Razat Kaur
P2508373

The Vulnerability Analysis of Industrial Control Systems

Contents

Razat Kaur
P2508373

Abstract

Studies have shown that there has been an 2000% uprise of attacks since 2018 in the Industrial control system assets. These attacks involve “a combination of exploiting known vulnerabilities in supervisory control and data acquisition” (Bisson 2020). In this review, I will be exploring the vulnerabilities that ICS face in different major infra structures such as Oil and gas, electricity, and water distribution. Furthermore, I will talk about the effect it has on the economy and society and provide potential solutions that may be implemented to reduce the attacks. Major infrastructures are especially vulnerable as hackers get more sophisticated. This is due to the lack of cyber security measures which allows for attacks such as ransomware, phishing, and social engineering to occur. Additionally, password spraying attacks have also increased which is a traditional brute-force attack that attempts to gain unauthorised access to an account by guessing the password. As most ICS use default password, this makes it easy forthe hacker to gain control of the account which subsequently could give them unauthorised access to physical systems of the ICS. I have found this is one of the biggest vulnerabilities that the ICS faces: weak password protection. As hackers get more sophisticated, it becomes easier for them to attack the systems. This issue must be tackled quickly as infra structures such as water distribution are critical to human life.

Literature Review

In this literature review, I will be exploring ways in which industrial control systems are used across the world and how they are vulnerable against cyber-attacks. I will explore the different architectures used within each control system and the vulnerabilities they have. The Supervisory Control and Data Acquisition (SCADA) systems are made done without security in mind. As now, SCADA systems are used to carry some data over the internet, they are prone to cyber-attacks. The maximum security implemented is the use of a username and password with no encryption of the data being carried across the internet. The data can easily be interpreted. I will be reviewing different ways in which the industrial control systems may be able to overcome the vulnerabilitie s.

An industrial control system is a general term used to describe the combination of hardware and software components with network connectivity to support the different infra-structures that they are found in nationwide. One of the biggest infra structures that control systems are used in is in the electrical industry. The control systems are described as the “sauce of electrical engineering” (Lawkay 2018). There are several different ways in which control systems are implemented within the electrical industry. One of the most common that is used across the world is a power switch. Lawkay illustrates this as an open loop system and goes on to explain that once the switch is given an input, “it doesn’t stop executing that command for any set of output conditions” (Lawkay 2018) meaning no matter what time of day it is, the switch will always stay on. Although a small circuit, it shows the bases of how a control system was used and how this technology has been improved and used in large scales. A power switch does not need much security however when control systems are used in larger scales, it begs the question of how secure they really are.

A larger scale example of an electrical control system is the electric power generator. Due to the lack of security measures, there was “an attack on the electric power system” (Farrell A.E., Zerriffi H, Dowlatabadi H 2004) which had led to a blackout in 2003. Attacks such as phishing and password spraying had allowed sophisticated attackers to gain unauthorised access to the IT servers and in combination with the vulnerability of high-voltage transformers within this infra structure resulted the city to experience a black out. Most companies encourage “efficiency, invested cost utilisation and return on investment” (Farrell A.E., Zerriffi H, Dowlatabadi H 2004) rather than the security and reliability of it. A successful attack would cause detrimental damage to capital infra structures such as blast furnaces and it will disrupt “vital services for e.g., health services and water supply” (Farrell A.E., Zerriffi H, Dowlatabadi H 2004). This has a massive impact on society causing the country to lose out on millions in money. The cost to repair the damage as well as dealing with the backlash of vital services being disrupted causing detrimental effects, is time consuming and has a negative effect on the economy. There are security guidelines that may be implemented for the physical and cyber security of vast power generating companies. One security guideline is having a “threat response capability”(Watts D 2003) which will, as well as alert the company of how dangerous the attack is, it will also “suggest specific actions that may be appropriate” (Watts D 2003) to overcome it. Companies that are responsible for major infrastructures should have better security against cyber-attacks considering the negative effects of an attack are detrimental to the economy, both in short and in long term.

One of the other major infrastructures that control systems are used in is water distribution. Water distribution systems have the objective to transfer drinking water to consumers through a series of complex networks which consists of structural elements for example tanks and pipes, sensors to measure quality and pressure, and actuators such as pumps. Attacks are the exploitation of the vulnerabilities in the industrial control systems implemented in the infra structures. The vulnerabilities in the software such as Supervisory Control and Data Acquisition are what causes the attackers to gain access to the physical attributes of the system. The attack that occurred on the Kemuri Water company in 2016 which “resulted in the exposure of personal information of the utility’s 2.5 million customers” (Adepu S 2017). SCADA system is often used for the application within the water distribution and used from a computer running on windows 7. This is an older version of windows which does not have the new features that may enable better security. The manufacturers all use default passwords and as the authors explain in the article that the “during the installation and configuring period” (Adepu S 2017) the default passwords are not changed. This exposes the system to phishing as the “attacker can use those default passwords from each manufacturing unit and exploit the system” (Adepu S 2017). This is a good way of understanding the level of security in place currently and raises concern as one of the biggest infra structures have the most basic security levels. I believe not enough security measures are in place in making sure that the water distribution is safe from cyber-attacks.

Additionally, the water distribution systems are the most critical infra structures as it is “importance to human life” (Pollert 2006). It is suggested that there is an “urgent need to develop emergency response plans” (Pollert 2006) which is similar to what Watt suggests in his article. Perhaps for the water distribution, there may also be a threat response capability put in place which will detect and alert authorities when an attack has occurred and furthermore give appropriate actions to counteract it. Although within this infra structure, there are several networks involved in distributing water and handling each component in the water supply system so implementing new security measures will be expensive and time consuming thus less appealing to businesses. There are less developed countries which have taken on the intermittent water supply system as a way of controlling the water demand in their country. Furthermore, it is suggested that the “adoption of intermittent water supply systems aggravate urban water insecurity” (Aboelnga 2018) which meansit does not consider the impact it has on the condition of the water supply systems and on public health. This system costs more and people are not willing to pay for it therefore the need for more staff is not met. As staff is less and there is inadequate water for towns, the system becomes corrupt allowing “the most privileged to take matters in their own hand” (Aboelnga 2018) and allow them to get the water in other ways. The water supply system like previously discussed has little security against cyber-attacks and therefore can be hacked and altered by people who have enough money to ensure they receive sufficient supply of water. I believe this is unfair for the working-class people and furthermore it may be the reason for uprise in deaths in the less developed countries.

The final major infra structure in which control systems have been implemented that I would like to discuss is within Oil and gas. Although most people believe that this side of the industry is not targeted as much, it has rising cybersecurity risks. There is “only a handful of energy companies that cite cyber breaches as a major risk” (Mittal, Slaughter, Zonneveld 2017) which means majority of the companies believe that a cyber-attack is not a major risk and therefore do not have the means for quick recovery if an attack should occur. Companies believe that the business of handling crude oil and gas “is about barrels, not bytes” (Mittal, Slaughter, Zonneveld 2017). However due to the vastness of the industry, “half a million processors” (Mittal, Slaughter, Zonneveld 2017) are used just for the oil and gas reservoir simulation. Therefore, this causes it to be highly vulnerable to cyber-attacks. Additionally, the ICS software used are often not chosen by the IT team but chosen at the unit level causing them to be used for decades without being replaced for better technology. The companies suggest due to the “remote operations and complex data structure” (Mittal, Slaughter, Zonneveld 2017) that this will provide as a natural defence however in recent years, the cyber attackers have grown in frequency and sophistication thereby easily hacking into the ICS computers.

Research shows how the world’s biggest oil producers “Saudi Aramco and Qatar’s RasGas” (Clayton, Segal 2013) fell prey to cyberattacks since 2009. An attack such as ransomware targets big infra structures and due to lack of knowledge, employees and other important staff fall for it. Ransomware sends out a trojan disguised as a legitimate file tricking the user into downloading or opening it and this allows the attacker to gain the victims private data. The attacker asks for money in return to not publish the data online. An attack like that on a major infra structure company have several setbacks, for the company and the economy such as the cost of the breaches. The oil and gas industry are named as “one of the nation’s most technically advanced and economically important sectors” (Clayton, Segal 2013) and yet the industrial control systems installed within this infrastructure has extremely limited cybersecurity. Why is that? An attack to “obtain confidential data from five major western energy companies” (Clayton, Segal 2013) was successful by the China-based hackers which began in 2008 extending into early 2011. This shows the limited knowledge of such threats within this sector and poses a worrying problem for each nation. If one of the most important sectors are easily being hacked into, within it taking highly sensitive information, it can be used as leverage to blackmail a whole country which could be detrimental in the long term.

As one of the most valuable targets, there should be better cybersecurity. There is an “oil and natural gas subsector cybersecurity capability maturity model” (Kumar 2020) for companies to use as a guideline for better security measures. This specific model allows companies to evaluate their cybersecurity programs which are already in place and make improvements. It is a guideline to create better security for the industrial control system computers and a tool to inform the companies on how they can address their needs and invest in areas in cybersecurity specific to their company that needs improving. Furthermore, “originally, there was little need” (Mittal, Slaughter, Zonneveld 2017) for cyber security but like previously discussed, although the ICS designed within oil and gas sectors are “fail safe” (Mittal, Slaughter, Zonneveld 2017), they talk about the “Sophistication of cyber criminals” (Mittal, Slaughter, Zonneveld 2017) which increases the risk of dangerous incidents. Previously, I discussed the cost that it will cost however in this article, they talk about the “safety, reputation and commercial or financial losses” (Mittal, Slaughter, Zonneveld 2017). This provides a different perspective as not only will it cost the company financial loss, but the country will also not trust it with sensitive information in the near future after the attacks.

A different idea for cybersecurity within this sector posed in the article "Are industrial control systems ready for the cloud? (Piggin 2014). Some of the main benefits of using cloud is it provides "increased flexibility, redundancy and availability" (Piggin 2014). Furthermore, it provides the opportunity to "reduce costs in infrastructure" and "is likely to be assured to particular security levels by third party" (Piggin 2014). I believe this could provide a big step towards a more secure ICS in this industry. Additionally, businesses will be attracted to it more due to the low cost and its ability to be accessed from "any internet location" (Piggin 2014). On the other hand, this could create "a large attack surface" as the number of clients using the cloud services could make it a "high value target" (Piggin 2014). I believe although using cloud has its disadvantages, it is an option that provides better cybersecurity than the ones in place currently.

Industrial Control Systems are implemented in major infrastructures in large scales across the world. The architectures such as SCADA that are mainly used provide little cybersecurity against attacks. As the attackers get more sophisticated, the more vulnerable the systems become. It is often the lack of security such as encryption that may enable a man in the middle to read data, modify or redirect traffic which causes detrimental effects not just on the company, but the country's economy itself. Things such as encryption and cloud should be implemented promptly. I believe just firewall in the IT systems within the ICS is not sufficient. There should be more cybersecurity and the technology that was first put in place should be updated frequently to prevent sophisticated hackers from attacking.

REFERENCES

Watts D 2003, *Security and Vulnerability in Electric Power Systems* 35th North American Power Symposium, University of Missouri-Rolla in Rolla, Missouri viewed January 6th 2021 from <http://cip.management.dal.ca/publications/Security%20and%20Vulnerability%20in%20Electric%20Power%20Systems.pdf>

Farrell A.E., Zerriffi H, Dowlatabadi H 2004 *Energy Infrastructure and Security* Energy and Resources Group, University of California, Berkeley, California 94720-3050. 2Department of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213-3890. 3Sustainable Development Research Initiative, University of British Columbia, Vancouver, BC Canada V6T 1Z2 viewed 6th January 2021 from <https://www.annualreviews.org/doi/full/10.1146/annurev.energy.29.062403.102238#_i24>

Pollert, Jaroslav, **Dedus**, Bozidar 2006 *Security of Water Supply Systems: from Source to Tap* Institute for Sanitary Engineering and Water Pollution Control, BOKU – University of Natural Resources and Applied Life Sciences, Vienna, Muthgasse 18, A-1190 Vienna, Austria viewed 7th January 2021 from < https://www.springer.com/gp/book/9781402045622>

Clayton B, Segal A 2013 *Addressing Cyber Threats to Oil and Gas Suppliers* Alfred P. Sloan Foundation viewed on the 7th January 2021 from <https://www.jstor.org/stable/pdf/resrep00313.pdf?acceptTC=true&coverpage=false&addFooter=false >

Piggin R, 2014 *Are industrial control systems ready for the cloud?* Atkins, Woodcote Grove, Ashley Road, Epsom, Surrey, KT18 5BW, United Kingdom viewed on the 7th January 2021 from < https://www.researchgate.net/profile/Richard_Piggin/publication/269820923_Are_industrial_control_systems_ready_for_the_cloud/links/5df11a06299bf10bc3544599/Are-industrial-control-systems-ready-for-the-cloud.pdf >

Mittal A, Slaughter A, Zonneveld P, 2017 *Protecting the barrels* Deloitte Center for Energy Solutions viewed on the 7th January 2021 from < https://www2.deloitte.com/us/en/insights/industry/oil-and-gas/cybersecurity-in-oil-and-gas-upstream-sector.html>

Mittal A, Slaughter A, Zonneveld P, 2017 *An integrated approach to combat cyber risk* Deloitte Center for Energy Solutions viewed on the 7th January 2021 from < https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/integrated-approach-combat-cyber-risk-energy.html>

Lawkay 2018 Electrical Control Systems (The sauce of Electrical Engineering) Steemstem viewed 6th January 2021 from <https://steemit.com/steemstem/@lawkay/electrical-control-systems-the-sauce-of-electrical-engineering>

Aboelnga H, 2018 *Beyond urban water security: the vulnerability of intermittent water supplies* Insight Cologne University Germany viewed 7th January 2021 from < https://www.thesourcemagazine.org/beyond-urban-water-security-the-vulnerability-of-intermittent-water-supplies/ >

Adepu S, Palleti V R, Mishra G, Mathur A 2019 *Investigation of Cyber Attacks on a Water Distribution System* iTrust Center for Research in Cyber Security, Singapore University of Technology and Design viewed on the 7th January 2021 from < https://arxiv.org/pdf/1906.02279.pdf>

Kumar A, 2020 *Defending the Oil and Gas Industry Against Cyber Threats* Security Intelligence viewed on the 7th January 2021 from < https://securityintelligence.com/posts/oil-gas-security/ >

Bisson D, 2020 *Attacks Targeting ICS & OT Assets Grew 2000% Since 2018, Report Reveals* viewed on the 7th January 2021 from < https://www.tripwire.com/state-of-security/security-data-protection/attacks-targeting-assets-grew-report-reveals/ >

Software functional Requirements

Software functional requirements in general define the functions a software must produce. This is important as it will give clarity to the users as to what is required of each function in the system. In my project, there can be several users that input data into the system however only two outputs are obtained. I will identify each requirement in this document and provide insight in ways the user can input data and what type of output may be given.

System overview

The basis of this system is to allow a user to input their userID and their password which is then sent to a server linked to a database which checks to see if the person is who they say they are otherwise authenticating the userID and password. On the userend, the userID and password will be encrypted by one key which is sent to the server that uses the same key to decrypt the message and checks with the database. This allows for a secure connection with the user and the server and furthermore allows authentication which is the target of this project.

Functional requirements of the system

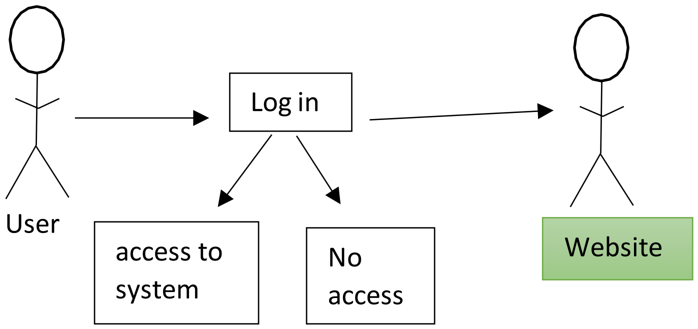
The function requirement of the system involves the application to be able to correctly encrypt and decrypt the userID and password and authenticate it. The following is a list of these functional requirements.

Functional requirements:

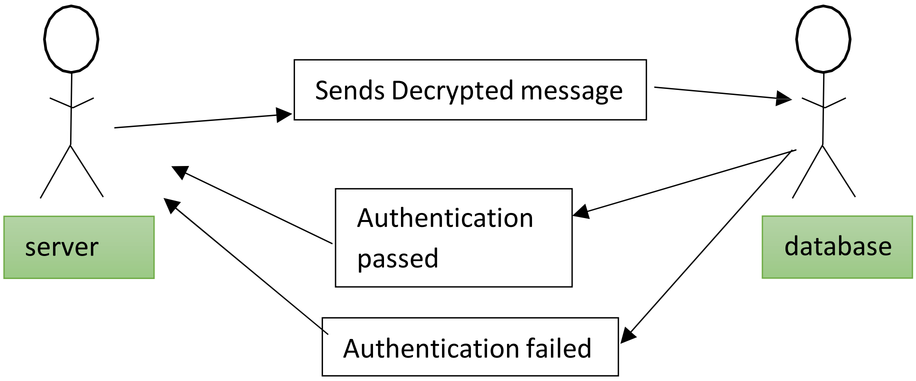
- The system will allow a user to enter their details
- The system will encrypt the user’s details
- The system will securely send the details to the server
- The system will allow the server to decrypt the details sent
- The system will allow the server to send the decrypted details to the database over a secure connection
- The system will allow the database to search for the userID and password
- The database will include list of employees who work within that company that implement ICS
- The system will allow the database to search through the list and determine whether the userID and password are correct and belong to the person entering the details
- The database will then send out a yes or no response to the server
- The server will encrypt the message with the same key
- The server will send out the message to the user
- The user will decrypt the message
- If the message says yes, the user is allowed to enter the system and is given specific permission to read, write, modify and delete
- If the message says no, the user is blocked from entering further

Software Use cases

The aim of the software use cases is to cover all aspects that are functional in the software being developed. It is essentially a list of actions that define the interactions between a role and a system to achieve a goal. In my project, the interaction between the user entering their userID and password and the server achieves the goal of authenticating the user trying to gain access to the system.



Use case diagram 2 shows relationship between the server and the user



Use case diagram 2 shows relationship between server and database

Methodology of Testing

The purpose of testing is to ensure that the proper functionality of system is carried throughout. It allows for defects to be discovered and thereby corrected. A series of tests will be conducted to ensure that my system meets the expectation required through its functions. In this document, I will provide different testing strategies with indicative test cases to illustrate how each scenario will be organised and measured.

Objectives

In the testing objective, the system will be tested to validate the system's requirement to correctly authenticate the user, the system will be tested on its reliability, performance, how quickly it can authenticate, how secure the connection is. It will be tested to see if it may be able to prevent a harmful cyber attacker to eavesdrop the channel and falsely gain access to the system without authentication. For testing, unit tests and black box tests will be carried out. This is to ensure the stability of the system and that each website works well without any bugs.

Strategy

I have chosen to adopt the agile testing approach as opposed to iteration or waterfall. In the agile methodology, the system is developed in incremental cycles. It involves the customer regularly and focuses on responding to change as opposed to long planning. In the iteration model, the whole system is tested all together however this could increase the time it takes to develop the complete system as if there are many fails, each different area will have to be looked again. In the agile methodology, it is possible to make changes any time within the project and the incremental testing minimises the risks.

Incremental testing is how my system will be tested throughout. This allows for the system to be working quickly and it allows more flexibility. It also allows the risks to be managed more easily as they are identified and handled during its iteration. This strategy also allows for test cases to be executed simultaneously to the configuration of the system. This means that any bugs or failures to the system can be dealt with as soon as possible and allows for the system to be executed quicker. If the requirements change, they can also be dealt with at each iteration.

Purpose of black box testing

Black box testing is often used to test the functionality of a system based on the requirement specification, so it does not focus on the code of the application. This ensures accuracy as it is measured from statistical basis.

Black Box testing cases

Case	Description	Process	Expected results	Actual Results	Passed?
1	The user is redirected correctly to a server by the website after submitting their userID and password.	The user is redirected to the authorisation server in which they are asked to allow access to or not.	The user is redirected to the server by the client website.	The user is redirected the server by the client website.	Yes
2	The user is able to allow access to authorise	The authorisation server confirms the connection has been made.	The user is able to allow access to authorise in the server.	The user is able to allow access to authorise in the server	Yes
3	The server sends encrypted message code to client.	The authorisation code is exchanged against an access random string generated by the	The server upon client's request sends an encryption code to client.	The server upon client's request sends an encryption code to client.	Yes

		authorisation server between client and authorisation server.			
4	The website informs the user that they have been authenticated and authorised to access their data.	The client uses the random generated string to query server and retrieve the user's data.	The user is able to see their data on their screen.	The user is able to see their data on their screen.	
5	The website informs the user they are not authorised to access any data.	The server sends call back response to client and blocks user from accessing any data.	The user is unable to access any data.	The user is unable to access any data.	

Unit case Testing

Unit case testing if often known as white box testing which is used to examine the program's structure and the allows validation of the code and program of the application. It identifies accuracy within the systems functionality.

Unit case Testing

Case	Description Summary	Process	Expected Results	Actual Results	Passed?
1	If the loading page allows input from user	Type into the userId box	Text is inputted	User is able to input text into the correct box	
2	The user gets redirected to different website (server).	The user after inputting the data will see a different screen in which they will be asked to authorise the server to send their information	User is able to see they have been redirected to a different screen.	User is able to see they have been redirected to a different screen.	

		out for authentication.			
3	The user can see the on the website they have been redirected and that they have two options to click yes or no to allow server permission to send their data for authorisation.	The user is able to click yes or no to allow authorisation of their data to be sent across from the server.	The user is able to click both yes or no buttons on the redirected website.	The user is able to click both yes or no buttons on the redirected website.	
4	Upon clicking yes, the user is redirected to the log in website	The user clicks on yes and the server sends out data to database to check for authentication	The user can see they have been redirected to the log in page.	The user can see they have been redirected to the log in page.	
5	User is given an output message on website to say whether authentication is passed or failed.	The database is generated, and it checks its list to see whether the specific userID is in there and if so, sends message to server who informs the client.	The user can see on the screen a message determining whether they have passed or failed authentication.	The user can see on the screen a message determining whether they have passed or failed authentication.	
6	Determine whether website presents user's data after authentication passed.	The server would allow access to the website to present data if authentication passed.	The user will be able to see their data on the screen.	The user will be able to see their data on the screen.	
7	Determine whether website blocks any further action from the user is	The server would not allow access to the website to present data if authentication failed.	The user will not be able to see theirdata on the screen and blocked from taking	The user will not be able to see theirdata on the screen and blocked from taking	

	authentication failed.		any further actions.	any further actions.	

System Design overview

The system design overview outlines the requirements, the system architecture, the format of the input, the user interface design. This information is necessary in the development and implementation of the system. I will highlight assumptions and constraints of the system design and the objectives of it. The target audience of this document is the developer and project manager.

System design

Within this project, it allows the user to enter their login details and they are redirected to another page in which their details are securely authenticated. The purpose of this is to allow a more cybersecure way of accessing the different areas within a major infra structure that implements the use of industrial control systems.

Design objectives

- User input details
- User redirected to server
- Details encrypted
- Details sent to database
- Database validates the details
- Database sends back confirmation of authentication
- User presented a message of confirmation
- User redirected back to login page
- User able to access their data

Design assumptions

The system will allow for a far more cyber secure log in prompt than ever before and allow for it to be implemented across the world in different infra structures that use industrial control systems. It will cause the attacks to lessen. Within the development of the system, I assume the development and the testing will be done simultaneously throughout. The system development will follow to the agile methodology and the system will be tested in iterations. The users of the system will be the employees of a major infra structural company that uses industrial control system. They will require an internet connection and be expected to only log in during working hours.

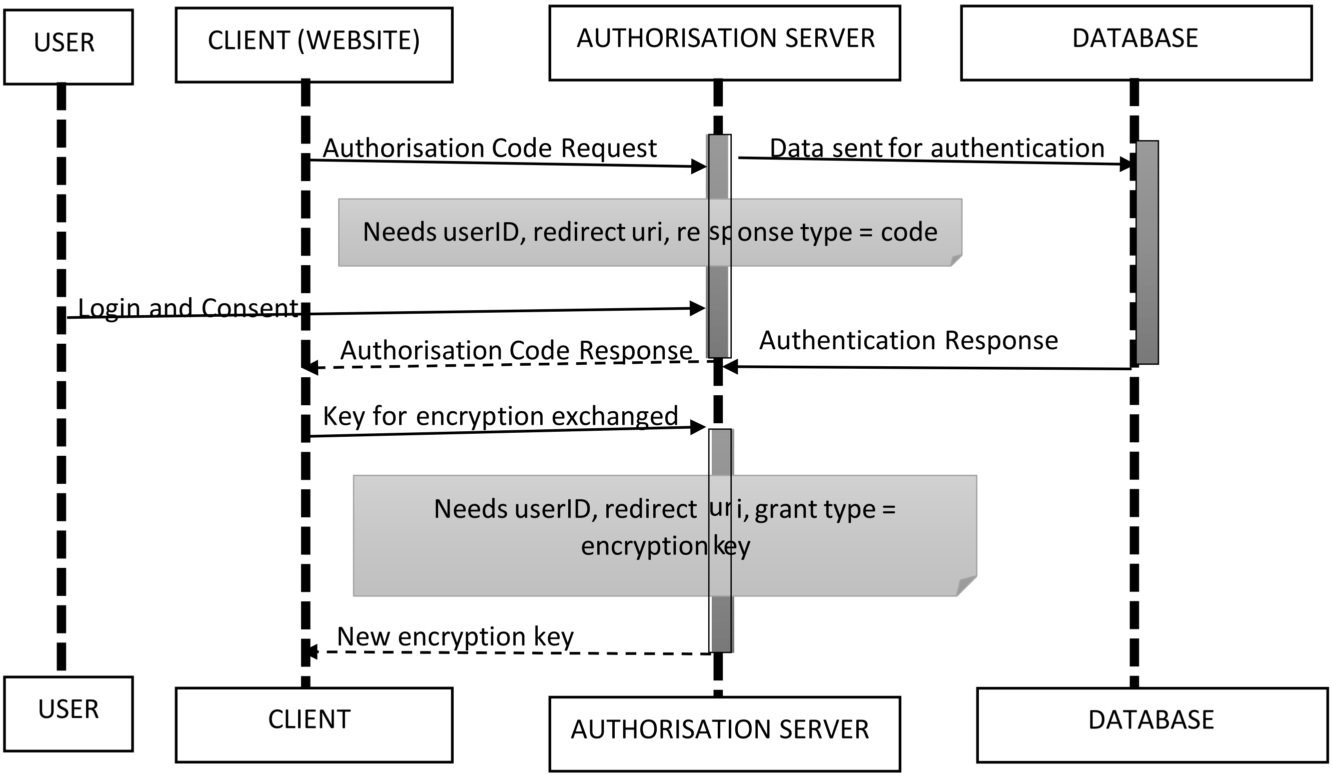
Design constraints

The focus of the system will on the security and the correct authentication of the employee therefore there will be less consideration on how aesthetically pleasing the website will be and furthermore the performance might be slow if there is a large traffic of users trying to log in simultaneously. This might freeze the website or crash it and if this happens, the system will undergo performance analysis to develop it further for better quality and to prevent it from crashing.

Architecture

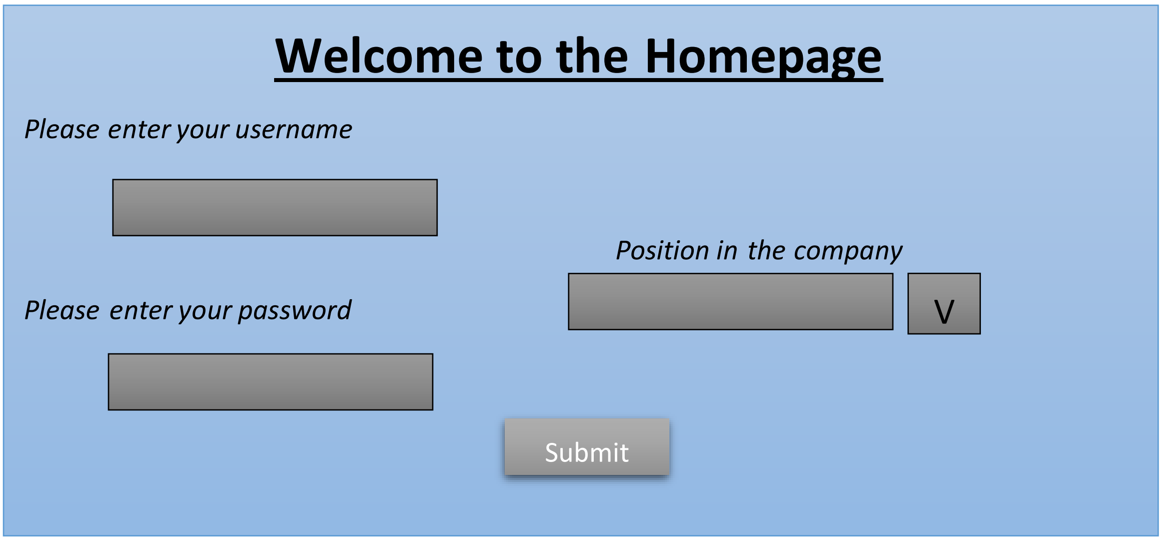
For the architecture, I have decided to utilise PHP coding approach for the use of tackling different areas of the system and MySQL for the database that will connect with the PHP. Php data objects (PDO) is an extension which allows for the database abstraction layer. It is an interface for the backend that allows an interaction with the database without making any changes to the PHP code. Each PHP file will be used to separate and get together different aspects and behaviours of the functions and data. The aim to use different files and directories within PHP is to allow the system to be structurally sound and avoid unnecessary collisions. I will be using MySQL server to store a list of userIDs that will correspond to each employee that tries to log into the website which will be created in visual studio in php. With another directory dedicated to the database, a file will be created with code to establish a connection to the database. A localhost database connection will be implemented.

To demonstrate the proposed system architecture, I have created a Unified Model Language diagram to present a structural system design. This diagram will aim acknowledge the relationship between the client, the authorisation server, and the user. The diagram is a preliminary system design and thereby subject to change in the future.


USER
CLIENT (WEBSITE)
AUTHORISATION SERVER
DATABASE
Authorisation Code Request
Data sent for authentication
Needs userID, redirect uri, response type = code
Login and Consent
Authorisation Code Response
Authentication Response
Key for encryption exchanged
Needs userID, redirect uri, grant type = encryption key
New encryption key
USER
CLIENT
AUTHORISATION SERVER
DATABASE

User Interface

User Interface design should have elements that are easy to access and understand and use. It is used to focus on anticipating what users might need to do and therefore must bring together all the concepts from visual design and information architecture. The user interface will be available to use from 8am until 8pm as I believe those could be the working hours of an employee and therefore anyone who tries to access the system out of those hours will automatically be denied entry. During the working hours, the user interface may experience a high volume of users trying to access their data especially in the early hours when they are expected to start their working day. The user interface will consist of two separate input buttons in which the employee will be able to input their unique userID and their password. In addition, there will be a drop-down box in which they can select their position within the company as the higher up you are in the company, the more permissions will be available to that user such as an executive or company owner may be able to override the system and log into the system out of working hours. When logging into the account, the user is redirected to another page in which they are asked if they may grant the website to send data for authentication. This step is crucial within the system as it allows the system to become more cybersecure. The user is then presented with a message indicating whether their authentication has passed or failed which consequently either allows them to access their data or blocks them.



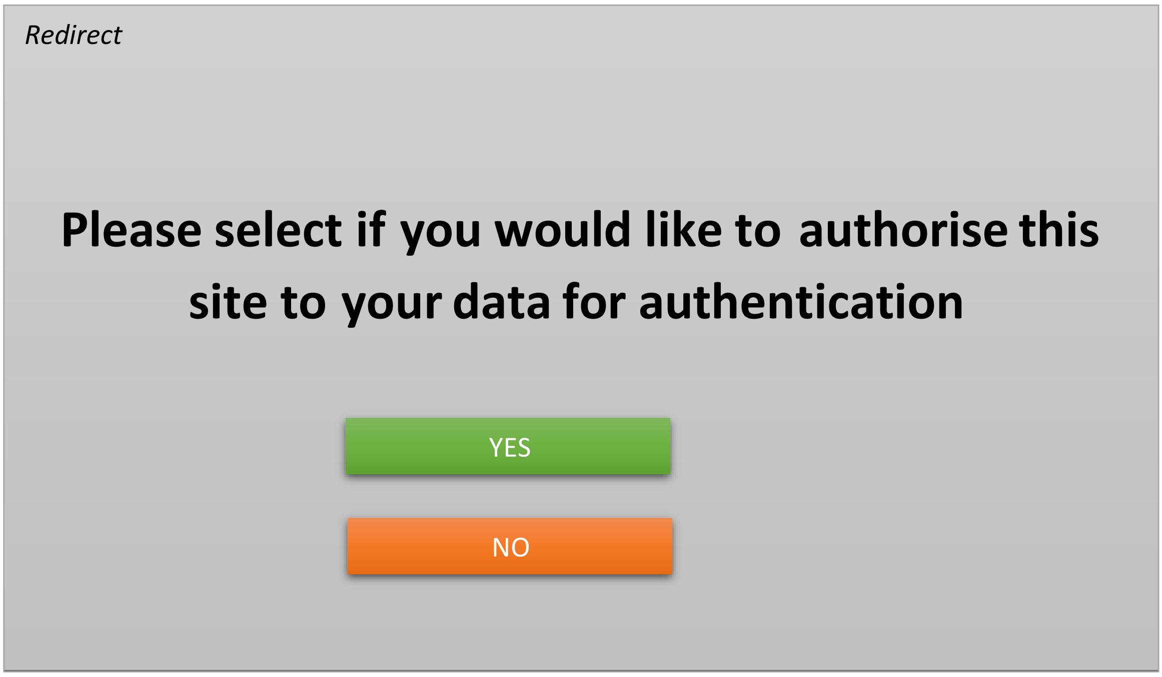
Welcome to the Homepage

Please enter your username

Position in the company

Please enter your password

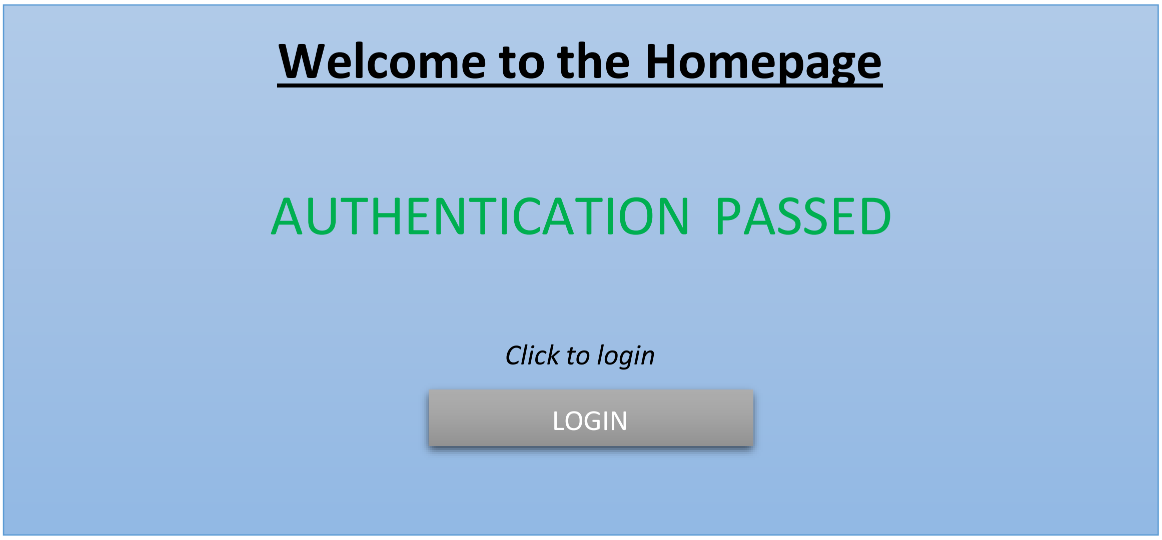
This is the front login page for the user to input their details.



Redirect

Please select if you would like to authorise this site to your data for authentication

This is the page the user gets redirected to, to allow access for server to send data to database for authentication.

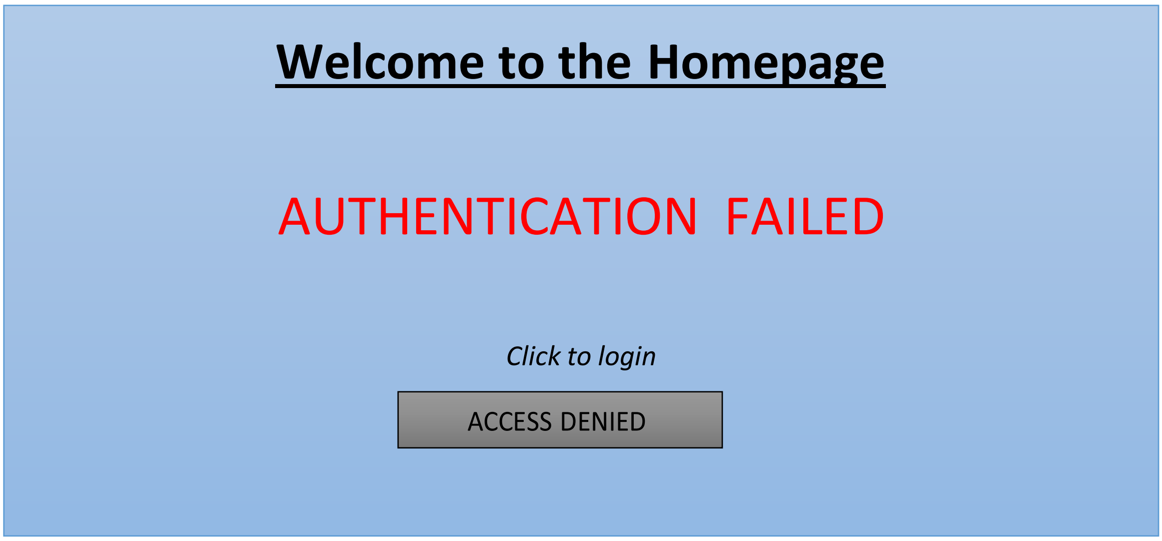


Welcome to the Homepage

AUTHENTICATION PASSED

Click to login

This is the homepage the user gets redirected to if the authentication has passed.



Welcome to the Homepage

AUTHENTICATION FAILED

Click to login

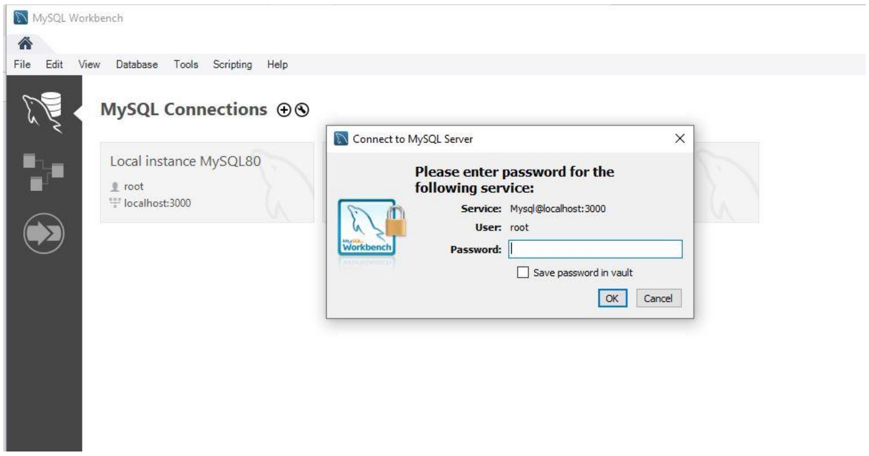
This is the homepage the user gets redirected to if the authentication has failed.

System Implementation

System development

Database Created

For the initial development process of the login system, a backend server was created. This was the first step in creating the login system as without it, the system would not work. The root of the project is dependent on the database that is used in the backend. A root server was created in MySQL workbench in which the port was changed from 3306 to 3000. This was done because there were other projects running on port 3306 that could later interfere with my login project.



Local instance MySQL80
root
localhost:3000

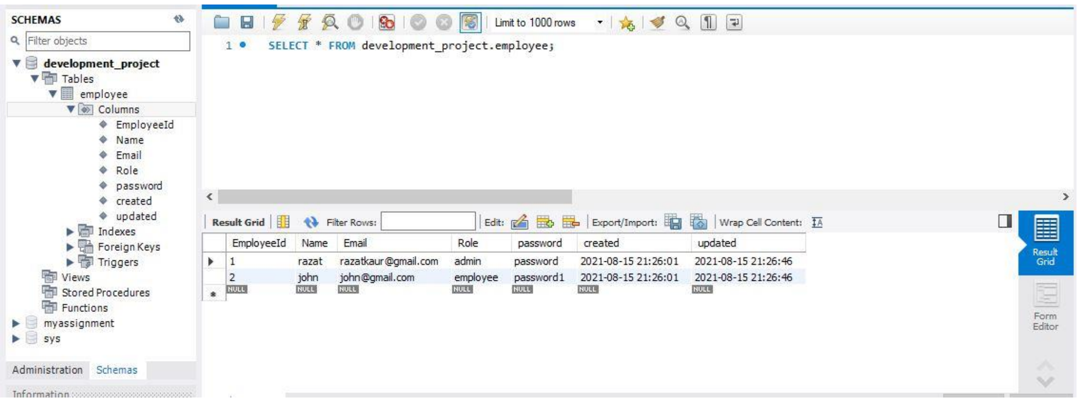
Connect to MySQL Server

Please enter password for the following service:

Service: Mysql@localhost:3000
User: root
Password:

□ Save password in vault

Within this server, a database was created which was named as "development_project" to differentiate from other databases on the server. As this is the default root server, more than one project will be saved here so naming it "development_project" allows for easier access to the database when using it for connections. Included within this database are tables that will showcase login credentials of a user within a company. The tables included were: EmployeeId, Name, Email, Role, password, created and updated. This will help determine how much information can be available to different employees depending on their role within the company. These tables were pre filled with dummy data to be able to use it in a demonstration in the login system. Two inputs were included that show two different types of users in the company: Employee or Admin. Naturally, the admin of the company will have more privileges than an employee.

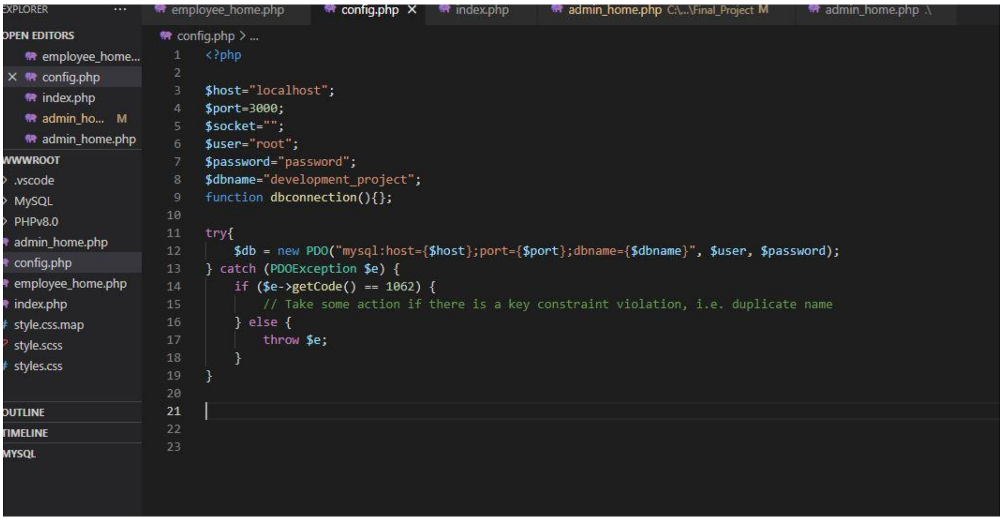


```
1 ●    SELECT * FROM development_project.employee;
```

EmployeeId	Name	Email	Role	password	created	updated
1	razat	razatkaur@gmail.com	admin	password	2021-08-15 21:26:01	2021-08-15 21:26:46
2	john	john@gmail.com	employee	password1	2021-08-15 21:26:01	2021-08-15 21:26:46
NULL	NULL	NULL	NULL	NULL	NULL	NULL

Config.php

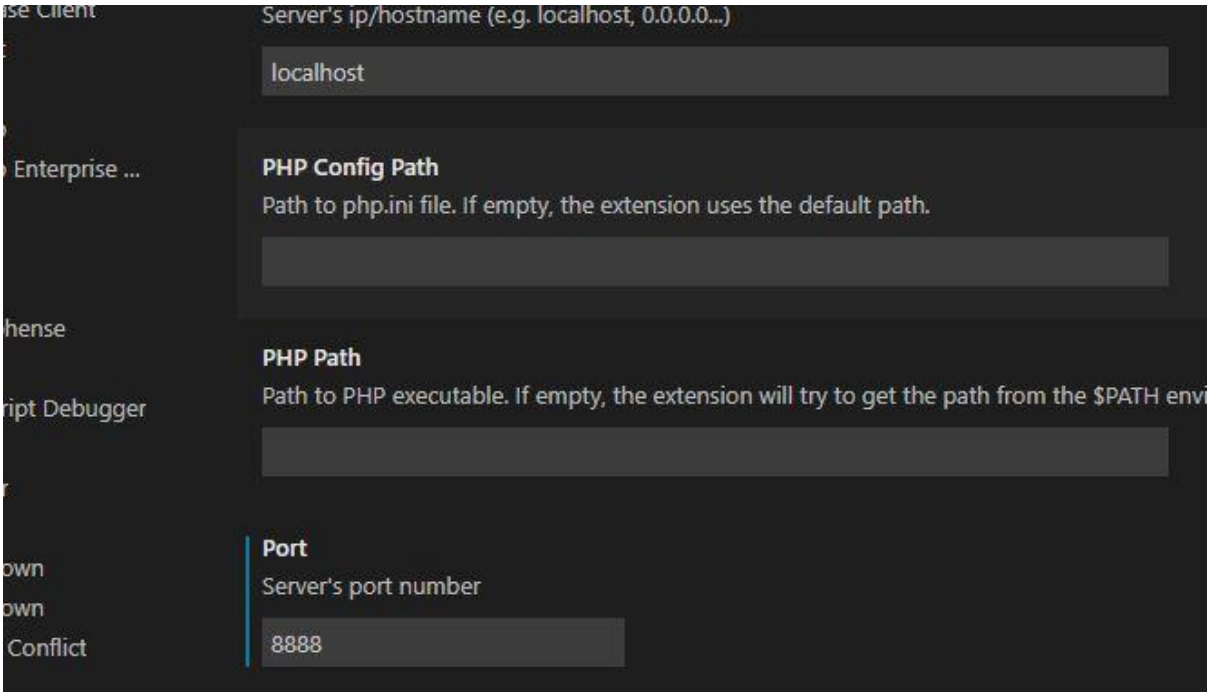
The second phase of development of the project included creating a secure connection to the database using PHP language. This was done in visual studio code. To create a secure connection, PHP Data Objects library was used to prevent attacks such as SQL injection. The connection was made using the host, name, port, user and password of the database that is being used. This is done so that there is a quick and secure connection to the database. There are various functions within PDO library that allows errors to be raised. The function "PDOException" was used here which gets thrown anytime something goes wrong while PDO is being used. This file is crucial as it will be used in the main file to validate and authenticate users logging into the system.



```php
<?php

$host="localhost";
$port=3000;
$socket="";
$user="root";
$password="password";
$dbname="development_project";
function dbconnection(){};

try{
    $db = new PDO("mysql:host={$host};port={$port};dbname={$dbname}", $user, $password);
} catch (PDOException $e) {
    if ($e->getCode() == 1062) {
        // Take some action if there is a key constraint violation, i.e. duplicate name
    } else {
        throw $e;
    }
}

```

Creating the servers

After the configuration file has been created, the next important step was to create a PHP server that will run on localhost that will allow for the project to run and be visible in the front-end. In order to do this, the IIS manager and the web platform installer was downloaded. Within this, PHP application was downloaded and using the IIS manager, PHP could be configured to allow the appropriate extensions that allowed for the PDO library to be run. The PATH that was created in the IIS manager was directed to the "wwwroot" directory in the "inetpub" folder on the C drive. This is the folder that was used to store all my php files as this is where localhost will look for files to be displayed on the front-end of the system on web browser. The PHP folder in the program files was moved to the "wwwroot" file and within visual studio code, the extension of PHP was configured to use the PHP folder in the "wwwroot" file instead of the programs file. This allowed for less confusion about where the extensions folder was located. Next, in the visual studio code extension for PHP, the port used to serve the project was changed to "8888" which will run on localhost. To ensure the visual studio code was using the PHP folder in the "wwwroot" file, I added a PATH to the environmental variables in the system advanced settings to allow for a direct root to the specified folder. In order to test this, in the "config.php" file, at the end of the code, an “echo” statement was added and the server was ran. The webpage automatically opened and displayed a “success” message. This showed that the server was ready to be used for other files and the creation of the login system.



Server's ip/hostname (e.g. localhost, 0.0.0.0...)

localhost

PHP Config Path

Path to php.ini file. If empty, the extension uses the default path.

PHP Path

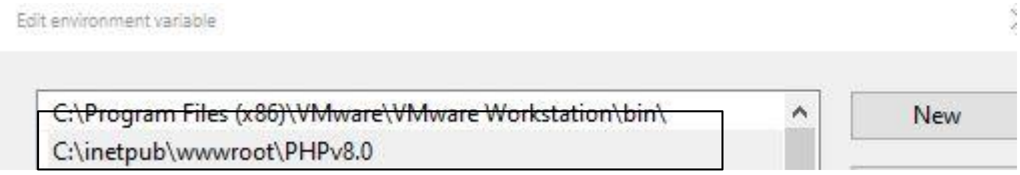
Path to PHP executable. If empty, the extension will try to get the path from the $PATH envi

Port

Server's port number

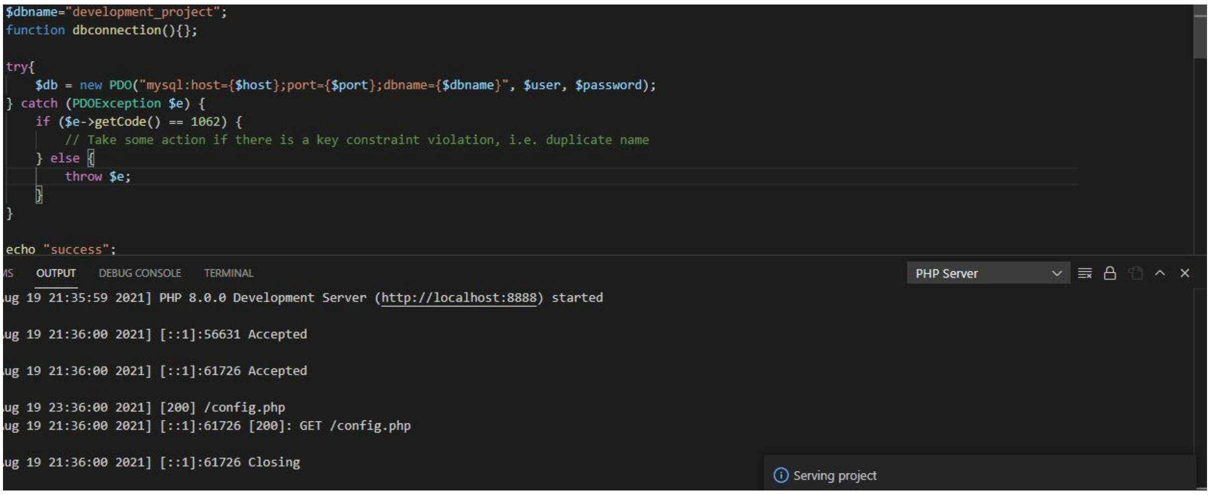
8888

The port changed to 8888 in settings file of php server



C:\Program Files (x86)\VMware\VMware Workstation\bin\
C:\inetpub\wwwroot\PHPv8.0

The path to “wwwroot” file added to the environmental variable for the PHP.

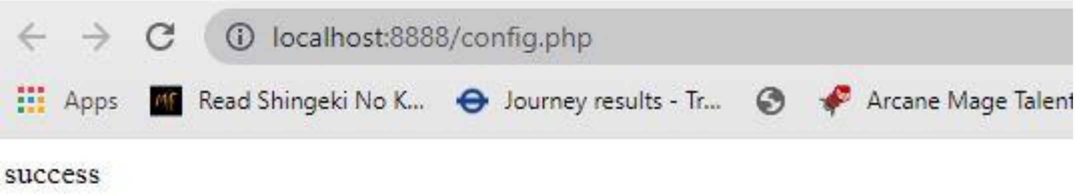


```
$dbname="development_project";
function dbconnection(){};

try{
    $db = new PDO("mysql:host={$host};port={$port};dbname={$dbname}", $user, $password);
} catch (PDOException $e) {
    if ($e->getCode() == 1062) {
        // Take some action if there is a key constraint violation, i.e. duplicate name
    } else {
        throw $e;
    }
}

echo "success";
```

```
ug 19 21:35:59 2021] PHP 8.0.0 Development Server (http://localhost:8888) started

ug 19 21:36:00 2021] [::1]:56631 Accepted

ug 19 21:36:00 2021] [::1]:61726 Accepted

ug 19 23:36:00 2021] [200] /config.php
ug 19 21:36:00 2021] [::1]:61726 [200]: GET /config.php

ug 19 21:36:00 2021] [::1]:61726 Closing
```

Serving project

Success message added and PHP server started

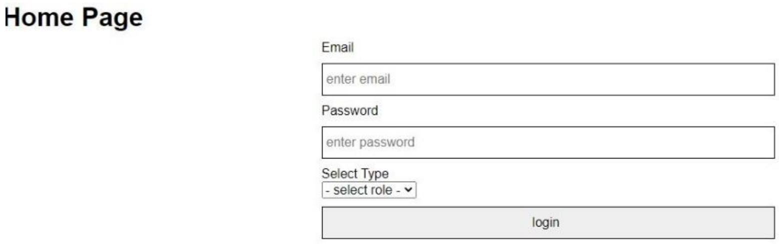


```
success
```

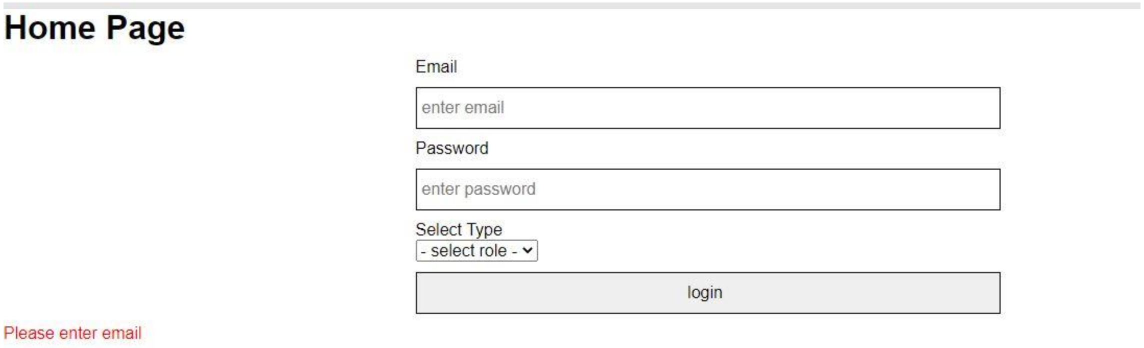
Success message displayed in browser of localhost running on port 8888

Login Page

The next phase is the creation of the login page that the user will see in the front-end. Once all the back-end database files have been created, they can now be utilised. The HTML aspect was coded first to ensure all the parameters of each button was used appropriately, ensuring no errors can rise later. The password field type was used as "password" so that when the user is logging into the system, the password isn't shown as plain text. This is a small security measure in place to ensure an unauthorised person does not see the password that is being entered by the user when logging in. Within this page, there are other security measures in place for example the error messages that are received by the user if the user enters the wrong email or password. The user will always receive the same error message whether the email is typed wrong, or password is typed wrong, or the role selected is wrong. This is to ensure safety of the user's information as if an attacker tries to brute force their way into the system, they will not know which information they are typing in is correct and which is not. Using the "PDO: : FETCH_ASSOC" which is a feature of the PHP Data Objects library, the table in which the email and password are stored is retrieved. A prepared statement is used to sanitise and embed external data into a SQL query in a safe way. Furthermore, the email that is entered into the system is filtered and sanitised before the user that is attempting to log in can be authenticated into the system. Validating data that is entered into the system determined whether it is in proper form and sanitising the data will remove any illegal character. Validation is crucial within a login system as it provided for an outer defence perimeter. Additionally, there are other errors that will be outputted onto the screen if the any of the fields entered by the user remains empty. The user will be prompted to enter each field that is left blank. If, however, all the fields are entered with correct information then the user will be displayed a success message on the screen and redirected to the appropriate home page for the user depending on their role.



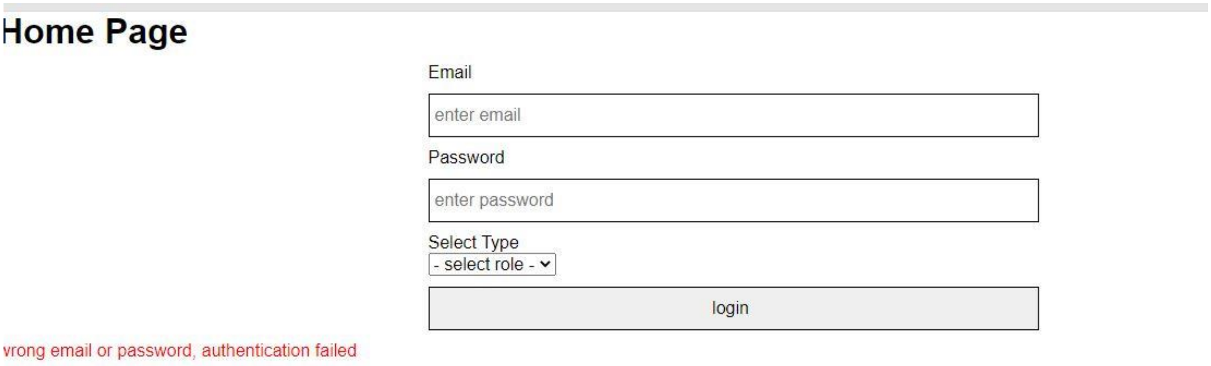
HTML output of login page



Home Page

Please enter email

Example of first error if fields are left blank



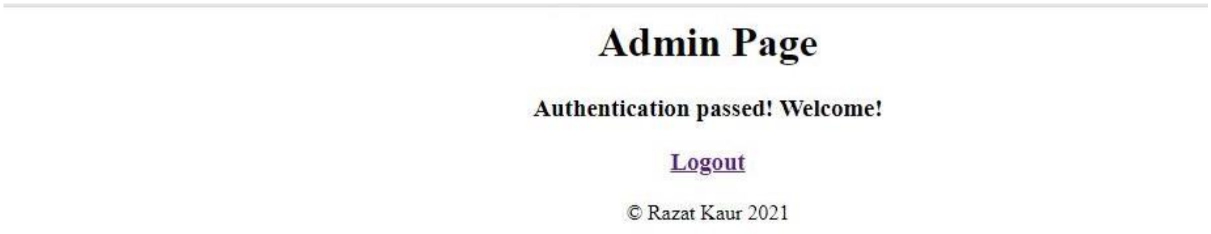
Home Page

vrong email or password, authentication failed

Example of error if information typed into the system is wrong

Admin/Employee Login

The final steps were to create the home pages were for the admin and the employee. These were redirected to when the user successfully logs into the system with the correct credentials that match the ones in the database. The home pages for both logins are similar in terms of coding it with a log out page and a heading that states which page it is welcoming the user. The reason there are no other details besides this is because it is out of scope of this project. These pages depend on the company it is being served for. The admin will have more privileges than employee, perhaps access to the database to input new employee details into the system as opposed to employees that could have access to their own details and position in the company and their tasks to be completed within that week.

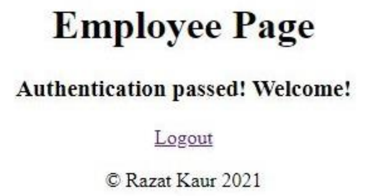


Admin Page

Authentication passed! Welcome!

© Razat Kaur 2021

Admin Home Page



Employee Page

Authentication passed! Welcome!

Logout

© Razat Kaur 2021

Employee Home page

Development Adherence

During the development and implementation of this project and the supporting documents, the agile framework, SCRUM implemented as the development scheme. This framework was chosen for its highly iterative process for application development. This has various development cycles, otherwise known as, 'sprints'. These are designed for uplifting the productivity of the development of the project and the delivered quality.

The incremental development focus of agile allows for all parties to provide feedback as the application is being developed in an efficient and effective manner and allows for the functionality of the application to be refactored quickly without causing other parts of the program to break. Although a Gannt chart was recommended, it was not used in the process of developing this application however in written hard copy, similarly to a gannt chart, various time frames were recorded to illustrate and dictate when each element of the project should be delivered by.

Problem Resolution

Throughout the development of the project, various number of defects within the login system were encountered, during testing and build procedures. As proposed in the indicative test plan and ethical review documents, improper functionality of the system will be looked over and upon discovery, an attempt would be made to dissolve the issue for a more efficient login system a company may implement.

Discovered within the login page, the errors that display whether the user has incorrect login credentials or whether the user has not entered anything into the fields were not showing. The code that was used to create this scenario was reviewed however there were no bugs that were visible. Step by step, under each line, an "echo" statement was published to see whether this will show up on the screen and if it does not then the problem will be in the code above the statement. However this was long and time consuming so upon research, a code was found that shows all the important information in the header of the web page. This information printed the values of the field of the email and password. This was useful in detecting where the fault was which showed that the name of the field in which the email was being inserted was wrong and hence when the email was being typed, nothing was showing up as the name of the button at the beginning that was bound to the email that the user typed was wrong. This was easily corrected. Next, after each little bit of code, it was ran to see if it worked to prevent any future errors.

Testing Regime

Overview

The application was intended to be tested upon completion of its code base. As agile's testing methodology was adapted, testing has enabled the application to showcase expected behaviours and over the course of developing this project, this has been achieved by refactoring the code base which have been responsive to the findings of the test cases.

The categories that have been tested include black box testing and unit testing for the front-end and backend implementations of the login system's design. This is used to advance the robustness, reliability, and the usability of the system.

Unit Testing

Unit testing was used to ensure that all the code meets the quality standards before it is deployed and used by various end-users. It is used to examine the system's structure and allows validation of the code. The system was categorically tested as although the pages are connected to one another, the features within each page are independent.

Black-box testing

Black box testing allows to find the gaps in functionality of the system and identifying the usability and correctness of the system from a front-end visual standpoint. This allows for each test case to be conducted quickly and reduces the complexity as opposed to unit testing.

For supporting documentation of unit testing, see appendix B
For supporting documentation of black box testing, see appendix A

Project Maintenance

Throughout the development of the project, the code that was implemented was categorically tasked and organised. This was done to maintain the project's rate of progress. The code is accompanied by docblocks to show what each piece of code is intending to do. In addition to a preliminary Unified Modelling Language (UML) diagram, a flow chart was implemented and referred to throughout the setup process of the login system's cycle. This allowed for an initial structured project which is crucial for code-based projects to allow the project to run smoothly. Alterations were made to the original design of the project to cater for unforeseen functional requirements of the application.

The testing documentation of the project was done simultaneously to the test cases being conducted.

Critical Evaluation

Project Evaluation

System Features

Relating to the criteria set within the project contract, the ethical review and the global checklist and the functional requirements section, the login system created addresses all the mandatory behaviours through the front end and back end as well the aesthetic of it. From the architectural standpoint, the login system conforms to all the principles stated in the document.

Given more time was available for the systems development, a "forgot password" feature would have been added to allow the login system to further its capability by allowing users who have forgotten their password to be able to change it and this would update the database in the backend in the table where the employee's login credentials have been added. Furthermore, in more time, a feature that gives the user three login attempts would have been included. This forces the user to log into the system within the three attempts otherwise the user will be blocked and will have to contact "admin" to log into their system again. This a security feature which could enhance the functionality of the system. After each attempt, the user will be shown how many attempts they have left, and each attempt will get recorded in a table in the database back end.

With regards to the user interface in which the user will be presented with a page to allow for authentication, this additional page was insignificant and added a page to the login system unnecessarily. It's absence from the system has no impact on it and was not a constraint of time nor complexity.

Lastly, if given more time, the passwords that get stored into the database will be hashed and the function "password_verify" will be used to match the input from the user to the password stored in the database. This is a basic security feature that is missing from the current login page due to time restriction however with more time this feature can be implemented.

Development Evaluation

Development Approach

For preliminary construction of the project, a hand-written hard copy of when each feature of the system was to be delivered. This was used to indicate how much time is spent doing each section and allowed for better time keeping.

However, reflecting on the process of the development, the time and order of each section deferred greatly from what was originally calculated. This was majorly factored by the coding errors on the login page which subsequently put the entire project on hold as the main purpose was to log into the system. This was refactored to allow for logging in and showing errors when appropriate.

Furthermore, complementing the structural development of the system, a flow chart addressing the back end and front-end architecture was formulated. From the existence of the flow chart, the system's expectation and developments could be quickly acknowledged.

Academic Advancement

For the role requirements of the project undertaking, my understanding of the PHP language and PDO library with connecting server has been informed by the delivery nature of the system. The procedures required to execute and structure a plan and implementing it in the front and back end have also been informed by the delivery nature of the system.

Tool Evaluation

Development Support

For the entirety of the development project, the visual studio code editor was used. This is renowned for its lightning-fast source code editor and provides many features that allow coding within this editor easy and quick. Things such as box-selection or formatting document provides for a cleaner code that is easy to work with. Furthermore, the extension within this editor is phenomenal and it compliments writing in PHP language and using PHP server within the editor. PHP language was previously taught and was selected to write this project in due to its capability of being able to interact with many different databases including the one used in this project. This language has many resources online about it and is easy to implement. The library within it PDO is a perfect extension to utilise to create a more secure login system.

Acknowledgements

For all the staff stationed at De Montfort University, I would like to express my thanks for such a fantastic experience as an undergraduate student and for all the resources and facilities that were provided and furthermore acceptance onto the programme. I would like to express my thanks to Dr Mehmet Kiraz as my supervisor and senior lecturer at de Montfort university over the last three years.

To my family and friends who have supported me throughout this emotional rollercoaster, during monumental times, I would like to mention that your efforts are never overlooked. Thank you.

Appendix

Blackbox Testing Appendix A

Case	Description	Process	Expected results	Actual Results	Passed?
1	The user is correctly shown the login page prompting to input email password.	The user is taken to the home page of the login system in which they are presented with a form where they can input credentials.	The user can input details into the appropriate fields	The user can input details into the appropriate fields	Yes
2	The user is able to click login	The authorisation server confirms the connection has been made.	The user is able to click login	The user is able to click login	Yes
3	The user is presented with error message “authentication failed” when the credentials are inputted wrong.	The user attempts to log in with the wrong credentials and the server validates this information and sends back a message saying, “incorrect email or password, authentication failed”.	The user is presented with error message “authentication failed”	The user is presented with error message “authentication failed”	Yes
4	The user is presented with error message “enter email”	If the field for email is empty, the user is presented with an error message prompting them to “enter email”.	The user is presented with error message “enter email”	The user is presented with error message “enter email”	Yes

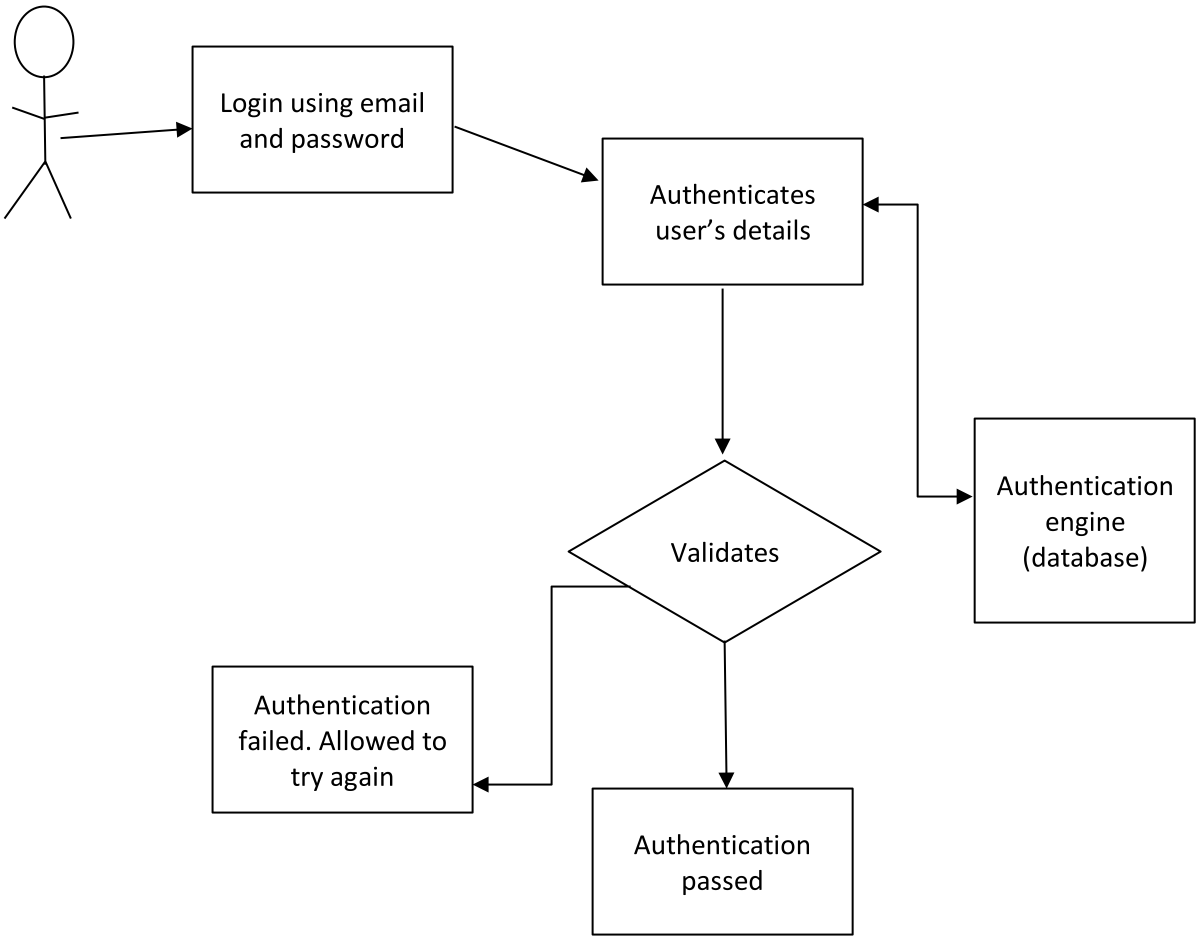
5	The user is presented with error message “enter password”	If the field for password is empty, the user is presented with an error message prompting them to “enter password”.	The user is presented with error message “enter password”.	The user is presented with error message “enter password”.	Yes
6	The user is presented with error message “select role”	If the drop down box for role is empty, the user is presented with an error message prompting them to “select role”.	The user is presented with error message “select role”	The user is presented with error message “select role”	Yes

Unit Testing Appendix B

Case	Description Summary	Process	Expected Results	Actual Results	Passed?
1	If the loading page allows input from user	Type into the email box	Text is inputted	User is able to input text into the correct box	Yes
2	The user can see they are on the log in page where they can click login	The user clicks on login and theserver sends out data to database to check for authentication	The user can see they are on the log in page.	The user can see they are on the log in page.	Yes
3	User is given an output message on website to say whether authentication failed.	The database is generated, and it checks its list to see whether the specific email is in there and if so, sends message to server who informs the client.	The user can see on the screen a message determining whether they failed authentication.	The user can see on the screen a message determining whether failed authentication.	Yes

4	User is given an output message on website to say whether authentication passed.	The database is generated, and it checks its list to see whether the specific email is in there and if so, sends message to server who informs the client.	User is given an output message on website to say whether authentication passed.	The user is redirected to a home page depending on their role in the company	Yes
5	Determine whether website presents user's data after authentication passed.	The server would allow access to the website to present data if authentication passed.	The user will be able to see their data on the screen.	The user will be able to see their data on the screen.	Yes
6	Determine whether website blocks any further action from the user if authentication failed.	The server would not allow access to the website to present data if authentication failed.	The user will not be able to see their data on the screen and allowed to try again to input correct credentials	The user will not be able to see their data on the screen and allowed to try again to input correct credentials	Yes

Appendix C


Login using email and password
Authenticates user's details
Validates
Authentication engine (database)
Authentication failed. Allowed to try again
Authentication passed