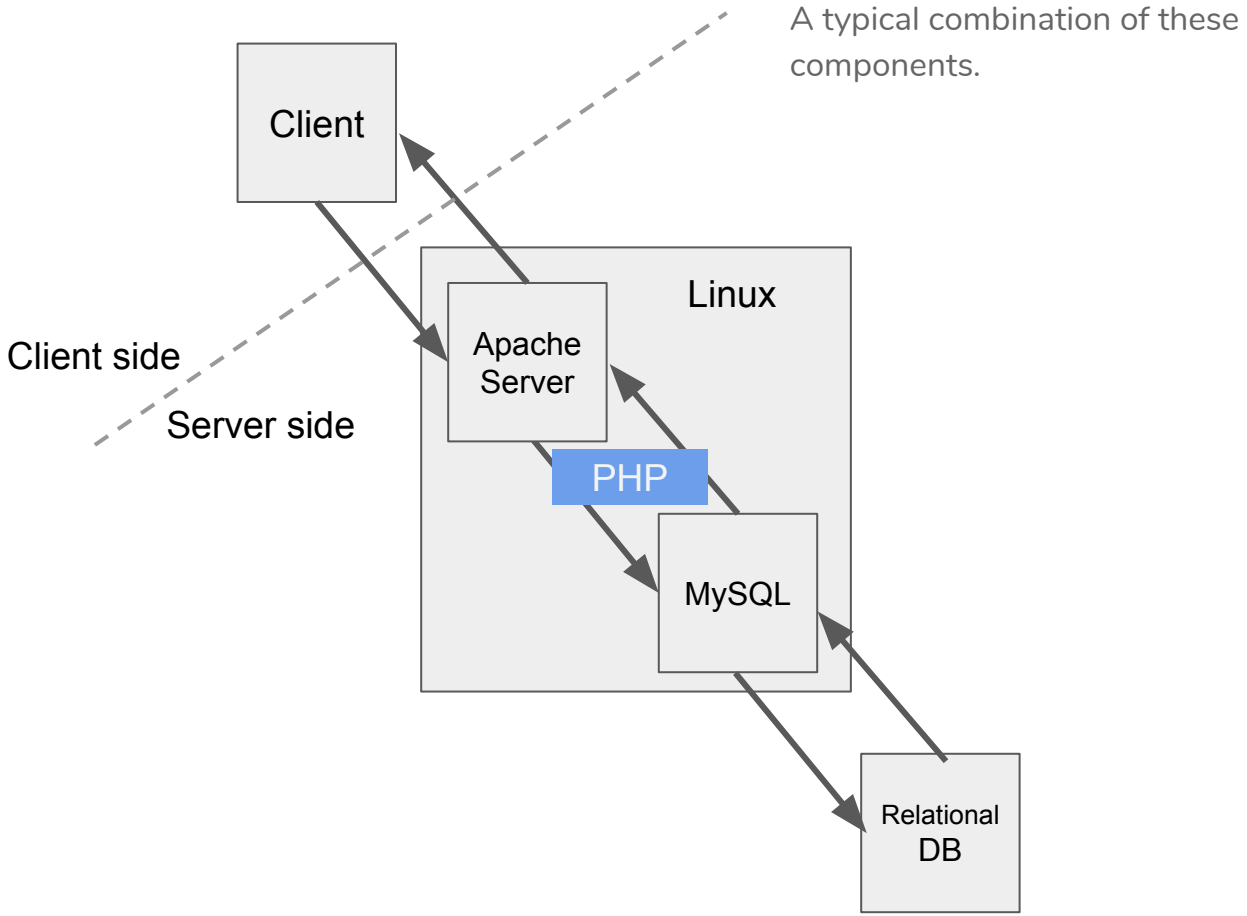


Putting together components of a Web Application

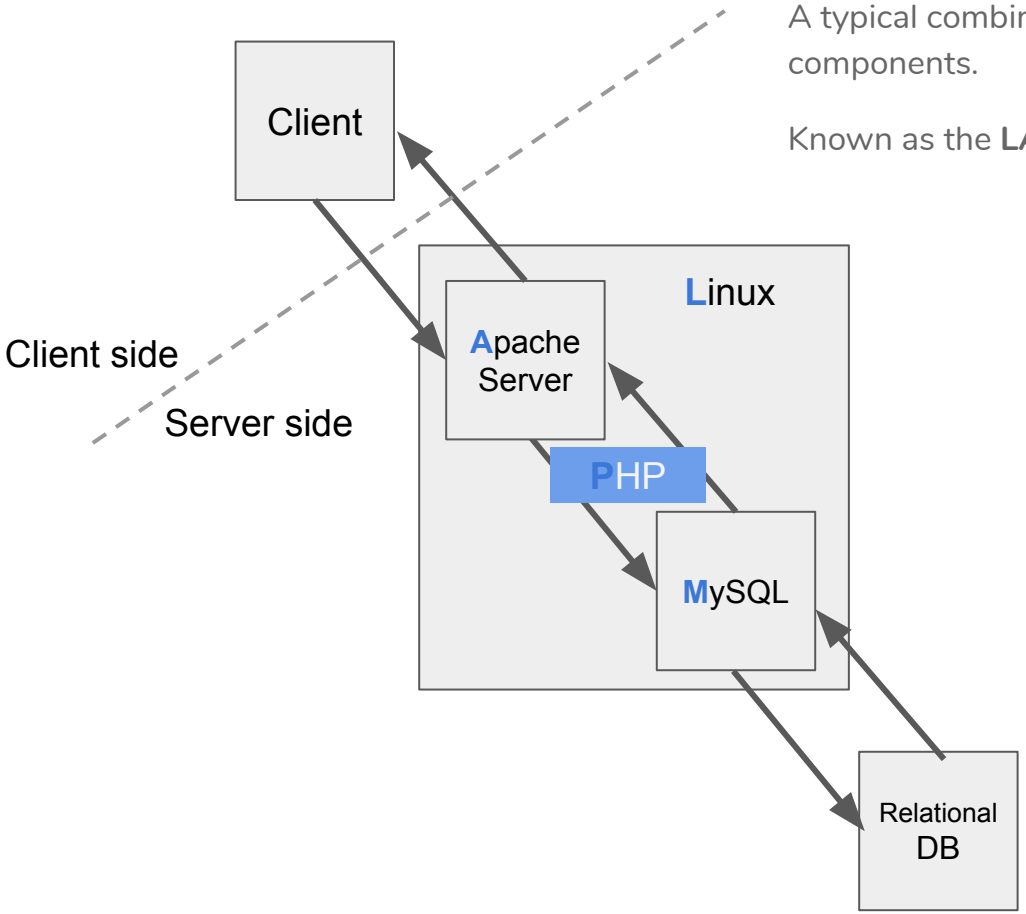
All these operations are enabled by the **Operating System** [ref]



Putting together components of a Web Application



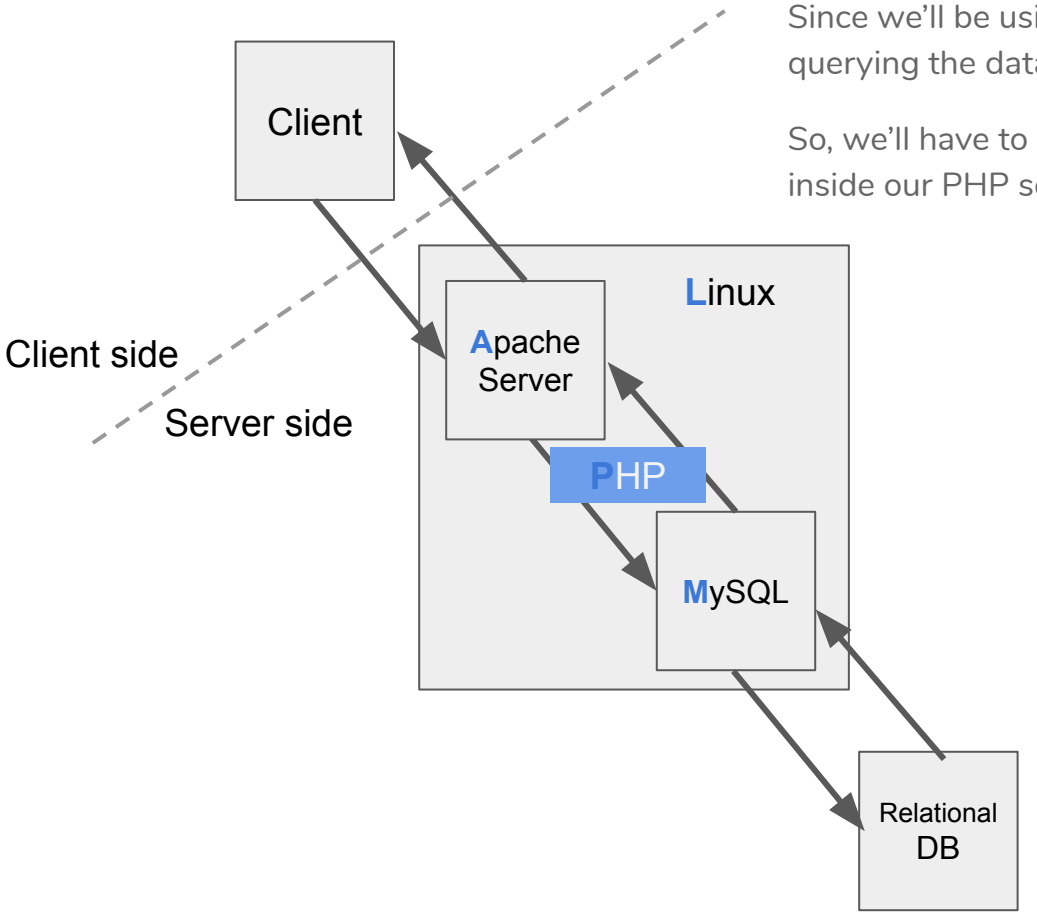
Putting together components of a Web Application



A typical combination of these components.

Known as the **LAMP Stack.**

Putting together components of a Web Application

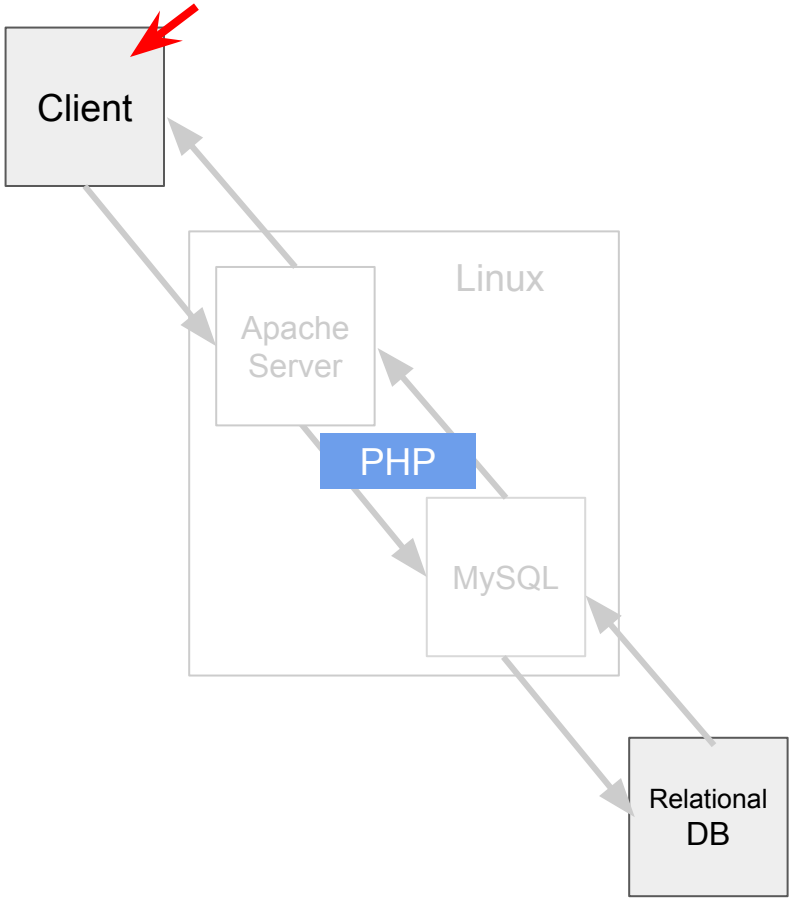


Since we'll be using MySQL, we'll be querying the database using SQL.

So, we'll have to plug in SQL code inside our PHP script.

SQL Injection Attack

A simple web app



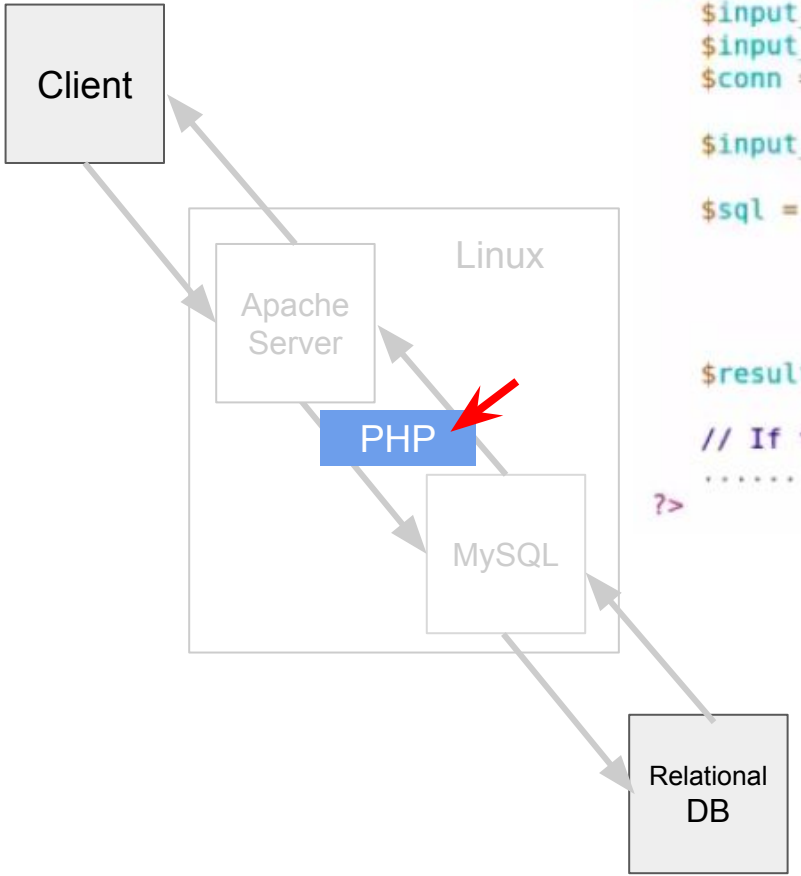
Employee Profile Information

Employee ID:

Password:

Get Information

Copyright © SEED LABs



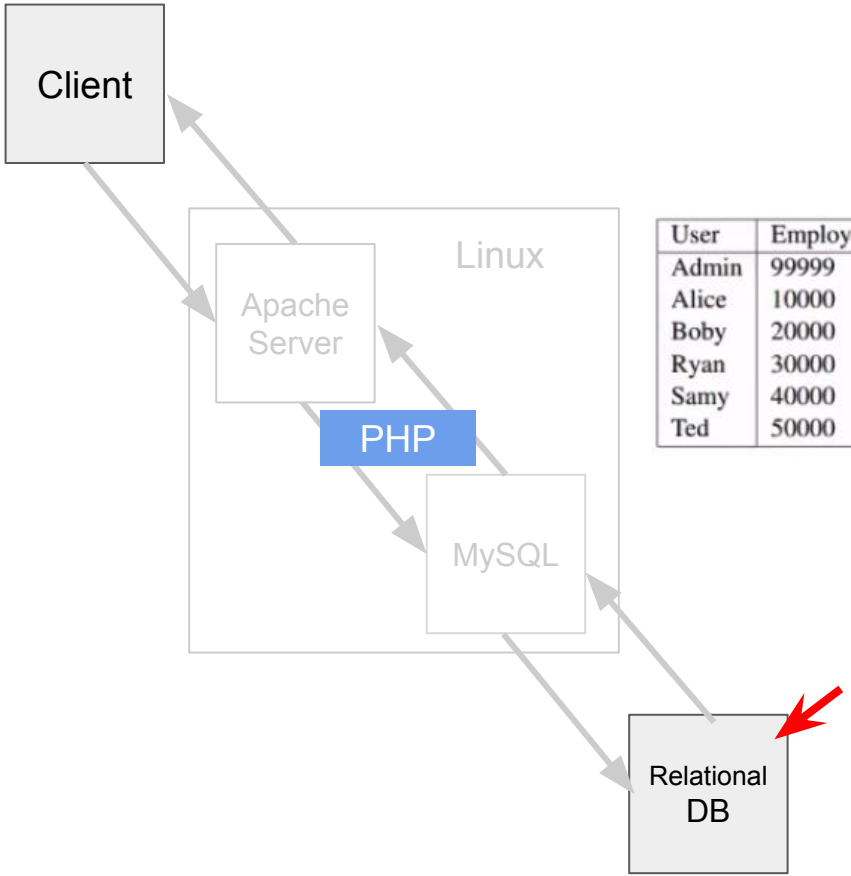

```php
<?php
    $input_eid = $_GET['EID'];
    $input_pwd = $_GET['Password'];
    $conn = getDB();

    $input_pwd = sha1($input_pwd);

    $sql = "SELECT id, name, eid, salary, birth, ssn, phoneNumber, address,
                   email,nickname,Password
            FROM credential
            WHERE eid= '$input_eid' and Password='$input_pwd'";

    $result = $conn->query($sql);

    // If there is a match, the user will be able to log in.
    ......
?>
```



User	Employee ID	Password	Salary	Birthday	SSN	Nickname	Email	Address	Phone#
Admin	99999	seedadmin	400000	3/5	43254314				
Alice	10000	seedalice	20000	9/20	10211002				
Boby	20000	seedboby	50000	4/20	10213352				
Ryan	30000	seedryan	90000	4/10	32193525				
Samy	40000	seedsamy	40000	1/11	32111111				
Ted	50000	seedted	110000	11/3	24343244				


```php
<?php
   $input_eid = $_GET['EID'];
   $input_pwd = $_GET['Password'];
   $conn = getDB();

   $input_pwd = sha1($input_pwd);

   $sql = "SELECT id, name, eid, salary, birth, ssn, phoneNumber, address,
                  email,nickname,Password
           FROM credential
           WHERE eid= '$input_eid' and Password='$input_pwd'";

   $result = $conn->query($sql);

   // If there is a match, the user will be able to log in.
   ......
?>
```

User	Employee ID	Password	Salary	Birthday	SSN	Nickname	Email	Address	Phone#
Admin	99999	seedadmin	400000	3/5	43254314				
Alice	10000	seedalice	20000	9/20	10211002				
Boby	20000	seedboby	50000	4/20	10213352				
Ryan	30000	seedryan	90000	4/10	32193525				
Samy	40000	seedsamy	40000	1/11	32111111				
Ted	50000	seedted	110000	11/3	24343244				

SQL Injection Attack

SQL examples

(Lecture on the topic by Prof. Du)

❖ Table in database

Table Name: **Users_Table**

Name	Gender	Age	Email	passwd
Alice	F	25	alice@syr.edu	wf732d582
Bob	M	24	bob@syr.edu	fgh34fg4
Cindy	F	30	cindy@syr.edu	rt34tbf34gh
David	M	35	david@syr.edu	34rtn45rue

Get Records

```
SELECT *
FROM Users_Table
WHERE name='Alice'
```

Update Records

```
UPDATE Users_Table
SET email='alice@syr.edu'
WHERE name='Alice'
```

Insert Records

```
INSERT INTO Users_Table
VALUES ('Ed', 'M', 30, 'ed@syr.edu', '234s23w')
```

SQL Injection Attack

Question

(Lecture on the topic by Prof. Du)

❖ Typical PHP Code

```
<?php
  $sql = "SELECT id, name, salary
          FROM credential
          WHERE eid= '$input_eid'";
  $result = $conn->query($sql);
?>
```

❖ Question

If you don't know any eid, can you get the database return some records?

Thank you