|  |  |  |
| --- | --- | --- |
| kUnit Title Web Application Development | **Unit Code**  WAD | Date Issued 22 January, 2018 |
| Student Name **Assignment Brief**  Wojciech Kozlowski | Student ID | Date Received |
| Lecturer Name Tanveer Ahmad | Internal Verifier Name | |

**Rules and regulations:**

|  |
| --- |
| **Plagiarism** is presenting somebody else’s work as your own. It includes: copying information directly from the Web or books without referencing the material; submitting joint coursework as an individual effort; copying another student’s coursework; stealing coursework from another student and submitting it as your own work. Suspected plagiarism will be investigated and if found to have occurred will be dealt with according to the procedures set down by the College. Please see your student handbook for further details of what is / isn’t plagiarism. |

**Coursework Regulations**

1. Submission of coursework must be undertaken according to the relevant procedure – whether online or paper-based. Lecturers will give information as to which procedure must be followed, and details of submission procedures and penalty fees can be obtained from Academic Administration or the general student handbook.
2. All coursework must be submitted to the Academic Admin Office and a receipt **must** be obtained. Under no circumstances can other College staff accept them. Please check the Academic Admin Office opening hours.
3. Late coursework will be accepted by Academic Admin Office and marked according to the guidelines given in your Student Handbook for this year.
4. If you need an extension (even for one day) for a valid reason, you must request one, using a coursework extension request form available from the Academic Admin Office. **Do not ask the lecturers responsible for the course - they are not authorised to award an extension**. The completed form must be accompanied by evidence such as a medical certificate in the event of you being sick.
5. General guidelines for submission of coursework:
6. All work must be word-processed and must be of “good” standard.
7. Document margins shall not be more than 2.5cm or less than 1.5cm
8. Font size in the range of 11 to 14 points distributed to including headings and body text. Preferred typeface to be of a common standard such as Arial or Times New Roman for the main text.
9. Web applications developed must be submitted online. Screen shots and links to the pages should be included in the assignment brief.

**Remember to keep your coursework receipt.**

Learning Outcomes (LO) and assessment requirements

|  |  |
| --- | --- |
| **Outcomes** | **Assessment requirements** |
|  | **To achieve each outcome a learner must demonstrate the ability to:** |
| 1. Be able to set up, configure and maintain web servers using server-side scripting languages. | 1. Set up, configure and maintain a web server |
| 1. Demonstrate server backup, migration and recovery procedures |
| 1. Program internet applications with common server-side scripting languages |
| 2. Be able to develop dynamic web-based applications. | 1. Design a front-end interface demonstrating business logic and data logic |
| 1. Advanced back-end database connection and manipulation with queries |
| 1. Be able to develop a database-driven web site |
| 3. Be able to identify threats to the security of data in an internet working environment. | 1. Implement authentication and authorization in web-based application |
| 1. Make use of session security mechanisms |
| 1. Be able to identify threats to the security of data in an internet working environment. |
| 4. Use appropriate design and testing techniques. | a. Identify business objectives, system functionality and information requirements when developing an application |
| b. Perform systems tests against specified criteria |

\* Please see the Assignment Evaluation Sheet for Merit and Distinction criteria

**Case Study/Background Information – Part 1**

Eurostar Travel is a tour operator in London. Currently, they have a paper based booking system in place. However, to streamline operations and to enable customers to place advance bookings, the CEO of Eurostar Travel has decided to put in place an Online Tour Booking System (OTBS) to replace the current paper-based system. The goal of the OTBS is to enable customers to book tours in advance via their website, to cut down operational cost as well as maintaining high level of accuracy.

**Description of problem to be solved**

Install, configure and administer a web server of your choice. When developing a web application, student must make use of a server-side scripting language i.e. PHP, CGI-Perl, ASP and a relational database i.e. MySQL, MS-SQL, Oracle etc. Please note that the use of flat-text file or MS Access to store data is not acceptable.

**Task 1**

1. Evidence of setting up, configure and administer (i.e. with discussion of server backup and recovery) a web server of your choice *(****LO 1a, b****)(why do we need one?)(for example ipage configuration)*
2. Justification of your choice for web server and scripting language. Provide an example of server side scripting program. *(****LO 1c****)*

|  |
| --- |
| **Feedback** |
| **Strengths** |
| **Areas for Improvement** |
| **Lecturer Signature: Date:** |

**Case Study/Background Info – Part 2**

Initial analysis reveals that System Actors in Eurostar Travel’s Online Tour Booking System include:

• Online Customer

• Company Staff

Initial analysis also reveals the following use case scenarios

**Customer scenarios:**

* Search and Make Advance Booking

Customers visiting the Eurostar Travel website will be able to search for a tour based on several criteria (e.g. destination, price etc.). If suitable result(s) found, they can select a tour and be provided with details of the tour including date, price, availability, descriptions, photos and travel itinerary.

If the tour is available for booking, the total cost of the tour is provided to the customer, and the customer confirms the booking for which a reservation reference number is provided. However, if there are insufficient places available for the tour reservation, the customer is invited to make another search.

**Staff scenarios:**

* **Add Tour**

Eurostar Travel staff adds details of a new tour. Tour details include travel date, duration, price, availability, descriptions, destination photos and travel itinerary.

* **Remove Tour**

Eurostar Travel staff can remove a tour i.e. make it unavailable for booking. The tour can only be removed if there are no booking on it.

**Description of problem to be solved**

Capture all business requirements using UML and ER diagrams. Design a logical front end interface which would connect to a relational database through online application.

**Deliverables**

1. Your front-end implementation should follow standards specified by World Wide Web Consortium (W3C) and should be cross-browser compatible. *(****LO 2a****)*.

*Please make sure your documentation includes screenshots from your website.*

1. Any dynamic content in application can be ‘pulled out’ from a database in real time with optimal queries. Your application is expected to implement select, insert, update as well as read-only operations. *(****LO 2b, 2c****)*.

Make sure you include evidences of server side programming and back-end database manipulation. (PHP, MySQL)

|  |
| --- |
| **Feedback** |
| **Strengths** |
| **Areas for Improvement** |
| **Lecturer Signature: Date:** |

**Case Study/Background Info – Part 3**

**Customer scenarios:**

* **Make Payment**

When customers book a tour, they will need to enter their payment information, which include card holder name, card number and expiry date. Payment cards may be one of two types – credit card or debit card. To secure the transaction, sensitive data must be protected and cannot be accessed / modified by unauthorized person (See Learning Outcome 3a, 3b, 3c).

**Description of problem to be solved**

Beside functionality and usability, the final implementation should have adequate security mechanisms and input checking (e.g. you can prevent mass subscribe/unsubscribe from mailing list, spam registration and/or form submitted, voter cannot repeatedly vote on a poll, customer’s data transmit to e-commerce application should be secured, etc). Your application should implement authentication to prevent unauthorized access.

**Deliverables**

1. An authentication (e.g. sign-up and log-in) system to prevent unauthorized access. *(****LO 3a****)*
2. The use of session, encryption to protect sensitive data *(****LO 3b****)*
3. Discussion on security threats and countermeasures *(****LO 3c****)*
4. Evidence of system testing: actual result of system testing and acceptance testing for your development. *(****LO 4a, b****)*

|  |
| --- |
| **Feedback** |
| **Strengths** |
| **Areas for Improvement** |
| **Lecturer Signature: Date:** |

Contents

[Introduction 7](#_Toc511304340)

[Task 1.1. Evidence of setting up, configure and administer (i.e. with discussion of server backup and recovery) a web server of your choice (LO 1a, b) 8](#_Toc511304341)

[Task 2. Justification of your choice for web server and scripting language. Provide an example of server-side scripting program. (LO 1c) 14](#_Toc511304358)

[Task 3. UML Diagrams 16](#_Toc511304359)

[Task 4. Any dynamic content in application can be ‘pulled out’ from a database in real time with optimal queries. Your application is expected to implement select, insert, update as well as read-only operations. (LO 2b, 2c). 20](#_Toc511304360)

[Task 5. An authentication (e.g. sign-up and log-in) system to prevent unauthorized access. (LO 3a) 24](#_Toc511304361)

[Task 6. The use of session, encryption to protect sensitive data (LO 3b) 27](#_Toc511304362)

[Task 7. Discussion on security threats and countermeasures (LO 3c) 27](#_Toc511304363)

[Task 8. Evidence of system testing: actual result of system testing and acceptance testing for your development. (LO 4a, b) 28](#_Toc511304364)

# Introduction

There are many ways I could have accomplish this task but the best way to learn something in IT industry is to try to build it from scratch. Nevertheless, below I have listed few examples how I could have accomplished my assignment in different, maybe quicker and more conforming to standards way:

* Stripe
* Wordpress
* PHP Frameworks (for example Zend, Laravel, Symphony, CakePHP etc.)
* MySQL Installer Dashboard from <https://dev.mysql.com/doc/refman/5.7/en/mysql-installer-catalog-dashboard.html>



Address to live website is: <https://wojtek78.000webhostapp.com/>

Login and password for dashboard are admin (for both).

Hostname: localhost

Username: id2283587\_wojtek

Password : cynamon

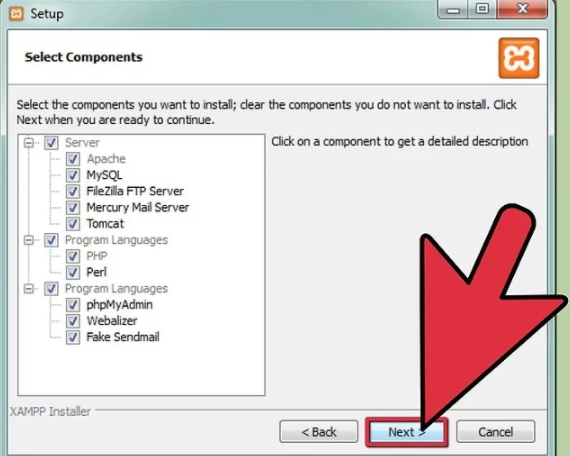
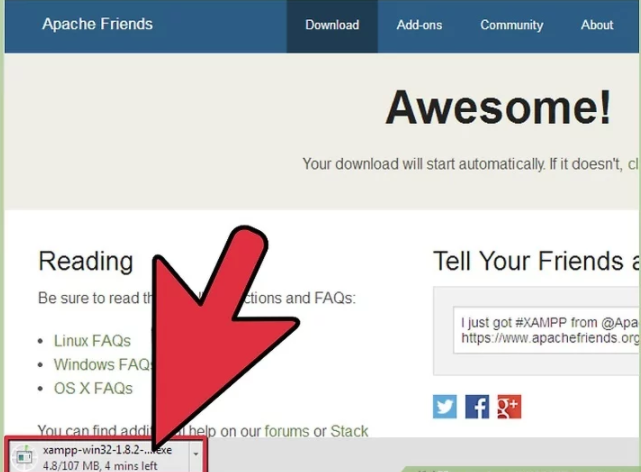
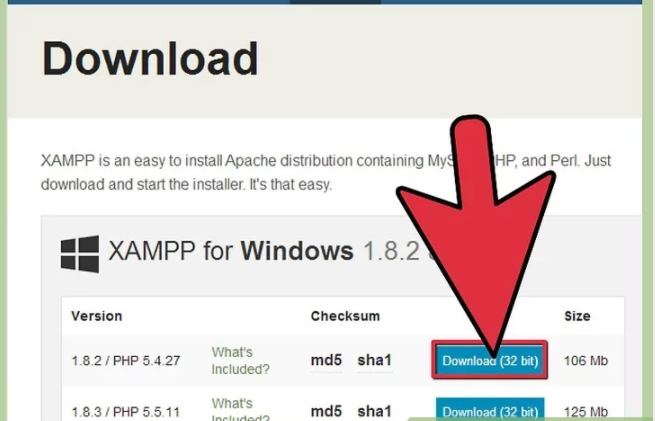
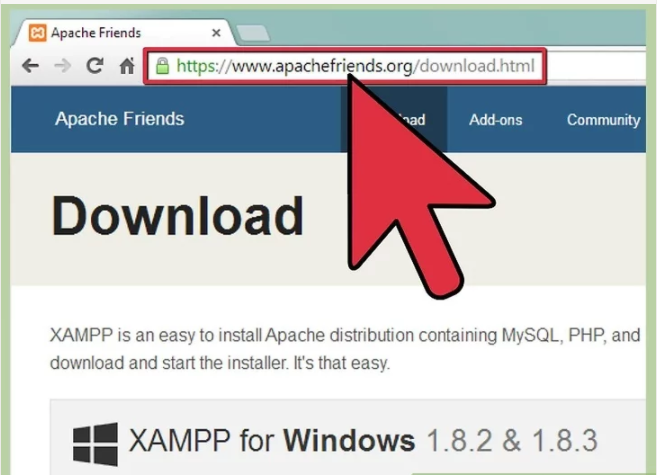
Database name: id2283587\_eurostar

If there will be problem with this site, please try: wojciechk.sgedu.site

# Task 1. Evidence of setting up, configure and administer (i.e. with discussion of server backup and recovery) a web server of your choice *(LO 1a, b)*

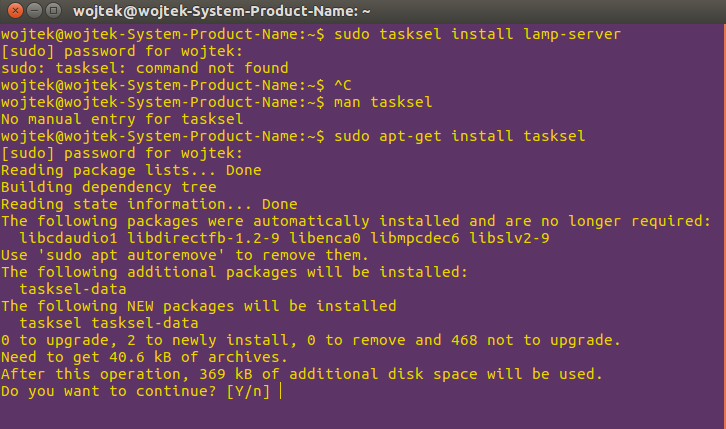
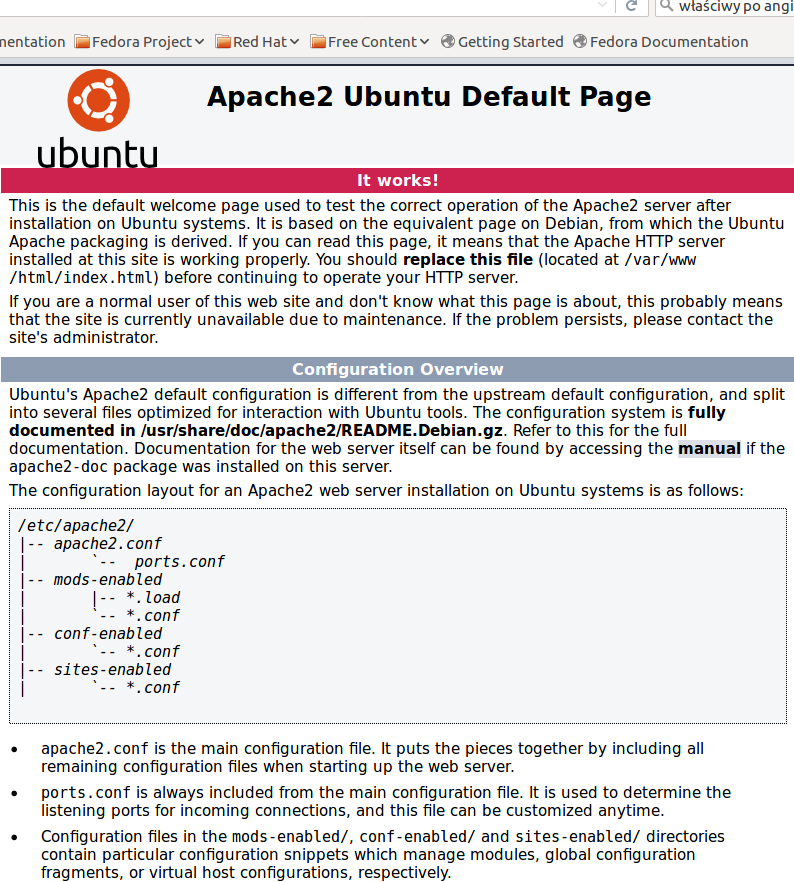
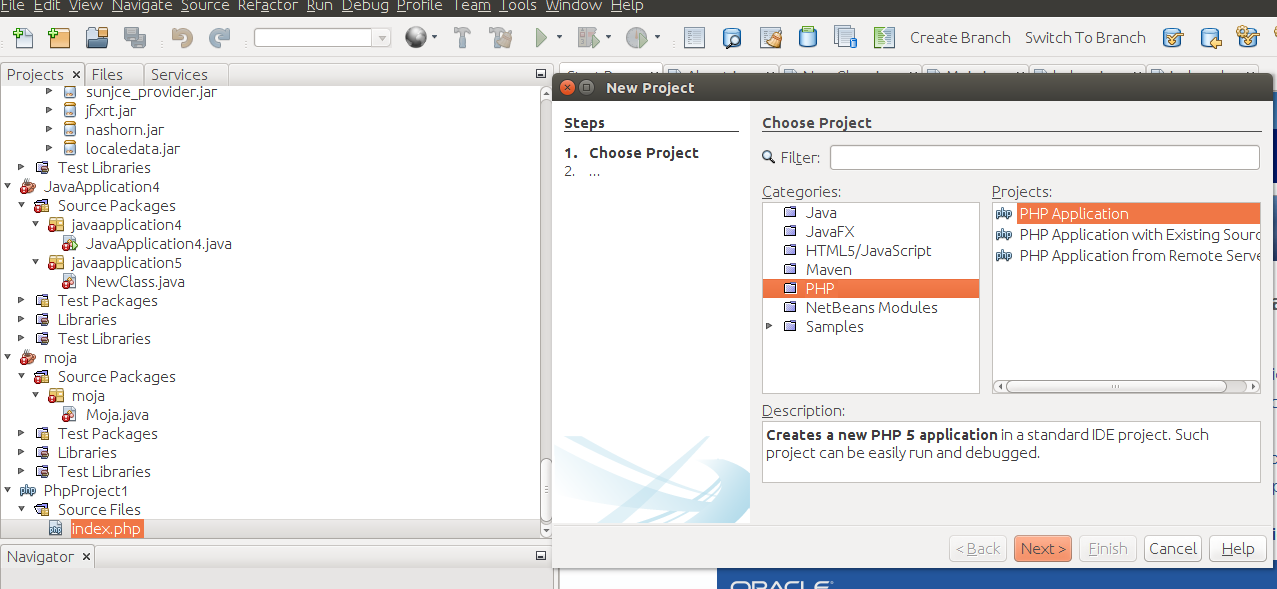
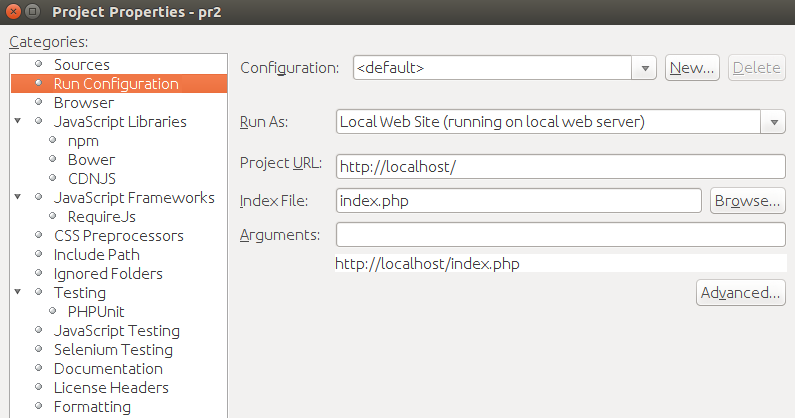
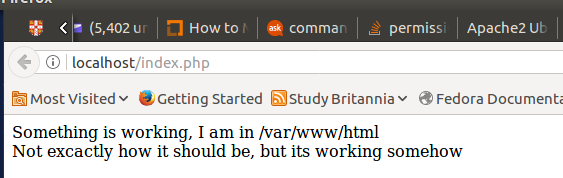
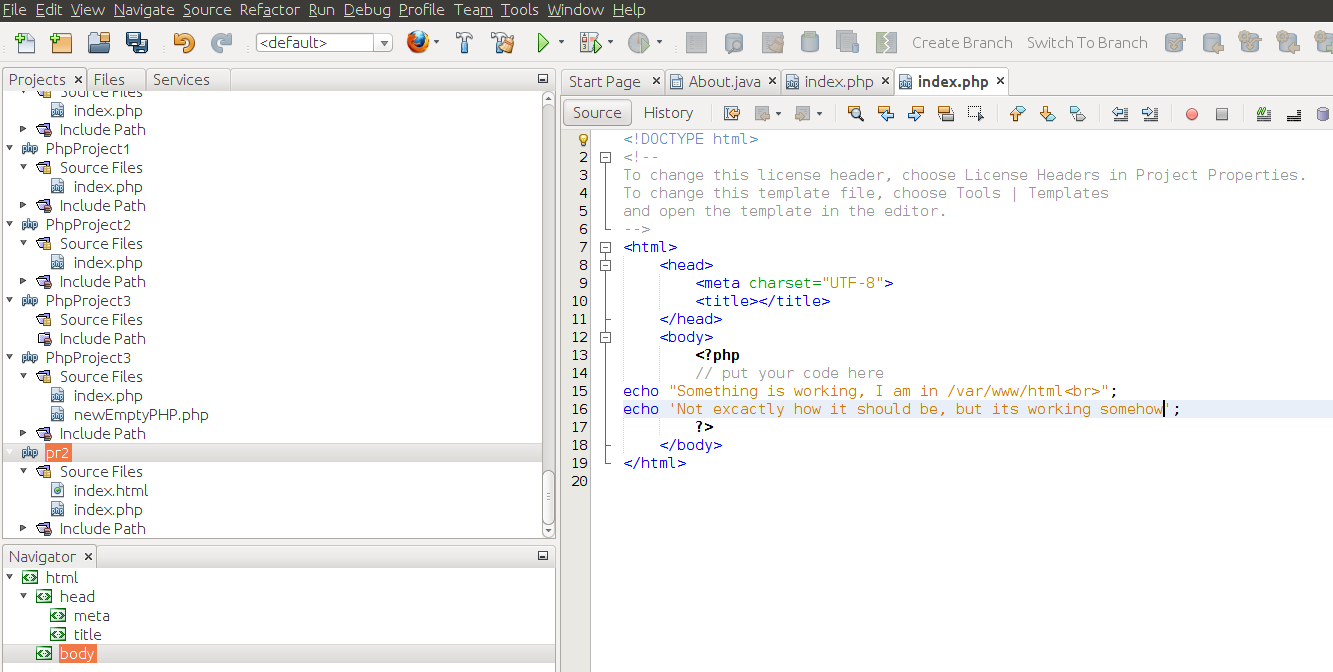
The term “web server” somewhat confusingly could be understand in 2 different ways: as a whole computer system or as a software solution which purpose is to serve web pages to the client. For simplicity this work will be considering the latter meaning.

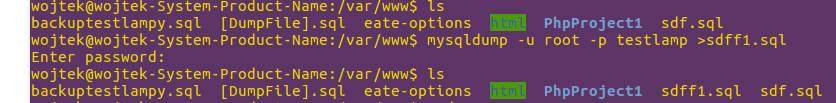
In this section I will show installation process of local server development environment XAMPP. XAMPP is the most popular, open-source WAMP (Windows, Apache, MySQL,PHP) servers.



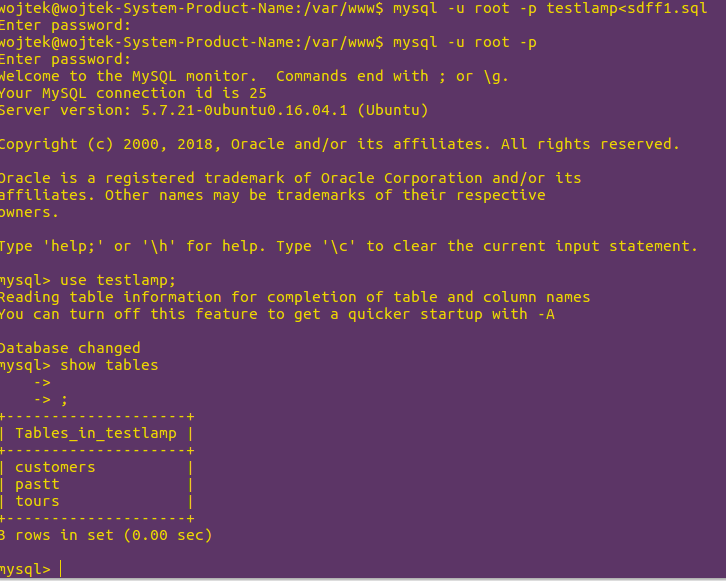
After installation is done, it is possible to reconfigure software using httpd.conf file. For example, it could be convenient to define user aliases there (if somebody want to use folder other than htdocs to open in the browser).

In addition to that I have decided to give a try to installation of LAMP stack (Linux, Apache, MySQL, PHP). I have used my existing Ubuntu distribution installed on separate partition. Following steps were executed in the process:

1. As a preliminary step I have installed tasksel tool which is used as multiple packages installer. In terminal: *sudo apt-get install tasksel* 
2. Now it’s possible to use tasksel to install LAMP components all-in-one go: *sudo taskse1 install lamp-server*
3. During installation it will be possible to choose password for the MySQL root user: 
4. To test the outcome I have typed localhost into browser:  which worked, and next I have used NetBeans IDE to create PHP project (after adding adequate PHP plugin):  which didn’t worked: 
5. After many trials and errors, I have changed permissions for var/www/html folder: *sudo chmod -R ugo+rw /var/www/html* and configuration settings: Now it works perfectly: 
6. To connect to MySQL server, the following command has to be executed: *mysql -u root -p.*
7. To back up database:



1. To retrieve(import) database:



Linux is more demanding system then Windows despite its numerous advantages so I will go back to using XAMPP on Windows at the moment.

Few words about configuration:

* Basics - after installing XAMPP all website files has to be inside htdocs folder. It is only then (well it is possible to add aliases to configuration files as well for other folders) when it is possible to start php files from the browser.
* Most of the installation processes – Apache, MySQL, FileZilla, Tomcat are pretty straightforward and automatic.
* More advanced options are available by tweaking http.conf, ssl.conf, xampp.conf, php.ini, config.inc.php, my.ini and other configurations files. All of them are easily accessible from Xampp control panel.

# **Task 2.** Justification of your choice for web server and scripting language. Provide an example of server-side scripting program. *(LO 1c)*

**There are quite a few of web servers available to choose from but the most popular are: Apache, IIS, Nginx, GWS and Lite Speed Web Server.**

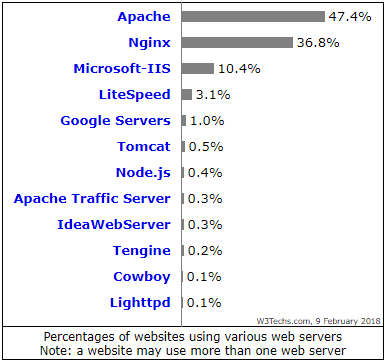


Figure 0‑1Web Servers according to popularity

The choice of web server could depend on many factors. Sometimes it rely on the fact what brand a stakeholder is affiliated with – for example Microsoft services would use probably its own software , in this case IIS. If a budget is on stake, an open source (and free) solution would be more preferable like Apache or NGINX. It might hinge on the choice of Operating System being used or what kind of support is needed. What is characteristic of the website being hosted could play a big role – if it is more static than dynamic the Nginx or lighttpd could be a good option due to their improved static objects serving performance. The best in term of professional level of performance, reliability, security and support probably would be the IIS but for a price.

Short summary of most popular web servers:

1. **Apache.** This is one of the most popular open-source servers without cost of licensing fees. Pros: modular structure, may be used on all popular operating systems, numerous enthusiastic members of the community. Cons: as it is a process-based, it creates a new thread for each new connection which might make it slower.
2. **Internet Information Services (IIS).** Proprietary product of Microsoft. Pros: works well with ASP, MS SQL, Active Directory and others Microsoft services, allows access to ASPX scripts and .NET framework. Cons: not as customizable as other open source solutions, cost.
3. **LSWS.** Stands for LiteSpeed Web Server. Pros: offers fast loading times, integrates well with Apache.
4. **GWS.** Acronym for Google Web Server.
5. **NGINX.** Cons: good speed,scalability and performance. It is event-based and reverse-proxy server.Perfect choice for Virtual Private Servers setting-ups. Capable of serving simultaneously thousand clients (resolving so called “C10K problem”).

My choice of server for this assignment is Apache as it is one of the most popular and it goes with free, open-source software license. For client-side scripting language I would choose JavaScript as it is most often used standard in web applications development, and for back-end I would choose PHP-MySql combo as this is what has been suggested in assignment instructions, it is only one that I have learnt and finally it is free of charge, very popular with a lot of help available.

One thing worth mentioning about PHP is that it is offering several styles of coding:

* Old mysql syntax
* MySqli Procedural style
* MySqli Object-oriented style
* PDO

In this assignment I was trying to use mainly MySqli Procedural style. Main reason is that at this stage it is a bit easier and the task is huge so I will leave OO PHP for later.

Apart from those choices, there is plenty of more front-end orientated technologies to pick up from which I was using sometimes: jquery, bootstrap,AJAX, JSON, google charts etc. At the top of that, for part of my website I have used HTML/CSS template from http://www.templatemonster.com/ , but I have customized it heavily.

# Task 3. UML Diagrams

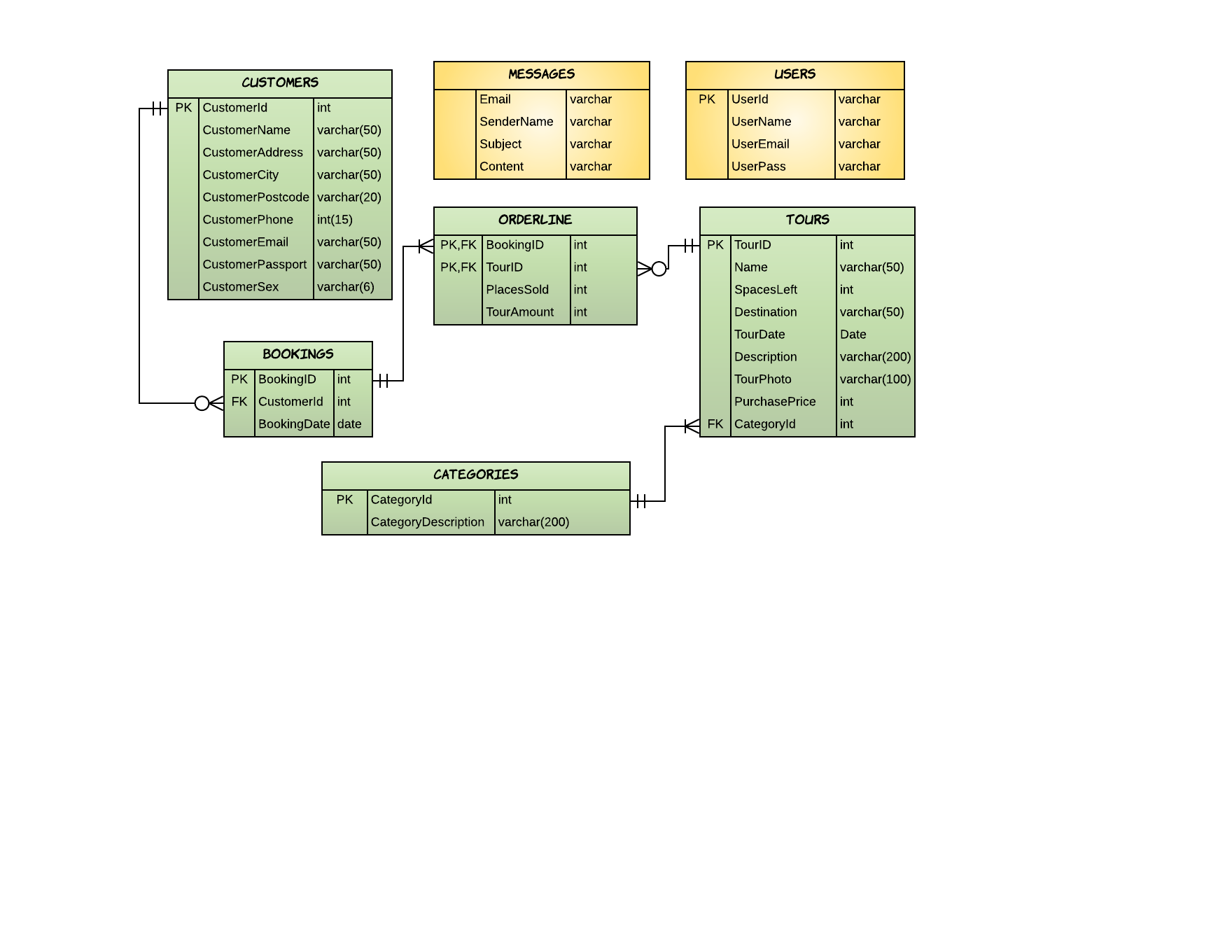
I have decided that there is no need to unnecessary overcomplicate things and I have made rather simple design. Main Actors are Customer and Admin. Their Use Cases are overlapping in few cases as you can see, but generally speaking Customer aim is to book service that Eurostar provides and Admin work is to make that service manageable and available for customer, and to provide basic channel of communication with customer (CMR).

A close up of a map

Description generated with high confidence

Overview of Eurostar database Schema.

I have decided to create 2 unrelated table to the rest of the management system. Users table represent other employees or staff members and messages are self-explanatory. The rest is a classic model of RDMS based on Northwind company case.





Site Map

A screenshot of a social media post

Description generated with very high confidence

There are as well a few PHP form-handlers(especially around dashboard.php) and also a few ones managing database connections and authentications like db.php and auth.php.

Standard practises of building website are specified by W3 Consortium. It is worth to notice that some official standards are really recommendations and the website could possibly be working fine without them, although according to W3C, will be lacking some basic functionality or features. Some of them will give website better ranking for SE (like alt attributes), some will give better responsiveness, others will improve speed or better compatibility with other browsers. Anyway, it works differently in every case and sometimes not following the official recommendations could actually be more beneficial. The list of those rules that website should follows to be qualified as W3C compliant is huge and therefore I will give just a few examples:

* Using proper syntax, and tags. If mark-up language is HTML5 the (static at least) page should be started with <!DOCTYPE html> , followed by html, head, body sections.
* The tags should be closed.
* Pictures should have “alt” attribute.
* Animations, and transformations should include alternative versions for different browsers, for example:

/\* Code for old Chrome, Safari and Opera \*/  
@-webkit-keyframes mymove {  
    from {background-color: red;}  
    to {background-color: blue;}  
}  
/\* Standard syntax \*/  
@keyframes mymove {  
    from {background-color: red;}  
    to {background-color: blue;}  
}

* There should not be deprecated code like “frame” used.
* The Marquee tag which we were learning about last year should not be used, not even because it is obsolete but because it was so badly built from the start that it was never recommended.
* One of the basic way to support responsiveness is by adding <meta name="viewport" content="width=device-width, initial-scale=1.0"> inside HEAD section.

There are many online validation tools for checking the website “correctness”. For example:

* <https://jigsaw.w3.org/css-validator/>
* <https://validator.w3.org/>
* <http://www.htmlhelp.com/tools/validator/>
* <http://watson.addy.com/>

On my web, compatibility with older browsers is managed by PIE.htc module. It is capable of rendering many important CSS styles. I have placed it inside css folder.

Simple example would be using favicon as “ico” to make it compatible with older internet explorer versions. I have done it in case of Eurostar website.

Every web browser is “injecting” some basic “agent stylesheets”. Those ones could be overwritten by using reset or normalize stylesheets downloadable form internet.

# Task 4. Any dynamic content in application can be ‘pulled out’ from a database in real time with optimal queries. Your application is expected to implement select, insert, update as well as read-only operations. (LO 2b, 2c).

Some of the forms I have used are just in the shape of buttons. In total I have many forms for customers and about twice as much for administrator for manipulating data in Eurostar database using carious techniques for example (in contrast to forms for messages and bookings) I have decided to build and display form for adding tours wrapped in modal box using mix of HTML,CSS (of course), w3 framework for styles, jQuery and a little bit of Bootstrap:

<button type="button" class="btn btn-default btn-lg" id="myBtn">Add tour</button>

Above is a trigger for showing the form.

<div class="container"> <!-- Modal --> <div class="modal fade" id="myModal" role="dialog"> <div class="modal-dialog">

<!-- Modal content--> <div class="modal-content">

<div class="modal-header" style="padding:35px 50px;">

<button type="button" class="close" data-dismiss="modal">&times;</button>

<h4>Add tour</h4></div><div class="modal-body" style="padding:40px 10px;"><div class="w3-container"><div class="form"><form class="w3-container w3-card-4" name="registration" action="" method="post"><h2>Input Form</h2>

<div class="w3-section"><input class="w3-input" type="text" name="name">

<label>Name</label></div><div class="w3-section">

<input class="w3-input" type="number" name="spacesleft">

<label>Spaces left</label></div><div class="w3-section">

<input class="w3-input" type="text" name="destination">

<label>Destination</label></div><div class="w3-section">

<input class="w3-input" type="date" name="date">

<label>Tour date</label></div><div class="w3-section">

<input class="w3-input" type="text" name="duration">

<label>Duration</label></div><div class="w3-section">

<textarea name="description" rows="10" cols="30">Description</textarea>

<br></div><div class="w3-section">

<input class="w3-input" type="text" name="photo">

<label>Photo</label></div><div class="w3-section">

<input class="w3-input" type="number" name="price">

<label>Price</label></div><div class="w3-section">

<select name="category" size="3"><option value=1>Economy</option>

<option value=2>Religious</option><option value=3>Firsty class</option>

<option value=4>Exotic</option></select><br><br><label>Category</label>

</div><input type="submit" name="submit" value="Register"></form></div>

</div></div><div class="modal-footer"></div></div></div></div></div>

And adding script below (apart of those, appropriate libraries have to be loaded to HTML inside HEAD tags):

<script>

$(document).ready(function(){

$("#myBtn").click(function(){

$("#myModal").modal();

});

});

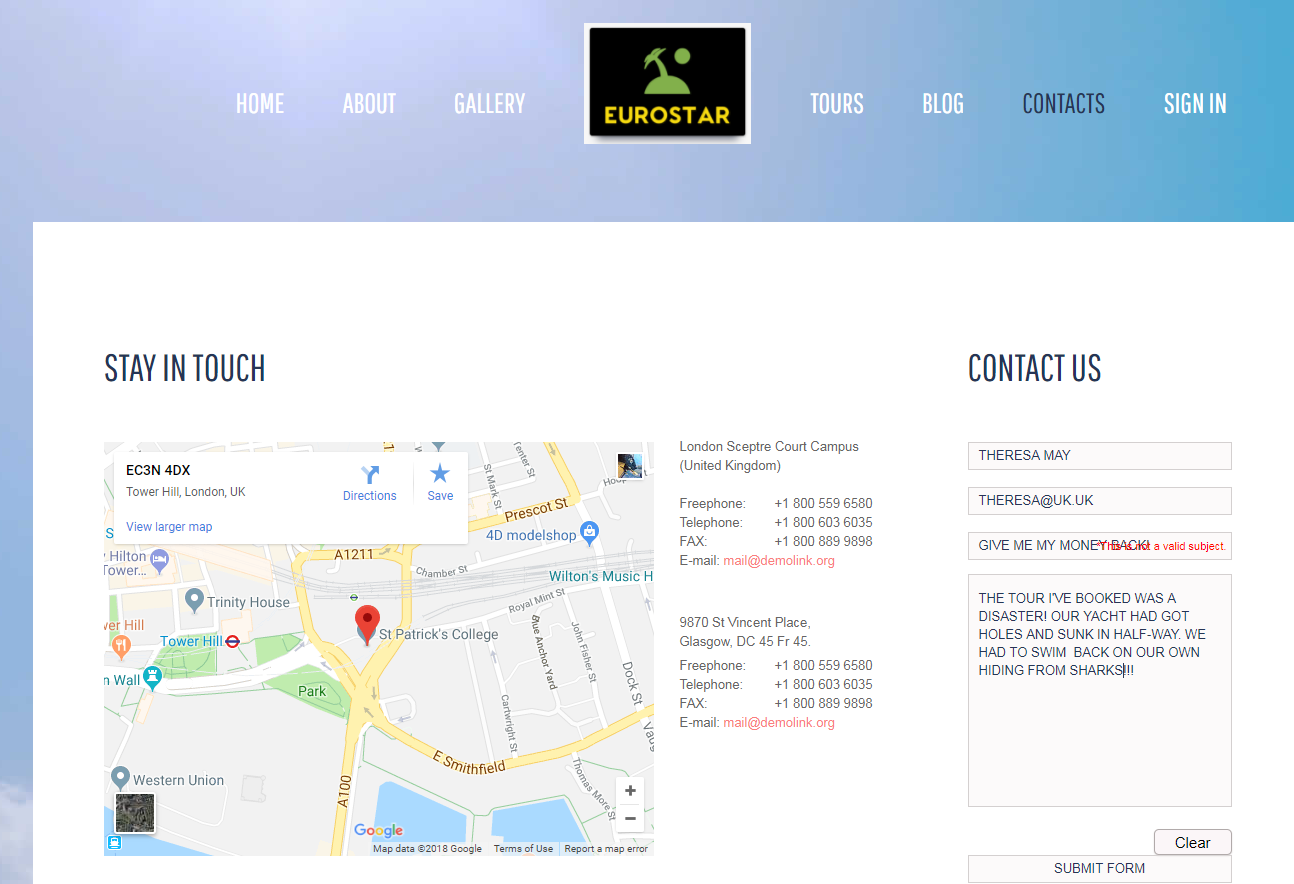
</script>

I have use quite different techniques for building table with Tours for customers and table customers inside dashboard:

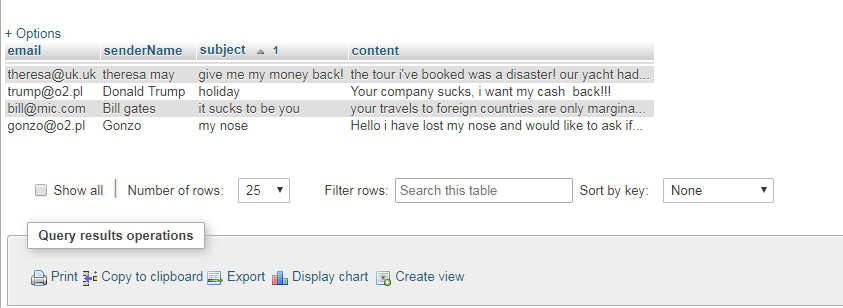
|  |  |
| --- | --- |
| Table tours from tourss.php page directed at customers and visitors. | Table customers from dashboard.php page for administrator. |
|  |  |
| HTML, CSS, Bootstrap, PHP, MySQL | AJAX, Bootstrap, jQuery, PHP, MySQL, JSON |
| Data in cells are inserted by direct PHP order. It is using “while” loop on the HTML table tags, drawing values from database by mysqli\_fetch\_assoc instruction. I have used INNER JOIN to display category name which was in other, referenced table. PHP is intertwined with HTML code. Booking operation is built on the HTML form submitting POSTs to external form-handler “bookingtour.php”. | jQuery is managing HTML by directing instructions to “id” selectors. The whole managing JavaScripts are outside in different place. By the way - It would be working even placed after </HTML>, I suppose that this is how “hoisting” of JavaScript works. To manage this table, I have created few PHP files to which the table is sending its requests. In contrast to tour table there is no HTML form. The data itself are travelling between PHP files by method Datatable() and are in json language. HTML “contenteditable” attribute is used to change data which is inside the given tag. That allows editing live table data in easy way. jQuery prepend method is used to add new records and inserting live data using PHP and Ajax. jQuery events, generated by Ajax requests are sending calls including database (crud) actions to server scripts. |

AJAX allows asynchronous page loading. The page can be updated without time consuming reloads.

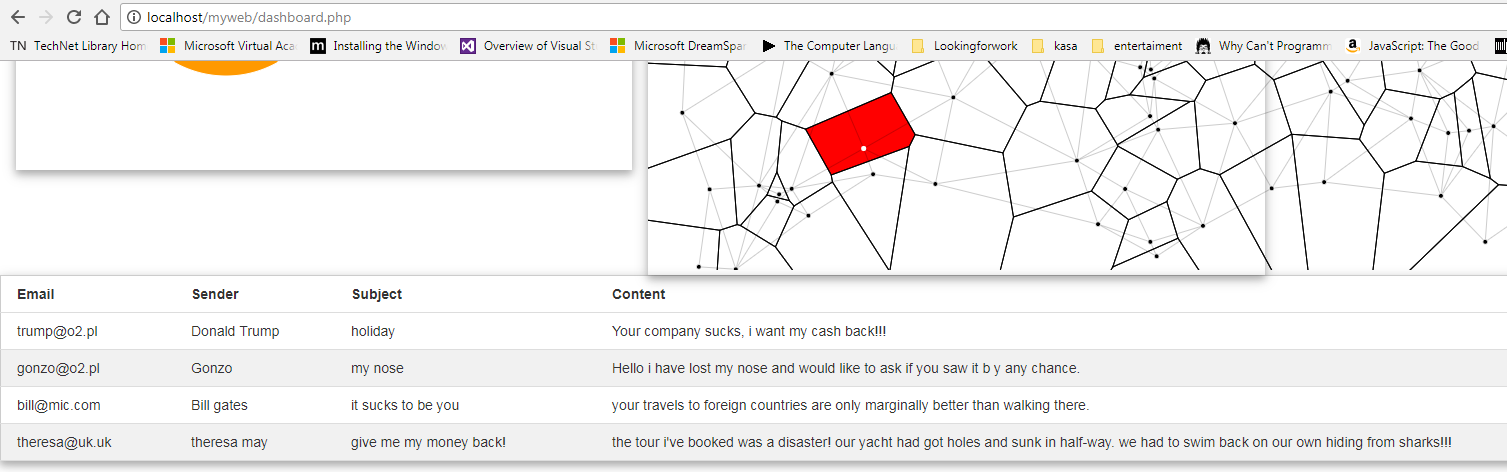
Here I will present Sending messages scenario, when visitor fill in the form, submit it to form-handler which is test.php. Data from there is using MySQL query to insert entry into messages table:



Form is then sent to database:

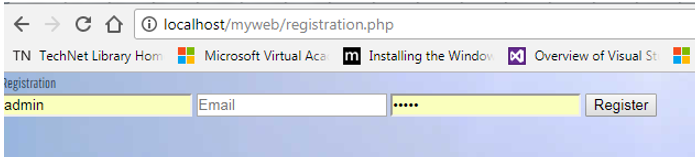


Finally, the messages are available for administrator to read:

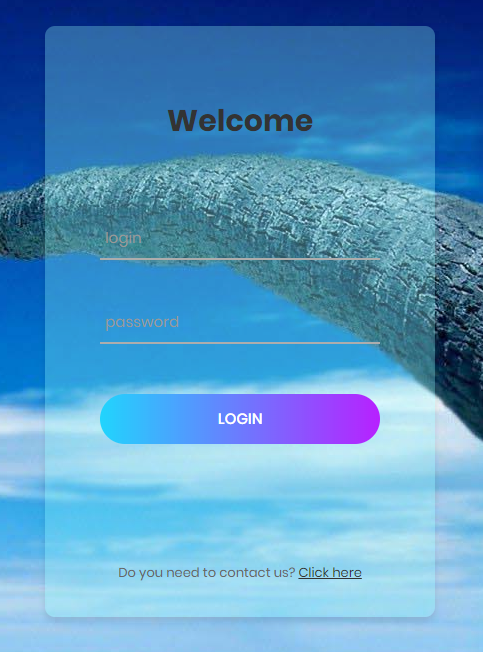


# Task 5. An authentication (e.g. sign-up and log-in) system to prevent unauthorized access. (LO 3a)

In my design I have assumed that dashboard administrator is a Eurostar worker and therefore the most suitable would be to give him/her credentials by the management. After that the dashboard can be accessible by clicking Eurostar logo or sign in link from the navigation menu. There is hard to create any smart plan for improving security by use of the online sign-up in case of Eurostar. Probably requiring some bank details that could be checked would be interesting idea. Something that would comply to multi-factor methods (such as famous, “something that user has, know or is”) Another option could be using Kerberos authentication but without those methods I don’t see how online registration using simple details like email address (with could be created in a minute) could be secure for dashboard or support significant functionality for customer so I have created and abandoned it. It has looked as follows:



My only authentication and authorisation case now is sign-in form on signin.php page which allows to enter dashboard:

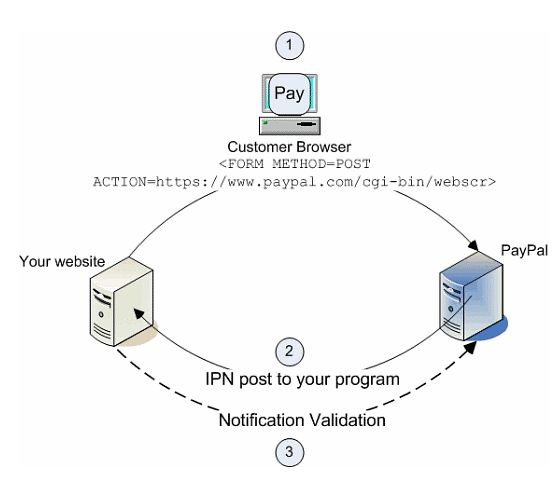


The action attribute for this form is empty which means that it is self-addressing.

As for customers payments authentication, Stripe and PayPal offer ready-made solutions. At the top of that Stripe gives complete e-commerce framework which include admin dashboard as well. I have included sample simulation forms for payments on the bottom of “bookingtour.php” page:

|  |  |
| --- | --- |
| Stripe |  |
|  |  |

And in the diagram below explains how PayPal’s Instant Payment Notification works:



# Task 6. The use of session, encryption to protect sensitive data (LO 3b)

The session() function allows to pass global data in GLOBAL array to different pages.

I have used session to pass global array with login and password to authenticate if the user has got correct login and password. I wrapped checking of the credentials in the auth.php file which investigate the $\_SESSION superglobals array. Now it is enough to add this file to every protected area on the website.

Although I have used POST and session methods I could have only use one of them. In the context of passing the data, session() is more an alternative to passing data by forms.

Session works by saving all the session data in special file (specified and changeable in the php.ini).

Session can as well works by sending cookie (PHPSESSID) with automatically created session key to the user.

For opening the session function “session\_start()” is used and it is storing a data in $\_SESSION array.

One example to show how it works is by checking how many time user was revisiting same page during the session:

<?php

session\_start();

if( isset( $\_SESSION['howoften'] ) ) {

$\_SESSION['howoften'] += 1;

}else { $\_SESSION['howoften'] = 1; }

$alert = "You have been here ". $\_SESSION['howoften'];

$alert .= "times during this session.";

?>

<html><head>

<title>Setting up a PHP session</title>

</head><body>

<?php echo ( $alert ); ?>

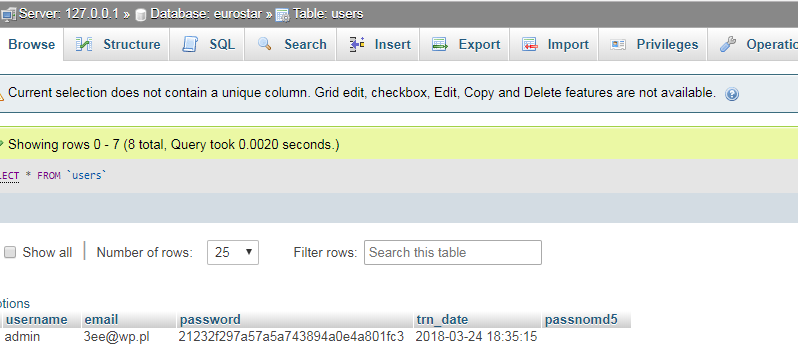
</body></html>

To close the session I have used:

* unset() to remove one variable from $\_SESSION array
* session\_destroy() to quickly and definitely finish session be clearing all variables.

They are invoked after clicking “log out” button from dashboard.

For encryption of the password I have used md5 algorithm:



# Task 7. Discussion on security threats and countermeasures (LO 3c)

There are many bad decisions that unaware (or ignorant) developer can make to threaten security of the website and there are gazillion ways to hack it. I doubt anybody knows them all and new exploits are being discovered all the time. I will try to give some Do’s and Don’ts:

* Do validate the form to prevent SQL injections. Remember that despite of plenty methods, existing to validate entry on the front-end, it is not enough and “true” validation can only be done on back-end. Validation in PHP could be looking las follow:

$name = stripslashes($\_REQUEST['name']); // removes backslashes

$name = mysqli\_real\_escape\_string($con,$name); //escapes special characters in a string

* Do test website. There are many methods available such as penetration testing.
* Do follow “fail securely” guideline which means to predict possible error and prepare a way to handle it beforehand to reduce chance of possible exploits of exceptions. if isset($\_POST['username'])){…}
* Do guard Against XSS Attacks – similar to SQLinjections.
* Don’t use GET method to send sensitive data.
* Do protect session data. On shared hosting there are written down in shared folders.
* Do update your software frequently and in time.
* Do use HTTPS protocol.
* Do manage file permissions wisely.
* Do use secure passwords.
* Do use firewalls, anti-malware software and other security applications.
* Don’t show admin pages for example by discouraging Search Engines.
* Do back up frequently. It possible to do this manually by exporting database, and downloading content, or by using software (sometimes free sometimes not) which is doing that automatically.

# Task 8. Evidence of system testing: actual result of system testing and acceptance testing for your development. (LO 4a, b)

Any modern browser nowodays offers some form of testing website even without being live.

For example using developers tools in Chrome it is possible to test responsivness:

|  |  |
| --- | --- |
| Galaxy S5 | iPad Pro |
|  |  |

Front-end appearance on different devices.

Chrome has many other tools, another example is testing CSS and HTML structure, functionality and interdependencies.

In console it is possible to run JavaScripts, even interacting with the view (static of course-any changes will not be physically saved).

Audits help to fix common issues with performance, UX or accessibility.

Allows to have a glimpse on Web manifest…and many, many more without even mentioning plugins and extensions.

Activating memory tab allows to check resources usage.

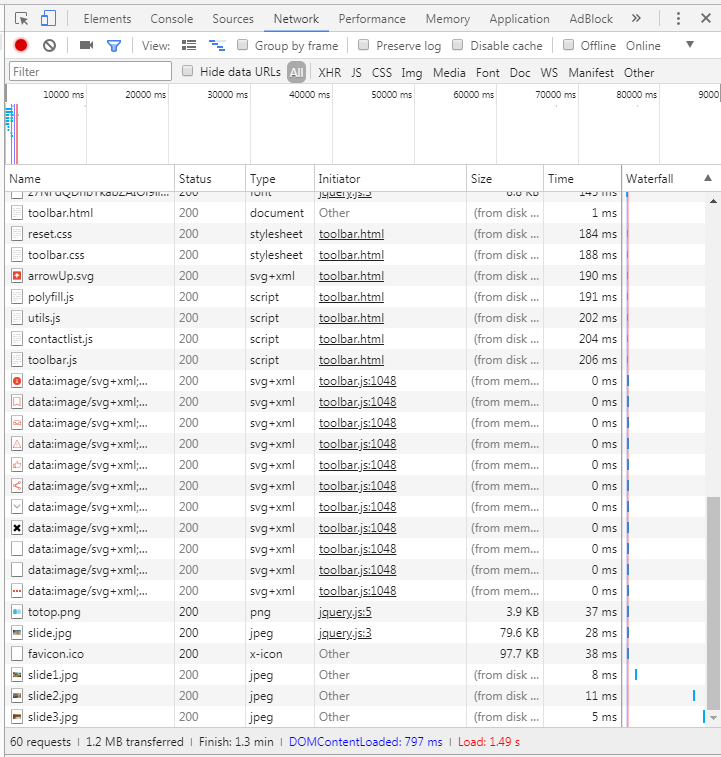
Network tag is used to check loading times, number of requests sent.

Below I will show 2 examples of how helpful it proved to be to me.

Example 1.

It was very helpful to me when I had problem with TTFB (Time To First Byte) while making website in Wordpress. Due to badly configured CDN, cache management and too many unnecessary requests to server, loading time was unacceptable, mainly due to long TTFB. TTFB measure time passed between starting requests for the site and receiving first byte if response. That knowledge helped me greatly to narrow the range of possible culprits.

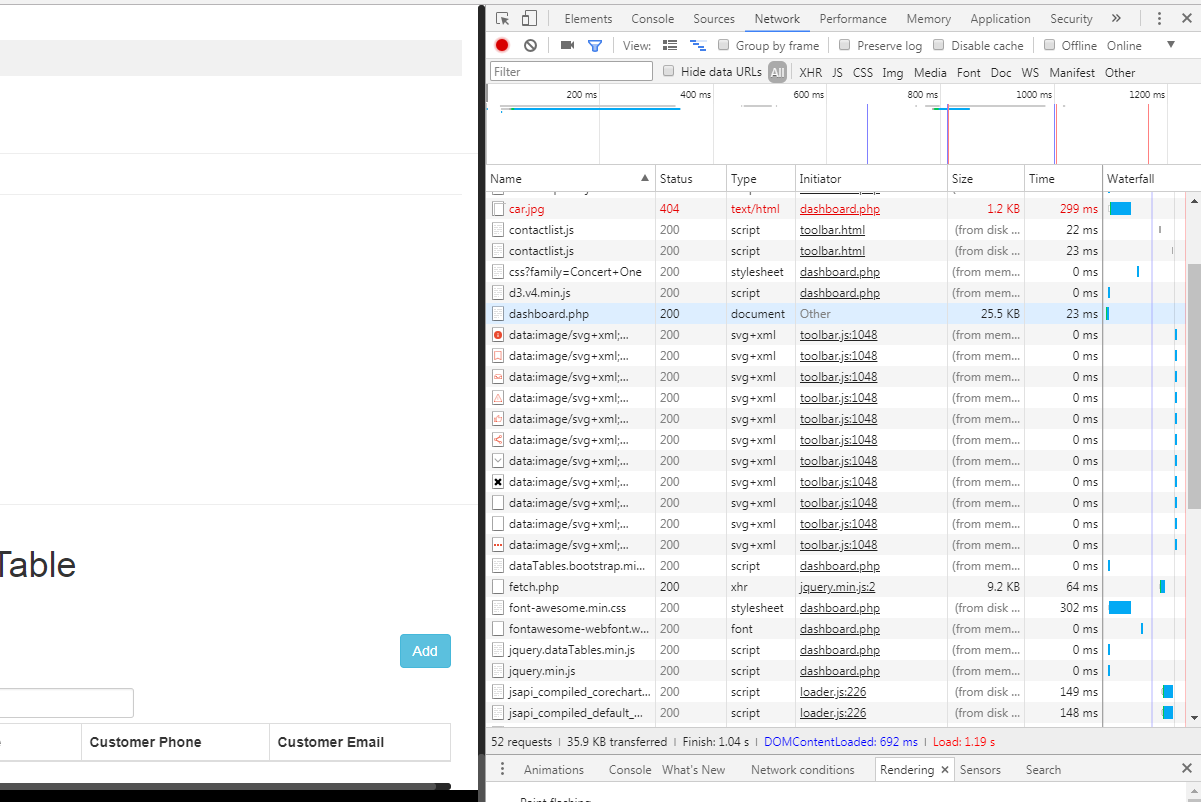
I have reduced number of requests, installed W3 Total Cache Wordpress plugin, minified CSS, JavaScripts configured properly server, htaccess etc. and finally managed to increase speed to acceptable level.



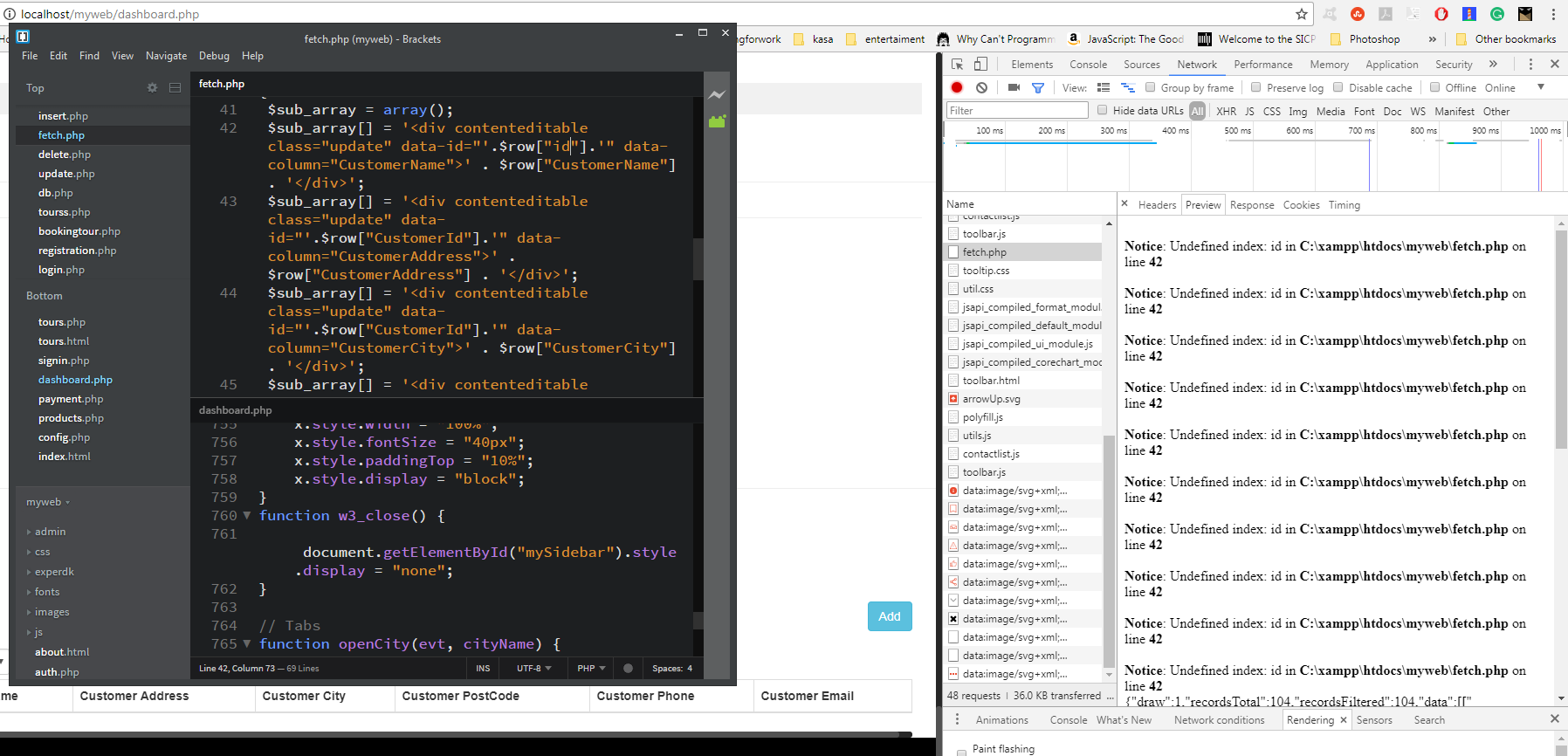
Loading time while site was still on my hard drive.

Example 2.

During my assignment I have encounter difficult error to debug while programming customer table in dashboard. That was the first time when I was using Json and jQuery and this fact has increased my confusion about the source of the problem even more. DeveloperTools helped me to noticed mistakes in entities names I was using in querying database from fetch.php file.



By the help of the Network analytics (it is important to remember about caching, if it is not disabled it could lead to strange and unpredictable results)which investigates the requests sent to the server I have found out that the problem lays inside mentioned earlier fetch.php:



In addition to Chrome Developers tools I have used some free online tools available to testing different aspects of websites. I have to admit that since this is my first dynamic website, a huge part of which I have programmed myself I have not got enough time to take care about the neatness syntax. I know that everything works more or less but I am sure as well that insides of the code are in a big mess and I should not expect high outcomes. Some files are not being used at all, because there are just outcomes of my experiments. Free, shared hosting will surely not give any advantages as well.

Before I had a chance to test my live website I had to face one surprising error – some of my relative links were broken after migration to live server. What was confusing me the most, was the fact that not all of them were affected but only a few (which was enough to damage visual experience though). I could not find out what logic set of rules this system could possibly follows. It took me another day to resolve this unforeseen riddle. The problem was caused by using upper cases in files extensions. For some reason 000webhost had problems with correctly recognising those files. How many work hours was lost in total by other people encountering same problem I wonder. Shouldn’t it be clearly instructed by 000wehost on their webpage? Anyway I change the extensions and the pictures start linking correct (two alternative way to correct that could be by moving all files in one folder or I guess playing around rewrite rules in htaccess)

Unfortunately, that wasn’t the end of the story. My pictures were loading correctly but navigation menu in the header was still messed up.

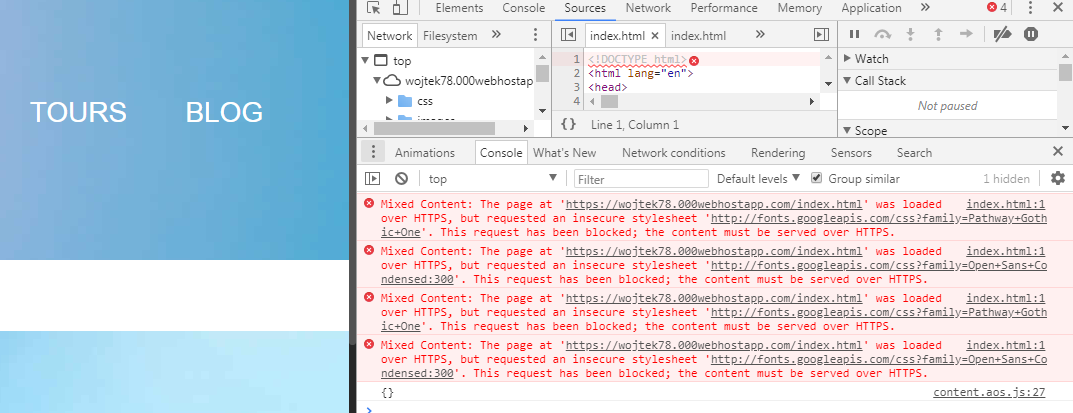


0‑1 Live version

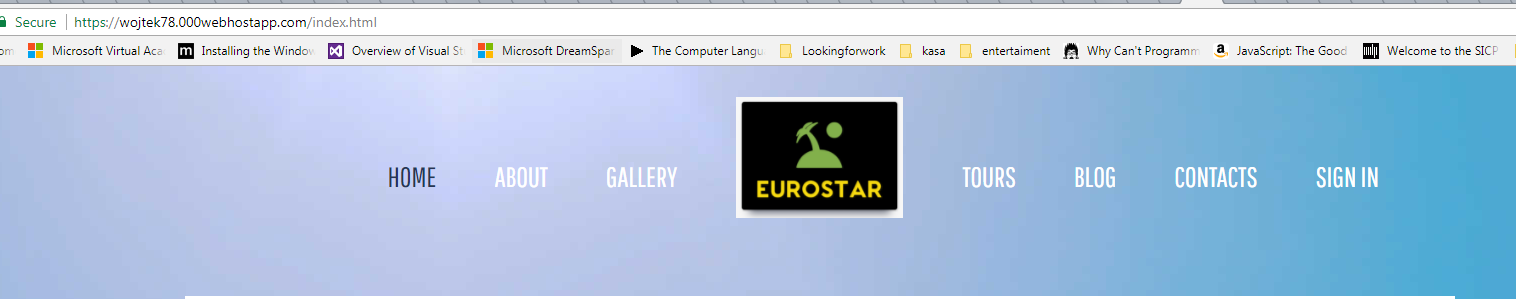


0‑2 Local version

Developer tools come to help again and showed that there were 4 errors indicating problems with the fonts requests:



Fortunately goggle provides https alternative altogether, so what was needed to do was to find style file responsible for importing fonts. I have found out it is style.css, after adding two letters ‘s’, finally everything looks fine:



The last step was to repair all the requests in every file comprising my website. It could be daunting and long task in itself but if not the function of my editor (brackets) allowing to replace any string in all files from the project.

Although those problems are not connected to database directly, nevertheless would have terrible impact for user experience and acceptance of this e-commerce system therefore I have decided to shortly describe them.

# Testing database functional requirements.

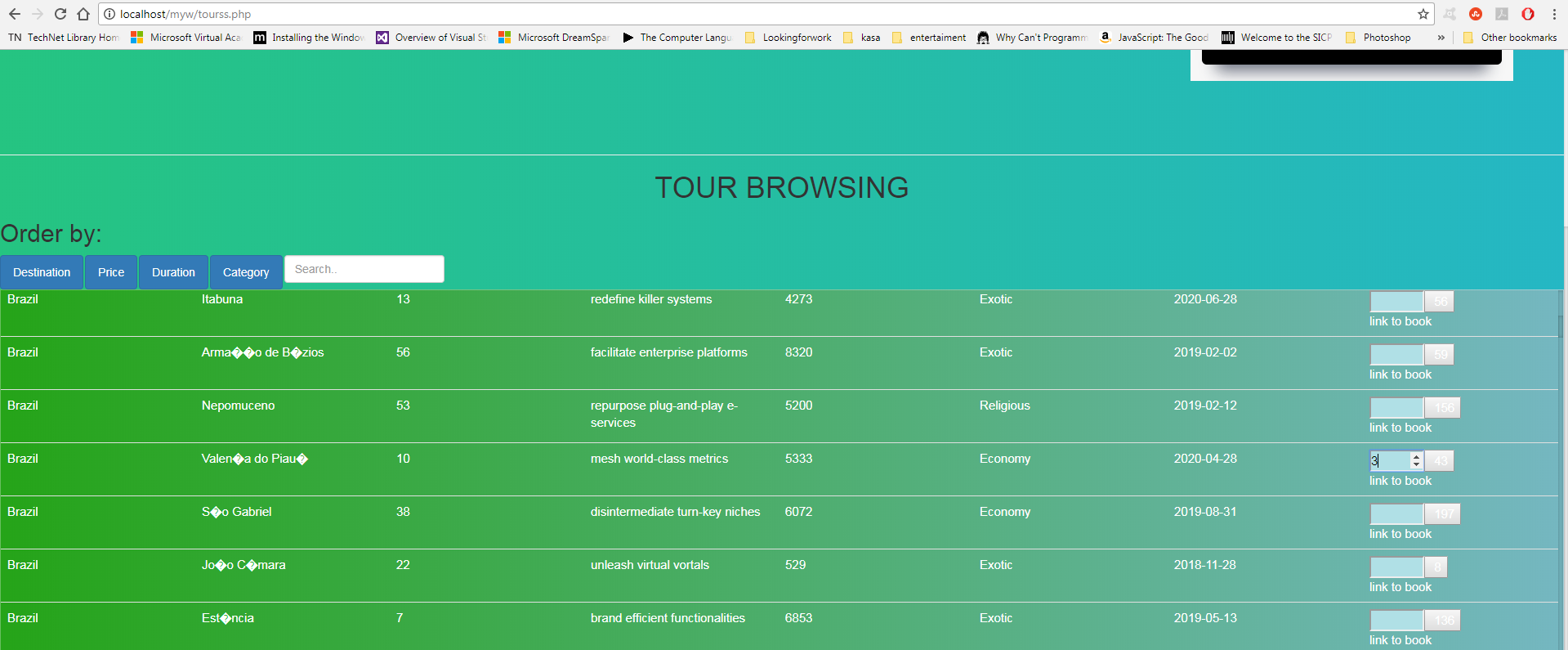
In this final part I will test the most important needs that the Eurostar website must fulfil:

1. **Customer should be able to browse for tours based on several criteria and book the tour he/she likes tour.**

I have made two main form of booking the tour namely from the map and from the table.

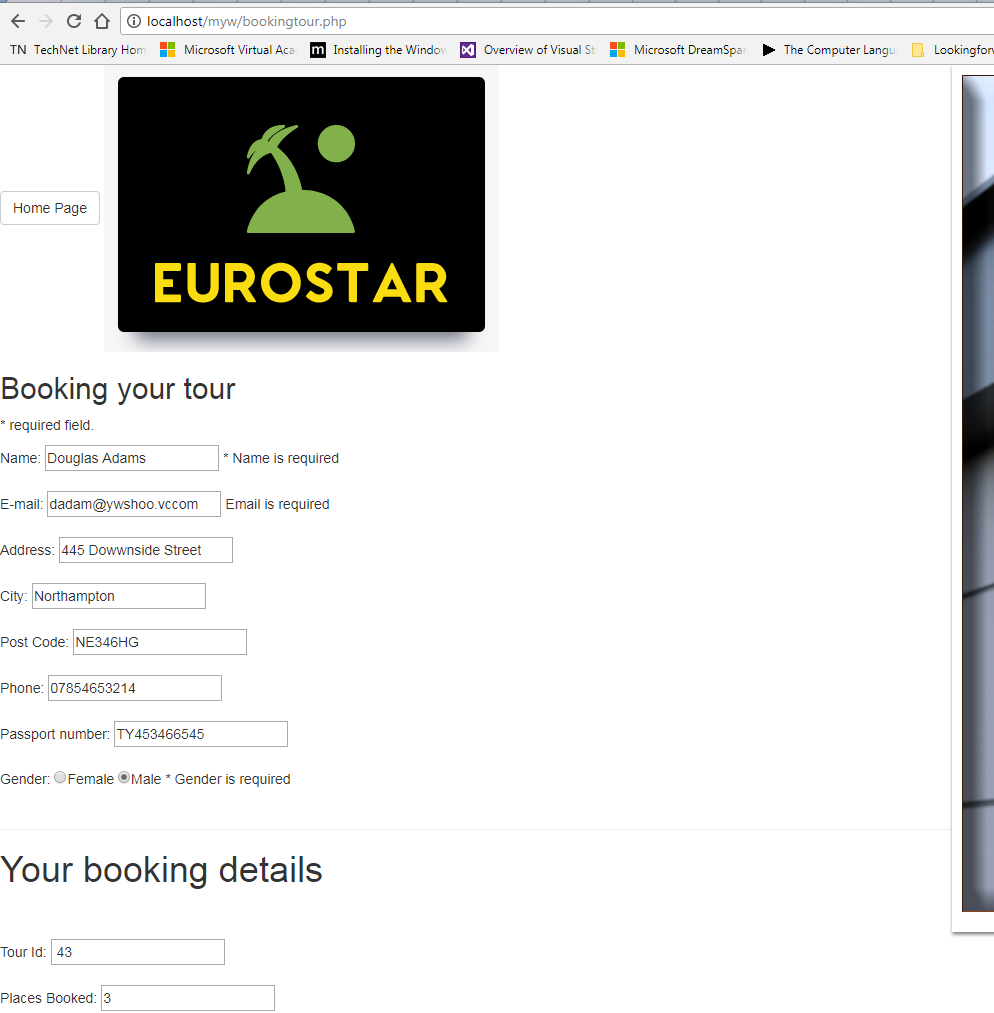
First, I will test table option tours.php:

Opening tours.php page, I will book 3 places to Brazil for 5333 (let’s say pounds):

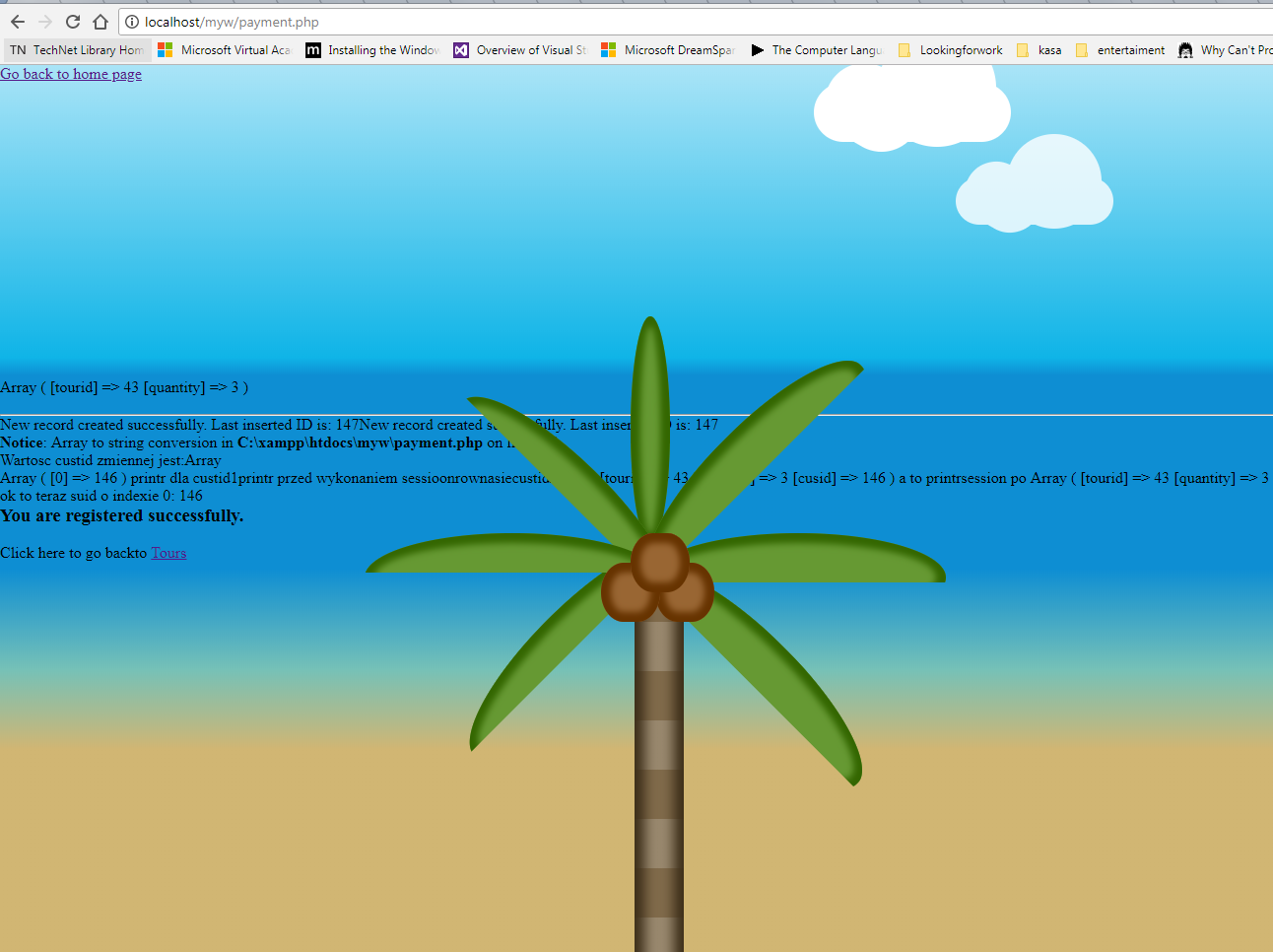


While being on this page, customer can sort the table according to several columns, here I have programmed 4 possibilities. I have used simple Bootstrap technology here to display different HTML blocks targeting containers classes. In each of those blocks there are different PHP segments, looping over the query to MySQL with different “order by” attribute. The last cell in each table comprise a form which sends request with Tour Id and quantity to bookingtour.php. In the form I have implemented max attribute and in the result, it is not possible to book more tours than there are places left.

After going to bookingtour.php, customer can see the form to book the tour. The Tour ID nad quantity data are already placed from the form before. Some basic validation is provided by using preg\_match(), trim(), striplashes(), htmlspecialchars() functions.

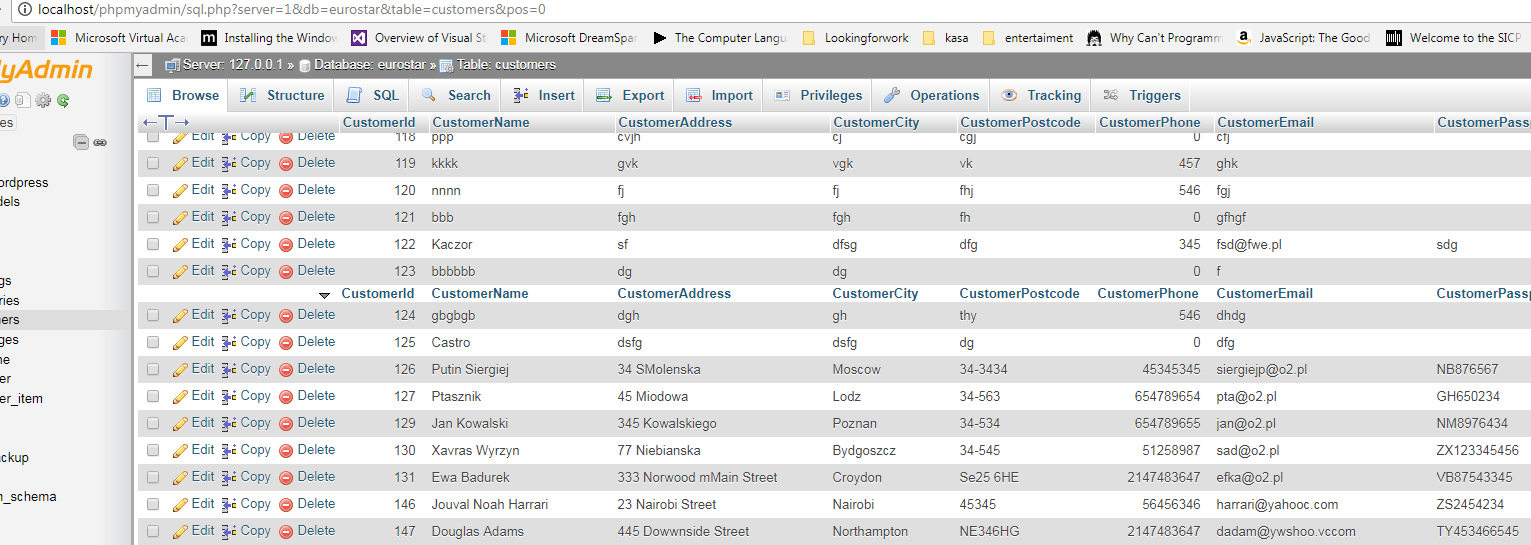


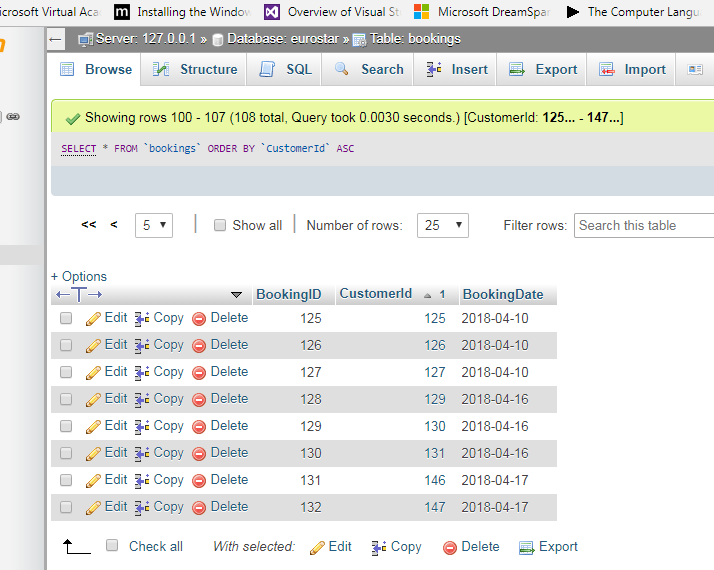
After clicking submit button, the confirmation is displayed:

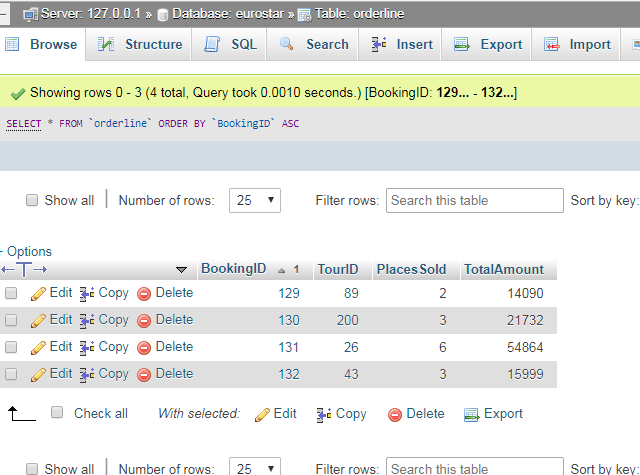


I also have checked data in phpMyAdmin to checked if everything works how it is intended:

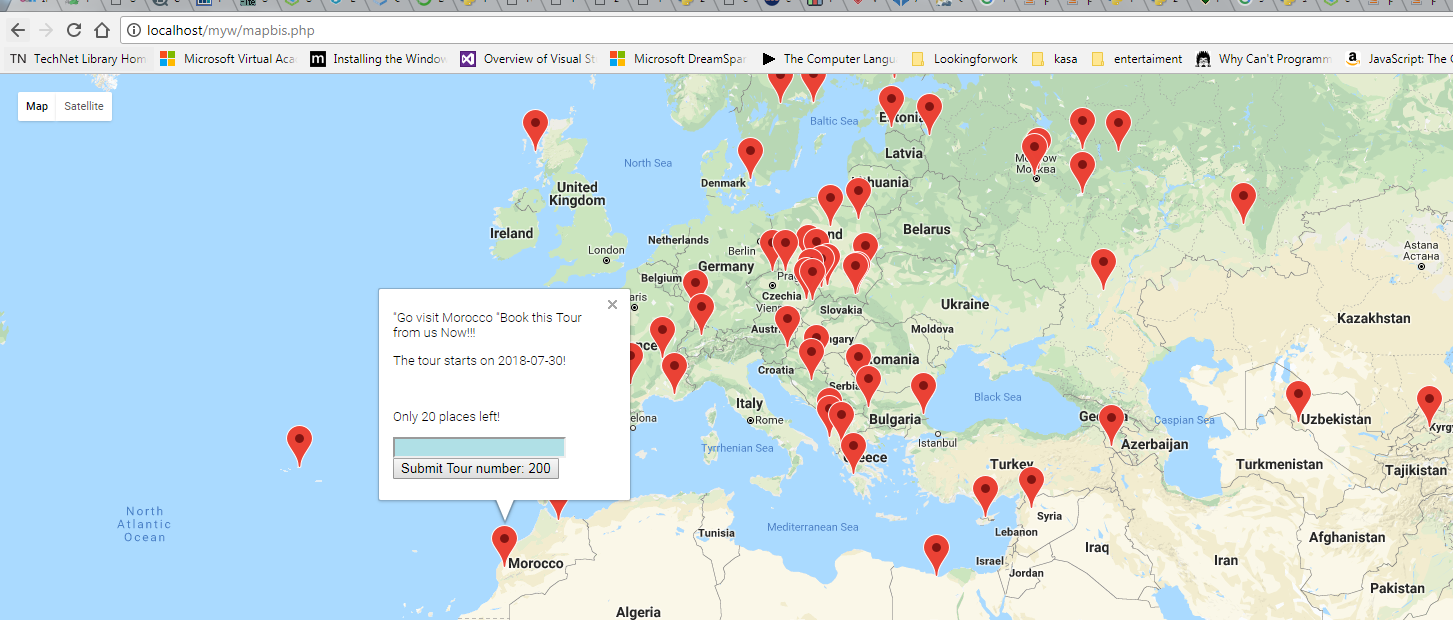
After booking there is new booking and order line records automatically created:







I have done similar testing from map page:



It has tested successfully (after going through similar steps as in table scenario to bookoingtour.php). Total amount is multiplied by quantity and the total places left is reduced.

1. **After booking tour, the total quantity of spaces available should be reduced.**

Is fulfilled by a).

1. **Administrator should be able to add and to delete tour.**

For this I have used Boodstrap modal module. After Clicking the “Add tour “ button, a entry form is displayed. I have tested it and it is adding new entry to tour table.

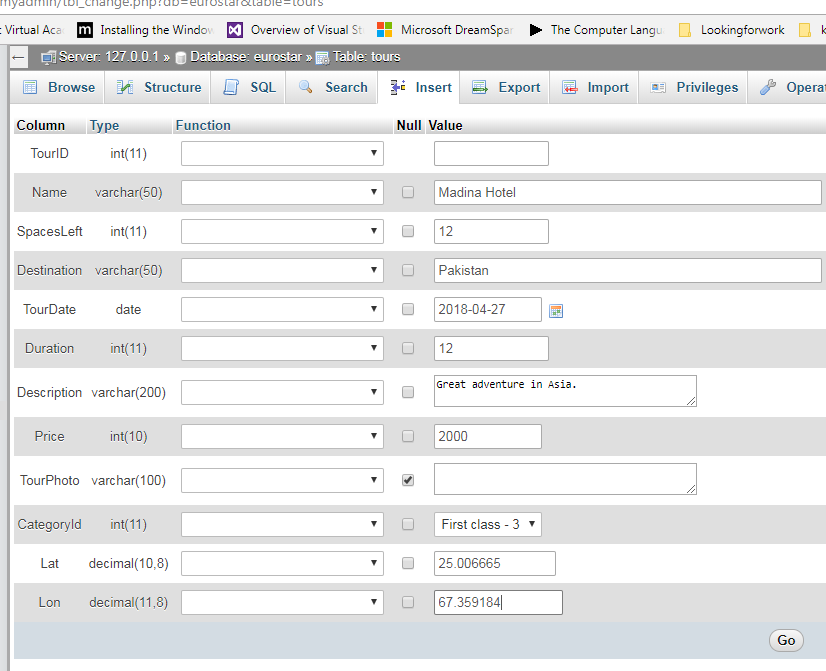
I have not implemented delete option because I think that tours with quantity 0 could be considered as deleted. Of course, that would have to be discussed with stakeholders and possibly added easily if really needed.

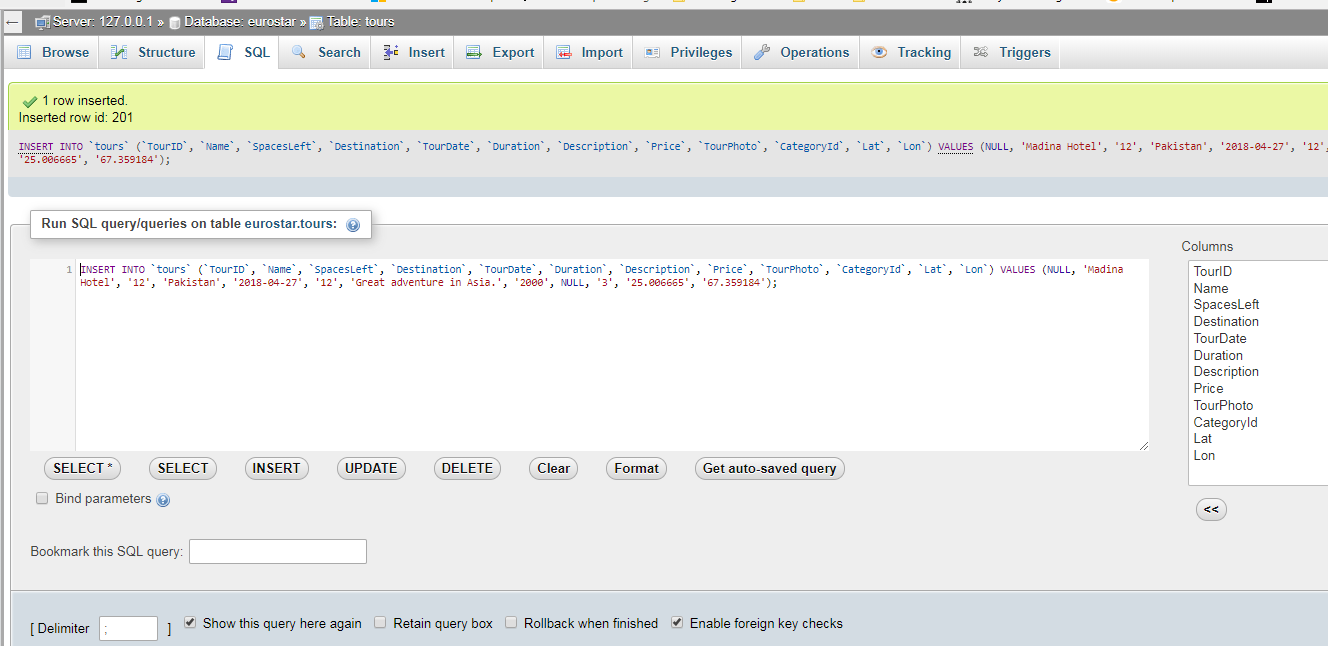
1. **Security testing.**
2. **Customer should be able to send messages to Eurostar and administrator should be able to read them (that was checked in task 4).**
3. **I have added additionally customer table in dashboard.**

I have tested that and it is updating corresponding database entries correctly.

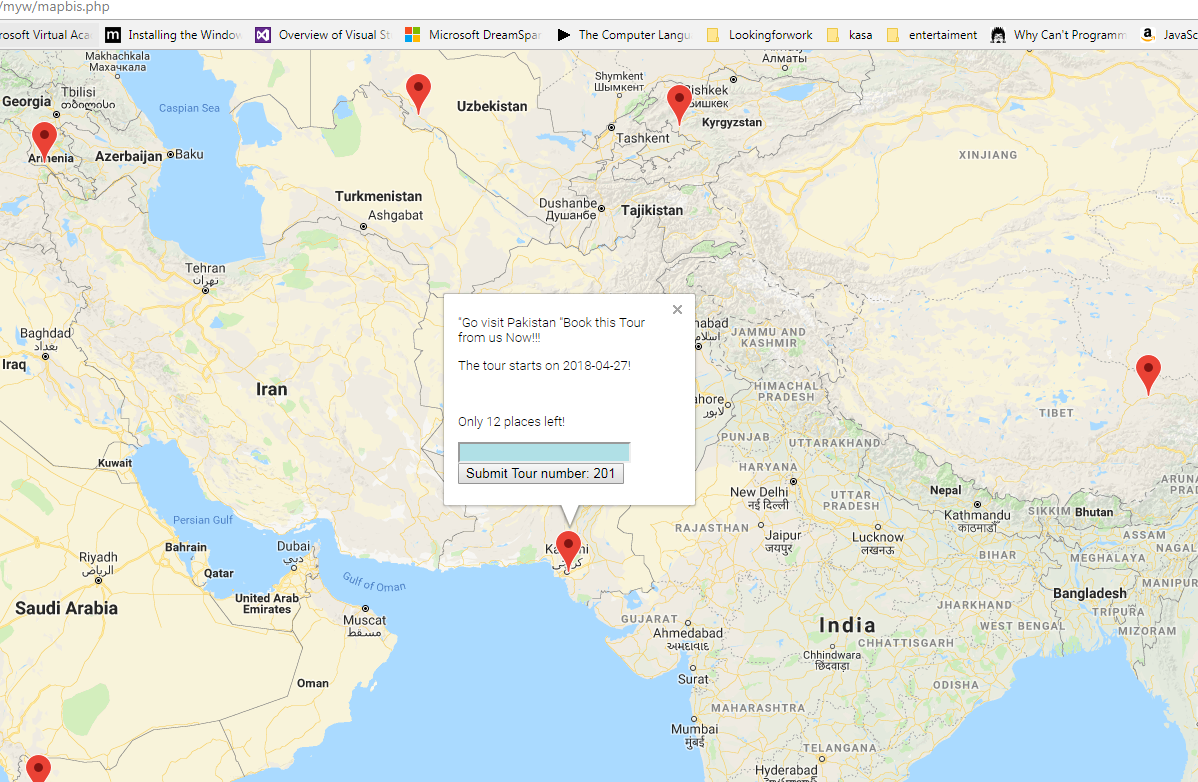
1. **Map update testing**

I have performed a test, checking if there is new marker on the mapbis.php map after adding new tour.





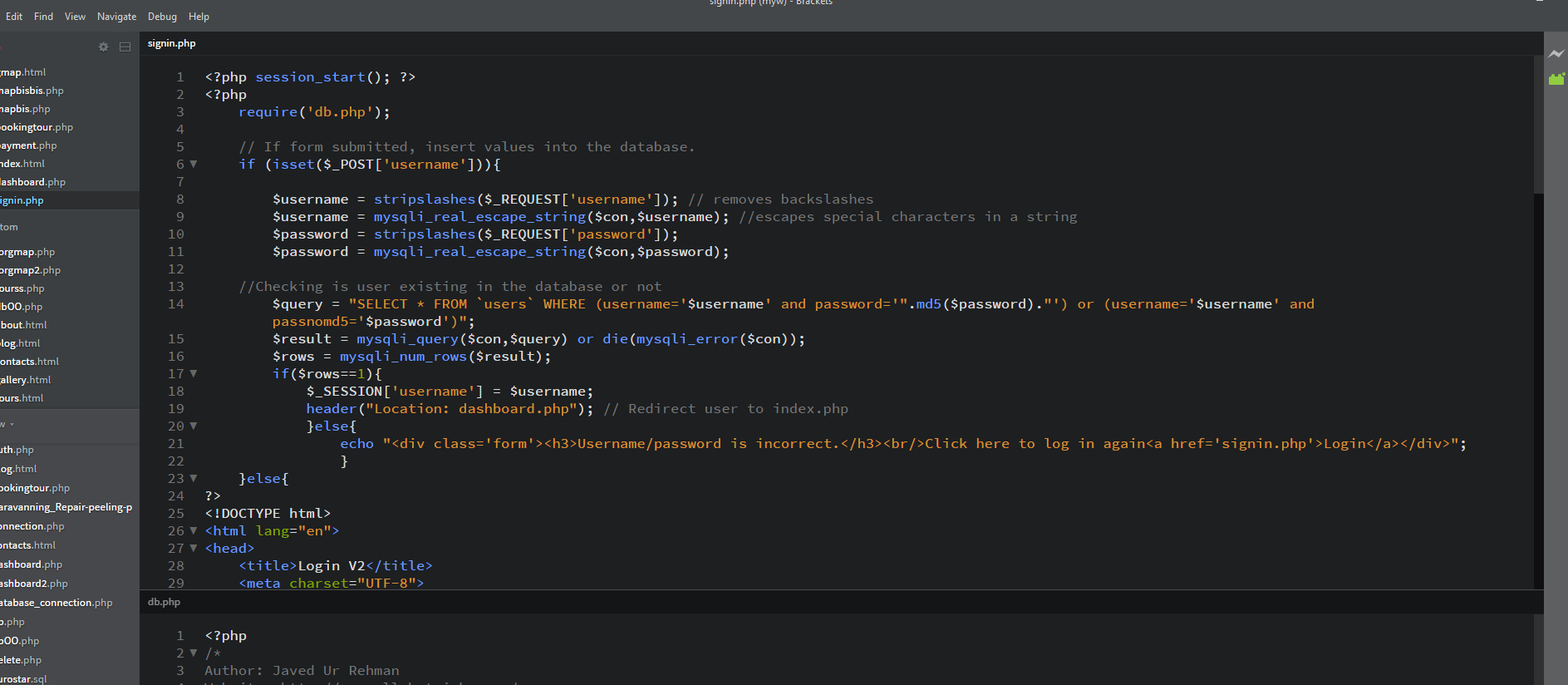
New tour is added automatically on the map:



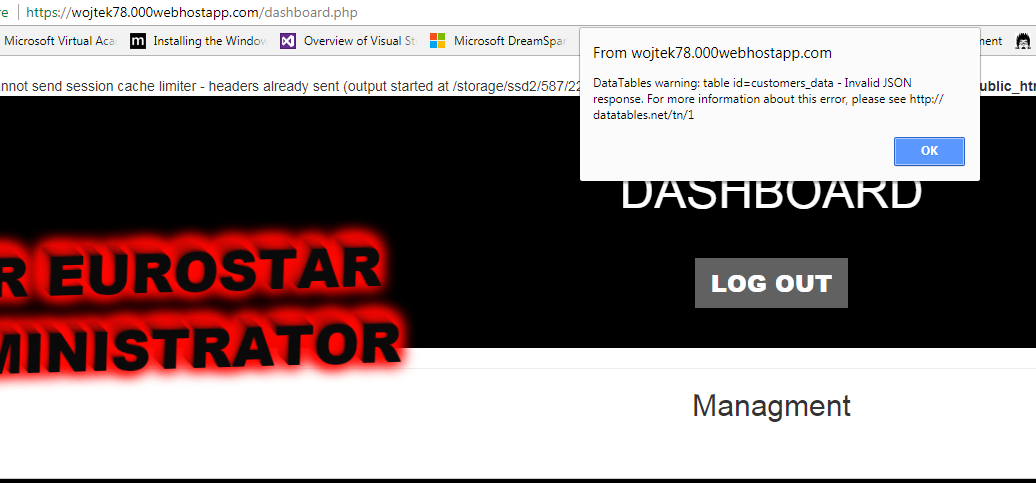
Testing live website:

I have uploaded website on the hosting server 000webhost and from the start I have encounter first problem with the back-end.

1. “Headers already sent” error in “signin.php” file. Source of this one came from me not taking seriously the manual. Some function in PHP must be executed befor any HTML output happens. Situation was improved by moving block of PHP code to beginning of the file.
2. Now, the problem is in error message giving me alert that username and password is incorrect before I even had a chance to log in. I didn’t have any other choice than to start analysing the code again. I realised that the problem is not in how the code (the same I have move up earlier) is written but that it is written:



After removing the unnecessary code, (practically the whole PHP part), finally I can see the dashboard and experience another adventure with the problem number 3:



1. The dashboard page open with the monit *”DataTables warning: table id=customers\_data - Invalid JSON response. For more information about this error, please see* <http://datatables.net/tn/1>*”*. This problem led to another, this time with my 000webhost account. Shortly after I have tried to make changes to my 000web host account files, my file uploader has stopped working. Repairing and even resetting the website wasn’t improving the situation so for a time being at least I decided to move my website to new hosting from Siteground (which I was going to do anyway). The new details are:

URL: wojciechk.sgedu.site

Conclusion

I have found the subject and the assignment very interesting. Despite moments of frustration (for example spending around 10 hours debugging the code after making simple mistake in HTML form) I have enjoyed it a lot. Each problem I have encountered and resolved (from which only a few I have described here) has taught me something valuable.

I can see many areas of improvement for which I have not got enough time. If I had, I would be thinking about implementing:

1. More diagrams form Google charts for administrator to visualize data flow. At the moment there is only mock-up on the dashboard.
2. Invoice management, automatic creation, sending to customer.
3. Implementing the real paying method with PayPal/Stripe/
4. General improvements and clean-up.

©2018 Add2Net, Inc., 2014. *www.lunarpages.com.* [Online]   
Available at: https://lunarpages.com/apache-vs-iis-which-web-server-should-you-choose/  
[Accessed 17 02 2018].

Anon., 2017. *www.tutorialspoint.com.* [Online]   
Available at: https://www.tutorialspoint.com/sdlc/sdlc\_quick\_guide.htm  
[Accessed 09 12 2017].

Anon., 2018. *w3techs.com.* [Online]   
Available at: https://w3techs.com/technologies/overview/web\_server/all  
[Accessed 09 02 2018].

Armando Padilla, D. H., 2010. *Pro PHP Application Performance: Tuning PHP Web Projects for Maximum Performance.* New York: Apress Paul Manning.

Bhatwada, B., 2018. *www.webslesson.info.* [Online]   
Available at: http://www.webslesson.info/p/contact-us.html  
[Accessed 10 04 2018].

iPage, 2017. *www.ipage.com.* [Online]   
Available at: https://www.ipage.com/help/article/online-security-hacking-and-malware  
[Accessed 01 12 2017].

mozilla.org, 2018. *mozilla.org.* [Online]   
Available at: https://developer.mozilla.org  
[Accessed 10 04 2018].

Swithinbank, P. et al., 2008. *Planning and Managing the Deployment of WebSphere Commerce.* s.l.:Redbooks.

Ullman, L., 2016. *Effortless E-Commerce with PHP and MySQL.* 2nd ed. s.l.:s.n.

W3 Consortium, 2017. *https://www.w3schools.com.* [Online]   
Available at: https://www.w3schools.com  
[Accessed 21 08 2017].

www.owasp.org/, 2018. *https://www.owasp.org.* [Online]   
Available at: https://www.owasp.org/index.php/OWASP\_Testing\_Guide\_v4\_Table\_of\_Contents  
[Accessed 10 04 2018].