Faculty of Engineering, Environment and Computing

Design and Develop a Functional Secure System for ABC Air

AKM HASAN

Student ID – 9755484

hasana19@uni.coventry.ac.uk

MSc Cyber Security – Coventry University

7032CEM – Secure Design and Development

GitHub links for this module (CU GitHub repository):
https://github.coventry.ac.uk/hasana19/7032_CEM_AKM_HASAN_STUDENT_ID_9755484
Dr. Derrick Newton

Coursework Due Date: 03 Jan 22

Introduction:

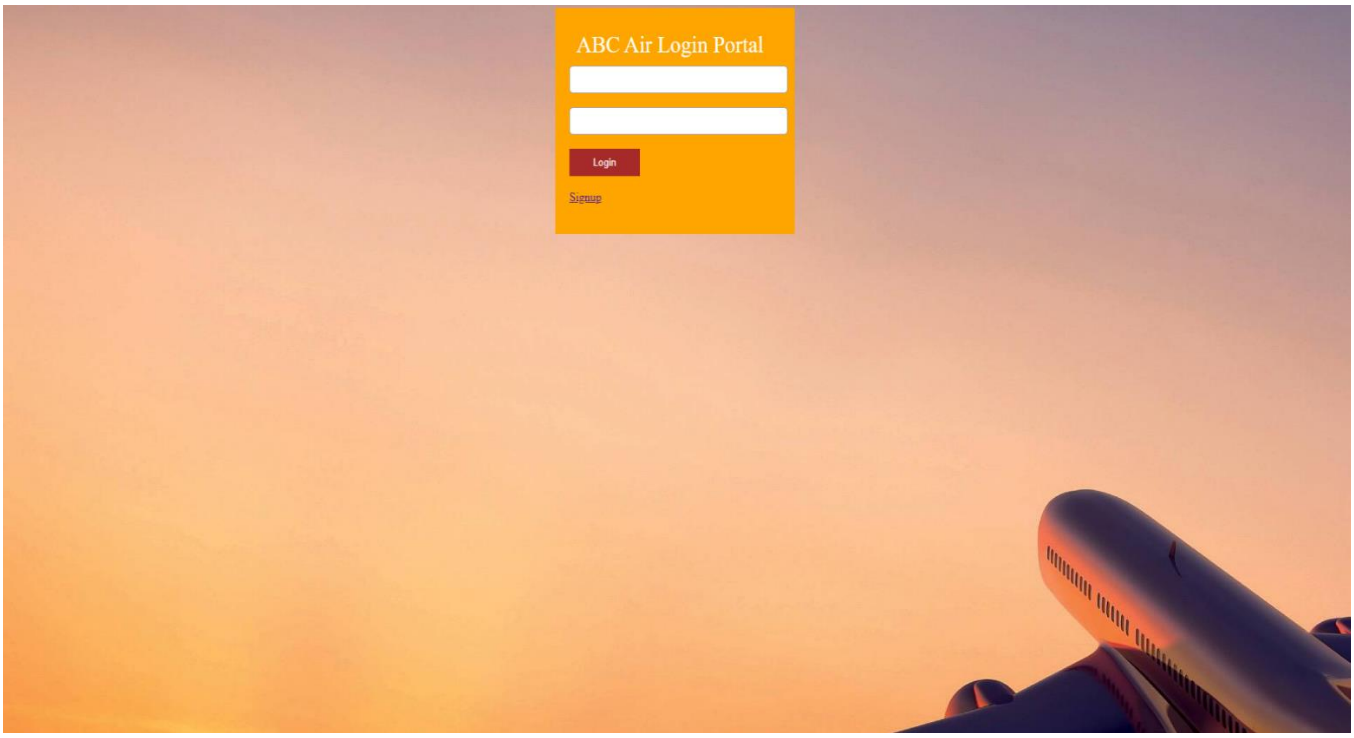
ABC Air is a small aircraft service company that carries out aircraft maintenance for civil operators, I have been contacted by them and they asked me to design and develop a functional security system for them and implement the secure online system.

ABC Air records the total number of flying hours for each aircraft, servicing time, man-hours of the engineers and related maintenance.

However, this report's aim to give comprehensive explanations of the security & development lifecycle of this project (Web App), which can create records for a new **airframe**, log **flight hours** for an airframe, log **scheduled maintenance** for an airframe, maintain **a list of engineers**, assign maintenance **tasks** to engineers. And my prototype should maintain the functionality regarding those I have mentioned above. Alongside this, the strengths and weaknesses of the developed system and the legal considerations taken.

Reports:

This platform shows that the users, including the admin of ABC Air, can sign up, can log in, can manage and maintain, i.e. their Aircraft ID (airframe), flight hours, and tasks. At the same time, they can action (edit or delete) on the website. This is achieved through secure communication mechanisms, which embrace the relevant information upon signing up and a secure Web platform that allows for data reporting, storage, and adjustment.



On above, the home page is the default landing screen reached after any user has logged into the webapp. It holds many features about ABC Air for its daily business, and for its users, from who we are to our privacy policy. On the ABC Air login page, users can maintain the functionality, which I already mentioned and also, they can update their information, i.e. their tasks.

Moreover, this project has been completed by **4 Phases**, and legal considerations, as per ABC Air's requirements. Additionally, I will discuss that how the **CIA** (Confidentiality, Integrity and Availability) model is anticipated throughout this report.

See below:

Design – (A design of the system, explanation, security principles and functioning security development life cycle),

Development – (Requirement, system design, development, testing, deployment, feedback),

Security – (Strengths and Weaknesses, Testing and Analysis techniques)

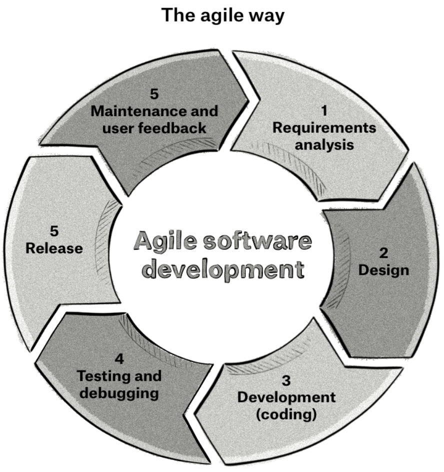
Formal Methods – (Flow charts, Wireframe, Petri Net),

Legal Considerations - (The companies act 2006, Accessibility, GDPR, Encryption and Respecting copyright).

[Ideas from 7032 CEM course materials, Day 1 - 5, from the question paper for the Coursework and own evaluation, and from Agile SDLC | Software Development Life Cycle - Javatpoint. (2021). Retrieved 27 November 2021, from https://www.javatpoint.com/agile-sdlc]

Design:

For this prototype, I have adopted the Agile model, where we would see the implementation of its SDLC, and by using the Agile model, when a cycle will be completed, I would be able to add or deduct any feature if we think that would be or would not be required for the next cycle. Each time ABC Air will be getting a different version and need to improve each time in order to get the best output for this SDLC. The reason for choosing the Agile model, that it is easy to understand, implement and straightforward to check its functionality.



However, for this Agile model, it is necessary to implement the CIA principle properly, as is required for this ABC Air's project. If I apply this security triad (CIA) for this Agile model in all Phases, which would be guaranteed in secure my design and development for ABC Air, as this principle is relevant across the whole subject of security analysis, from access to a user's internet history to security of encrypted data across the web.

I am giving some examples, as from this triad, **Confidentiality** would hide information from those people who are unauthorised by ABC Air to view it, it is most obvious when it comes under security measure. Similarly, **Integrity** is able to ensure ABC Air's data is an accurate and unchanged representation of its original secure information. Moreover, **Availability** would ensure that the information concerned is always willingly reachable to the authorised viewer of ABC Air.

[Ideas from Dr. Derrick's Feedback, 7032 CEM course materials, Day 1 - 5, own evaluation, and the SDLC photo taken from Sweeney, M. (2021). Agile vs Waterfall: Which Method is More Successful? - Clearcode Blog. *Retrieved 27 November 2021, from https://clearcode.cc/blog/agile-vs-waterfall-method/ and What is Security Analysis?. (2021). Retrieved 4 December 2021, from https://www.doc.ic.ac.uk/~ajs300/security/what.htm]*

Development (or software development lifecycle):

The main reason for adopting the Agile model is because of the purpose of the development model for my Web App proposed. As a result, of the ABC Aircraft maintenance, the Agile endorse creating prototypes very early in the Development Phase. The sequence of iterations, or modifications to the first version, will contribute to the finished product. This model is intended to represent short cycles in which the method is changed with each cycle. The model approach's Phase series consists of the following, see below:

The requirements:

The Web App provides a comprehensive and instinctive Web App for human interaction compatible with a browser to allow easy management of activities of ABC Air for its Aircraft maintenance for the civil operators.

This process will be allowing the administrator full access to all information, which I explained above; also, it gave other users the opportunity, as they need to do, as their job requirements. Additionally, it is maintaining the functionality, as per the design I have chosen, i.e. create, edit or delete; as an archive and remove older data for performance and privacy.

Furthermore, I am being flexible to evolve to meet future needs, as per this prototype performance.

System Design:

My design part was carried out using flowcharts and wireframes, as wireframes are used early in the implementation to map out the normal layout of a page, i.e. before graphic design. It is very frequently used to organise content and features on a web page.

Moreover, these flowcharts are expressed in simple terms, easy to understand all diagrams, which easily can research, schedule, develop, and sometimes can communicate in complex processes. See below:

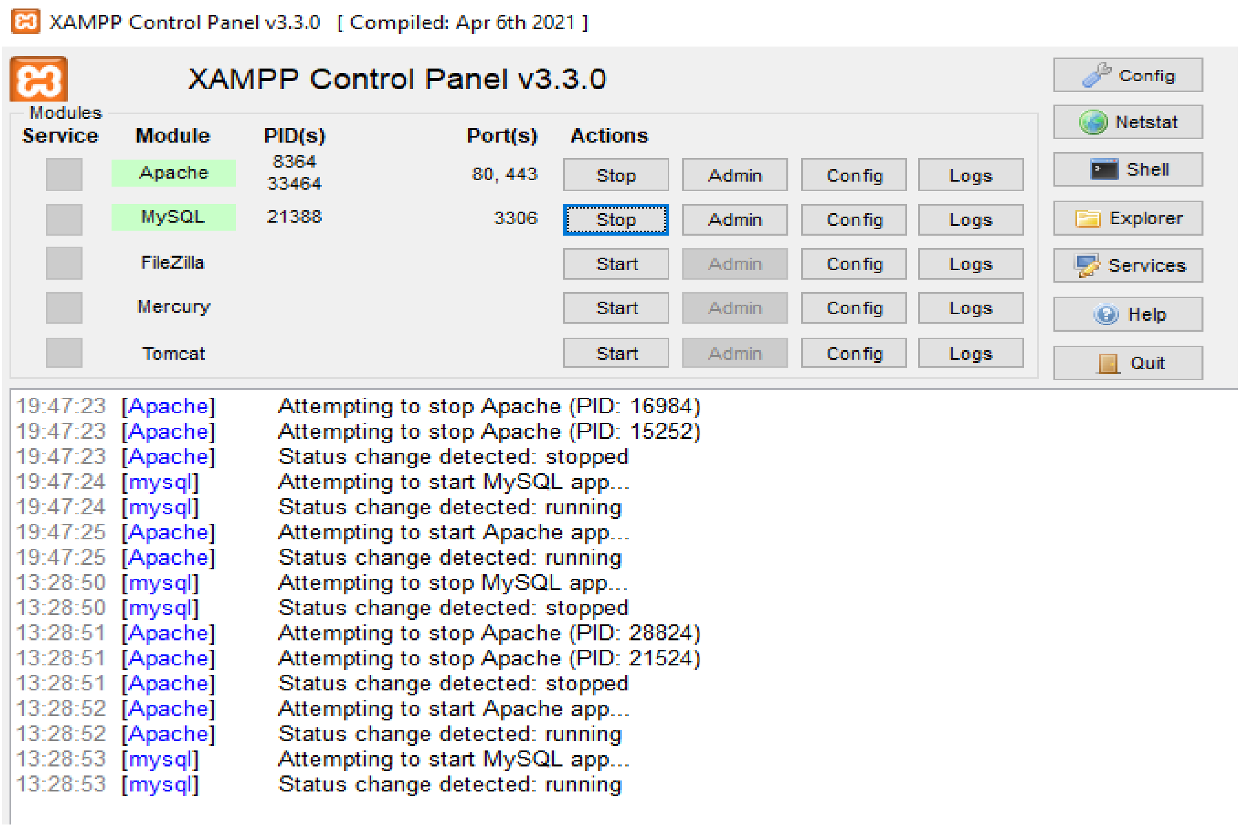
Development:

At this stage, the web application was not developed through a third-party application; however, it was in my best effort to apply coding standards throughout my code to avoid critical vulnerabilities, such as the use of vulnerable function calls. The Web App was built using the following tools.

[Ideas from 7032 CEM course materials, Day 1 - 5, own evaluation, and Software Development Life Cycle (SDLC) | Snyk. (2021). Retrieved 27 November 2021, from [https://snyk.io/learn/sdlc-software-development-life-cycle/?utm_medium=Paid Search&utm_source=google&utm_campaign=nb_ba_cnas&utm_content=sdlc&utm_term=software%20development%20life%20cycle&gclid=Cj0KCQiAy4eNBhCaARIsAFDVtI2-ZBr2AXAXTcrJc5qj4_idaFwP6gge9AWfFT_Lqykk4IlRL6fiDUkaAo89EALw_wcB](https://snyk.io/learn/sdlc-software-development-life-cycle/?utm_medium=Paid%20Search&utm_source=google&utm_campaign=nb_ba_cnas&utm_content=sdlc&utm_term=software%20development%20life%20cycle&gclid=Cj0KCQiAy4eNBhCaARIsAFDVtI2-ZBr2AXAXTcrJc5qj4_idaFwP6gge9AWfFT_Lqykk4IlRL6fiDUkaAo89EALw_wcB) and Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions. (2021). Retrieved 27 November 2021, from https://www.synopsys.com/]

See below:

XAMPP Control Panel – It was allowing me to use the Apache and MySQL services on the host computer. See below:



XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]

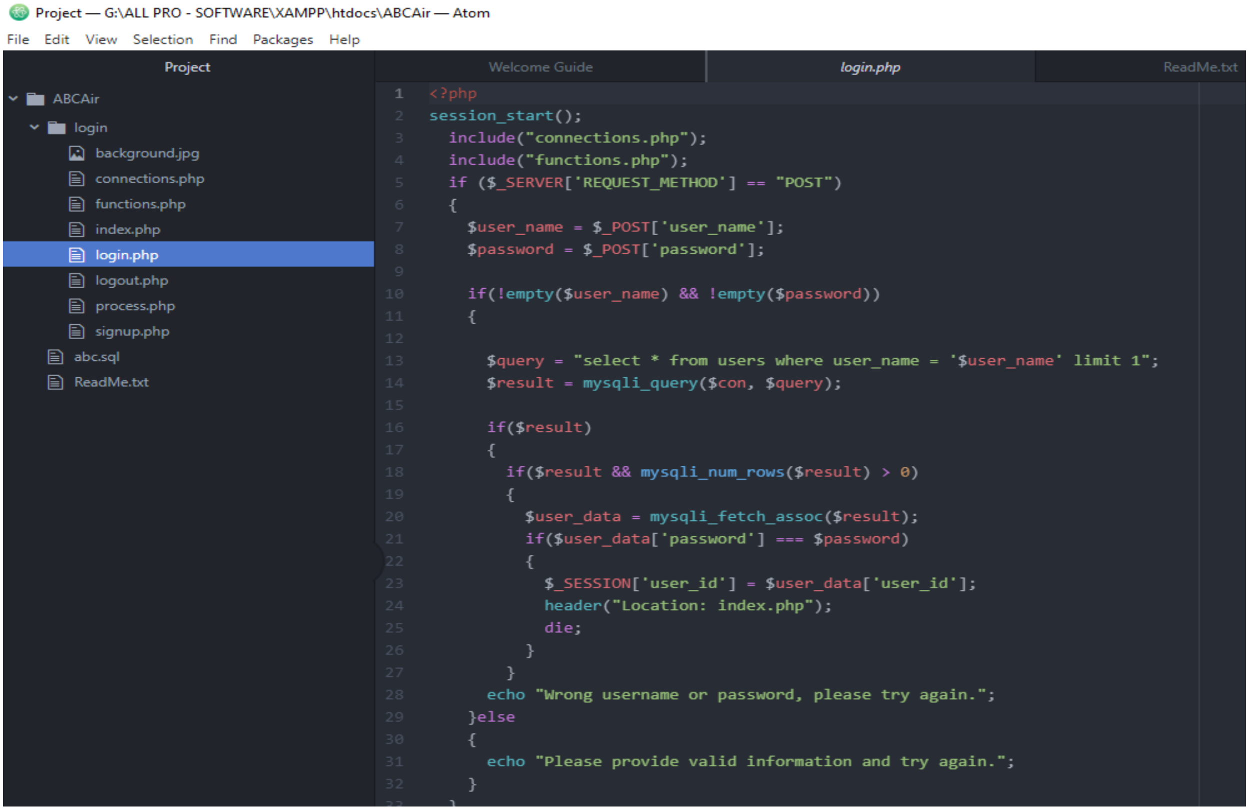
XAMPP Control Panel v3.3.0

Modules

Service	Module	PID(s)	Port(s)	Actions			
	Apache	8364 33464	80, 443	Stop	Admin	Config	Logs
	MySQL	21388	3306	Stop	Admin	Config	Logs
	FileZilla			Start	Admin	Config	Logs
	Mercury			Start	Admin	Config	Logs
	Tomcat			Start	Admin	Config	Logs

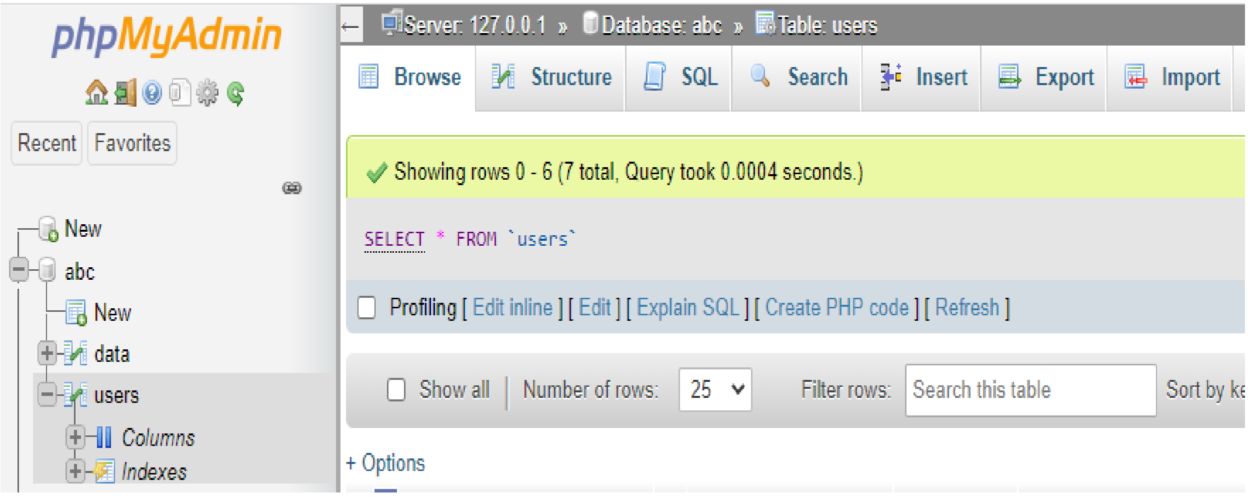
```
19:47:23  [Apache]     Attempting to stop Apache (PID: 16984)
19:47:23  [Apache]     Attempting to stop Apache (PID: 15252)
19:47:23  [Apache]     Status change detected: stopped
19:47:24  [mysql]      Attempting to start MySQL app...
19:47:24  [mysql]      Status change detected: running
19:47:25  [Apache]     Attempting to start Apache app...
19:47:25  [Apache]     Status change detected: running
13:28:50  [mysql]      Attempting to stop MySQL app...
13:28:50  [mysql]      Status change detected: stopped
13:28:51  [Apache]     Attempting to stop Apache (PID: 28824)
13:28:51  [Apache]     Attempting to stop Apache (PID: 21524)
13:28:51  [Apache]     Status change detected: stopped
13:28:52  [Apache]     Attempting to start Apache app...
13:28:52  [Apache]     Status change detected: running
13:28:53  [mysql]      Attempting to start MySQL app...
13:28:53  [mysql]      Status change detected: running
```

Atom - Text editor of choice for ABC Air.



```php
<?php
session_start();
  include("connections.php");
  include("functions.php");
  if ($_SERVER['REQUEST_METHOD'] == "POST")
  {
    $user_name = $_POST['user_name'];
    $password = $_POST['password'];

    if(!empty($user_name) && !empty($password))
    {

      $query = "select * from users where user_name = '$user_name' limit 1";
      $result = mysqli_query($con, $query);

      if($result)
      {
        if($result && mysqli_num_rows($result) > 0)
        {
          $user_data = mysqli_fetch_assoc($result);
          if($user_data['password'] === $password)
          {
            $_SESSION['user_id'] = $user_data['user_id'];
            header("Location: index.php");
            die;
          }
        }
      echo "Wrong username or password, please try again.";
    }else
    {
      echo "Please provide valid information and try again.";
    }
  }
```

phpMyAdmin - Necessary to manage the databases for ABC Air.


phpMyAdmin
Recent
Favorites
New
abc
New
data
users
Columns
Indexes
Server: 127.0.0.1 » Database: abc » Table: users
Browse
Structure
SQL
Search
Insert
Export
Import
Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
Show all
Number of rows: 25
Filter rows: Search this table
Sort by ke
+ Options

Showing rows 0 - 6 (7 total, Query took 0.0004 seconds.)

```sql
SELECT * FROM `users`
```

Alongside this, I have used other technologies, see below:

PHP - Server-side scripting used to manage dynamic content of ABC Air.

HTML and **CSS** - I used it because it's necessary to create the actual contents of the pages and necessary to provide ease of access and readability to users. Simply, they provide structure and visual layout for the app, and also, HTML and CSS and the colour vision and structure.

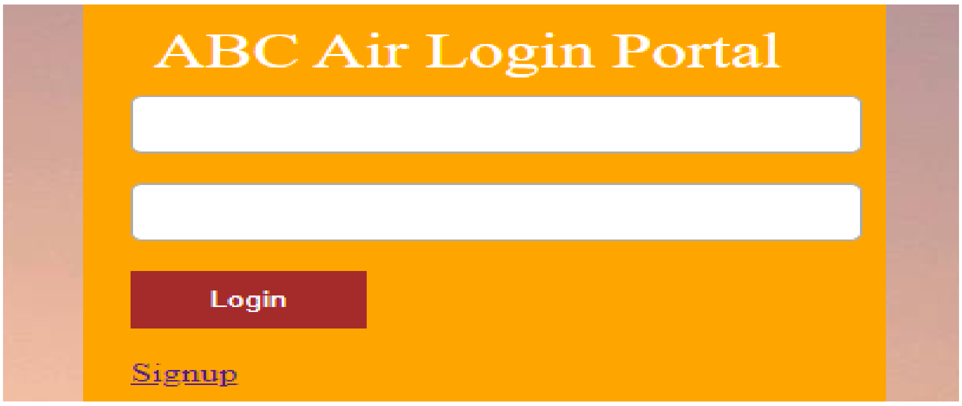
Bootstrap - I used to develop the front end of the app, which is to support the development of the records functionality.

JQuery - This is a javascript framework that greatly simplifies HTML document filtering and control for this prototype.

MySQL (Structured Query Language) - It holds the database information that is being stored.

By using those technologies above, I built the first login page of ABC Air, and all pages were done by **PHP** first, and then linked with the **PHP**; subsequently, all submitted information from **PHP** to **Database**, and **Database** is running by **MySQL**. See below:

Login Page:



Database running by MySQL:

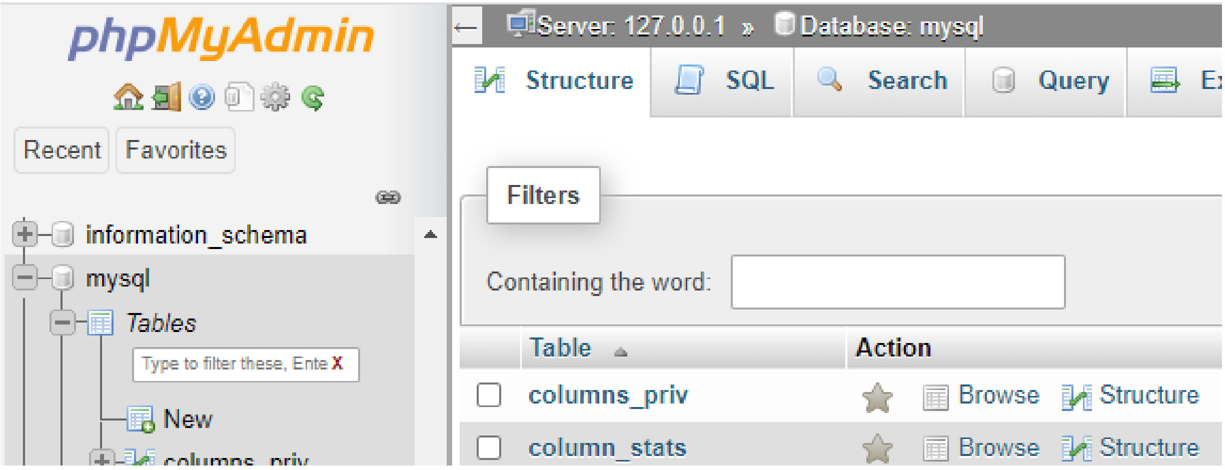


	Table	Action
□	columns_priv	Browse Structure
□	column_stats	Browse Structure

[Ideas from 7032 CEM course materials, Day 1 - 5, own evaluation, and Senior software development teams for digital products. (2021). Retrieved 27 November 2021, from https://relevant.software/ and Stack Overflow - Where Developers Learn, Share, & Build Careers. (2021). Retrieved 28 November 2021, from https://stackoverflow.com/]

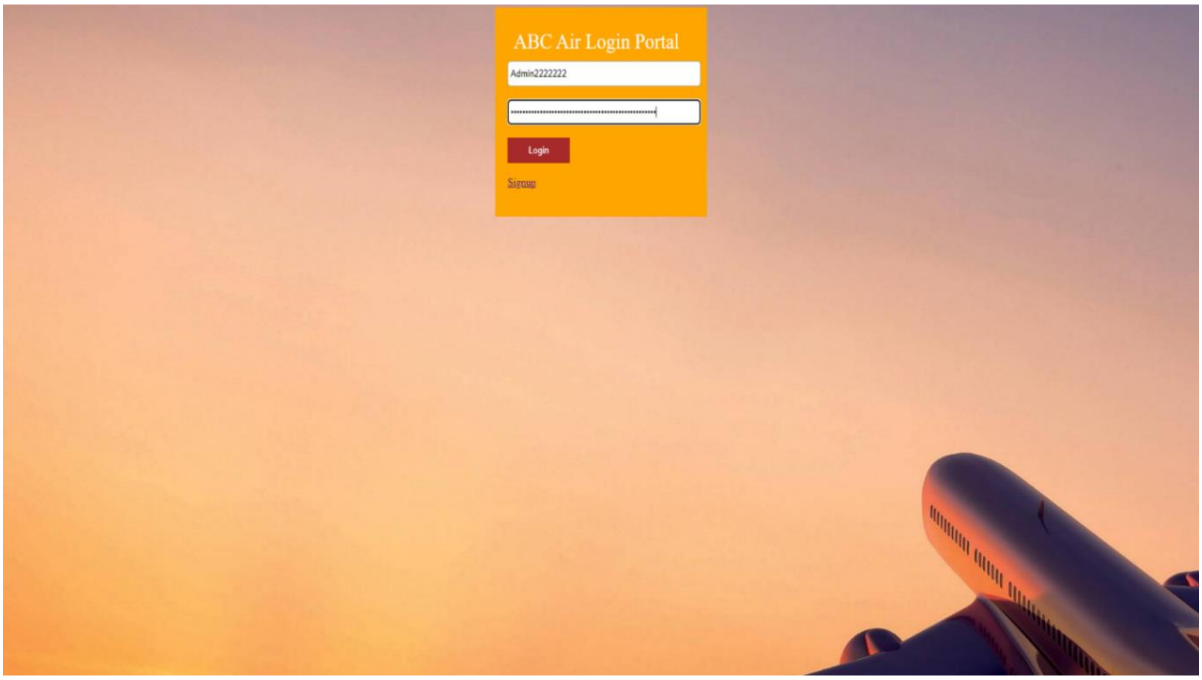
Testing:

This part (testing) is an actual test of the security measure, where I can see whether it is functioning well or not. I carried out to verify that the program can perform its basic requirements in the following ways.

White box testing – It was used for the platform to test for internal security flaws.

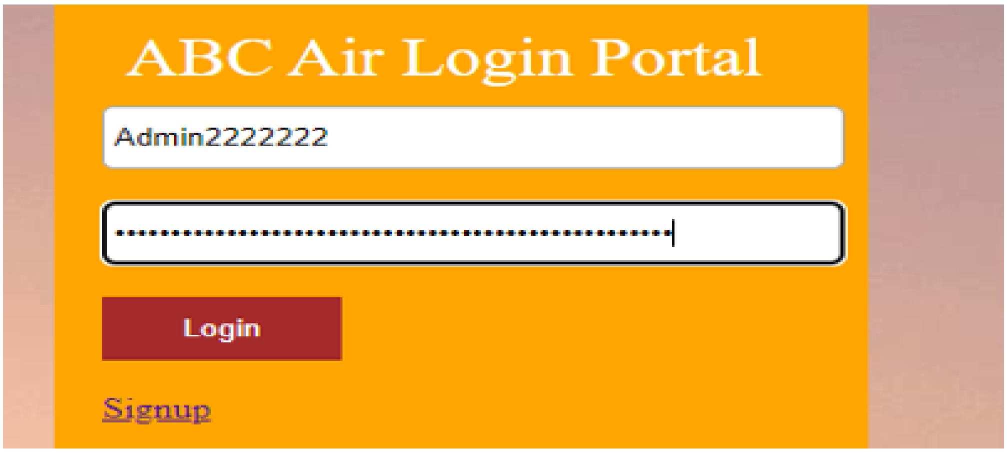
Petri net – It was used in the modelling of a logical system to test the state of the webapp.

However, signing up allows a user to provide a username and password, and that will be stored in the database. As I can say, this module was tested by providing a username and password then checking if the credentials were stored in the database as we can see in the **various screenshots**, below:
If any user tries to put a different username or password (wrong credentials), it will not allow to log in:



ABC Air Login Portal

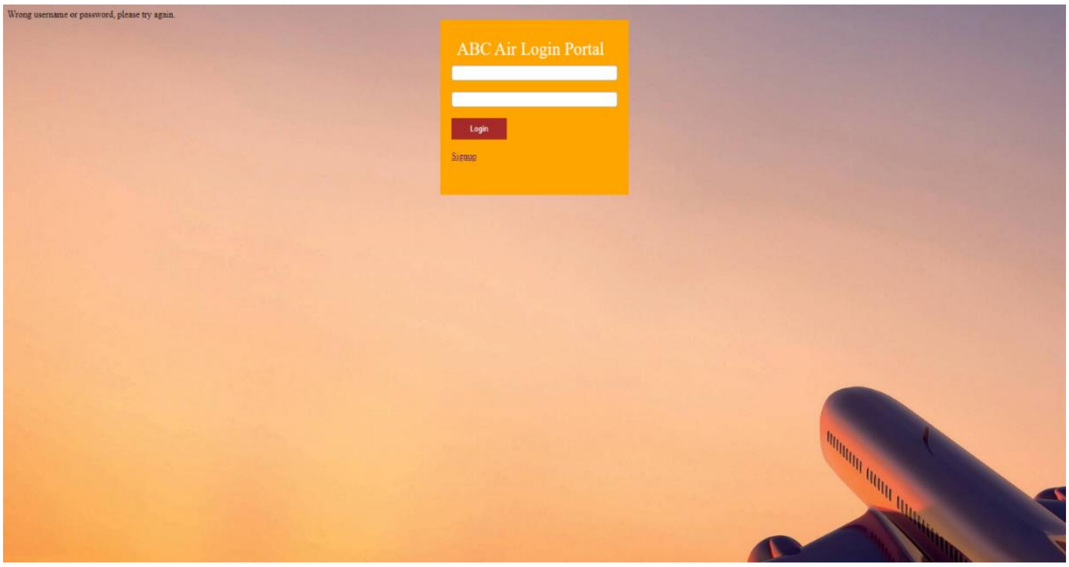
Admin2222222



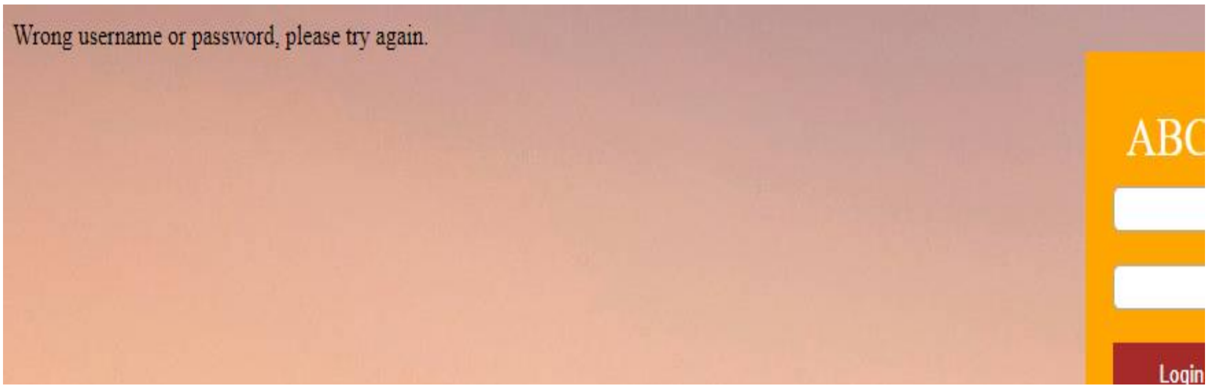
ABC Air Login Portal

Admin2222222

As a result of wrong credentials, below:

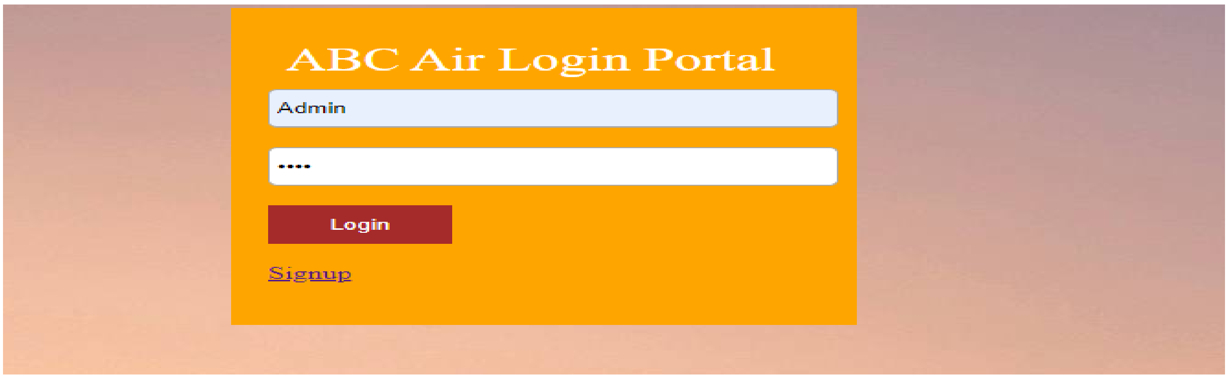


Wrong username or password, please try again.

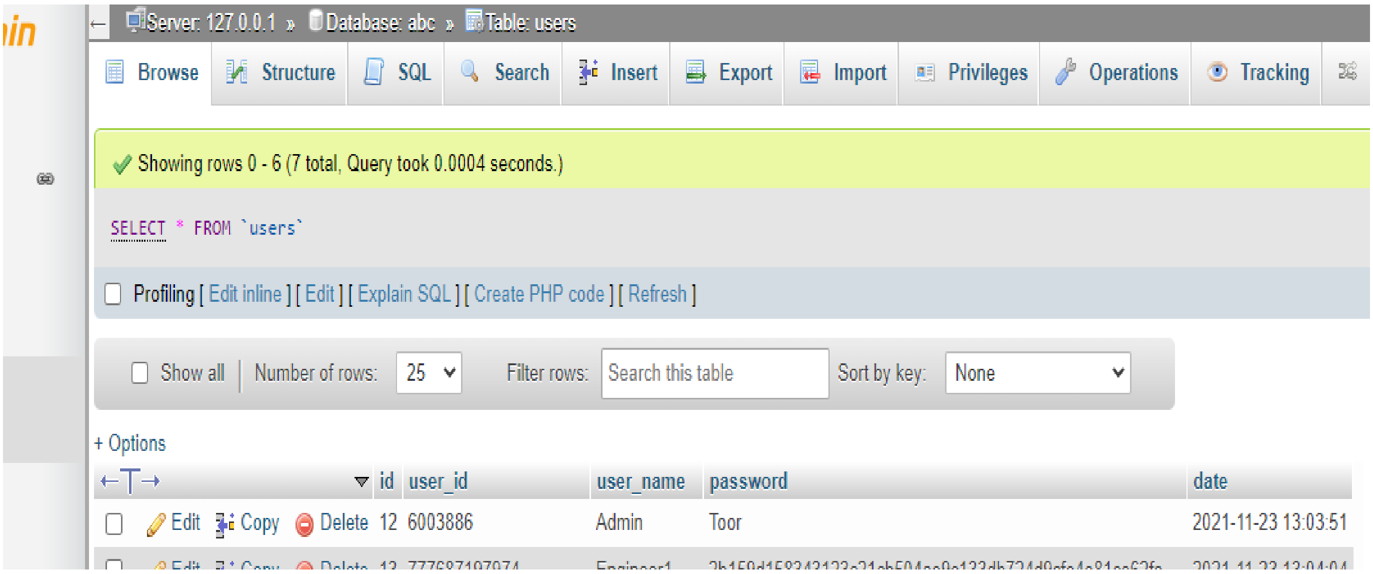


Wrong username or password, please try again.

Furthermore, login allows an already existing user to provide their credentials in order to give them access to the records; also, this module was by logging as an existing user to get access to the records. To make sure the variables go through their proper place in the Web Application, data flow analysis was done on features of the Webapp.



By signing up allows a user (*I would provide an example for Admin*) to provide a username and password that will be stored in the database. This module was tested by providing a username and password then checking if the credentials were stored in the database as can see below:



Showing rows 0 - 6 (7 total, Query took 0.0004 seconds.)

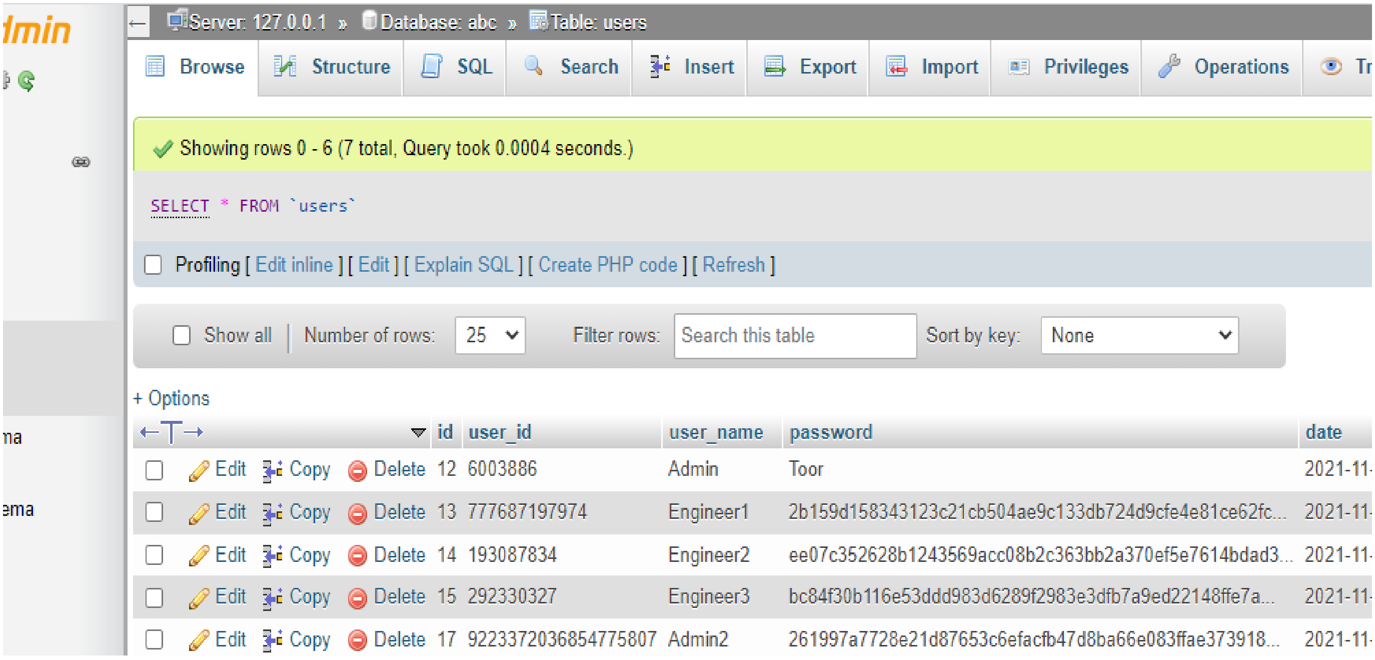
```
SELECT * FROM `users`
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

□ Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None

+ Options

	id	user_id	user_name	password	date
□ Edit Copy Delete	12	6003886	Admin	Toor	2021-11-23 13:03:51
□ Edit Copy Delete	13	777687197974	Engineer1	2b159d158343123c21cb504ae9c133db724d9cfe4e81ce62fc	2021-11-23 13:04:04



Showing rows 0 - 6 (7 total, Query took 0.0004 seconds.)

```
SELECT * FROM `users`
```

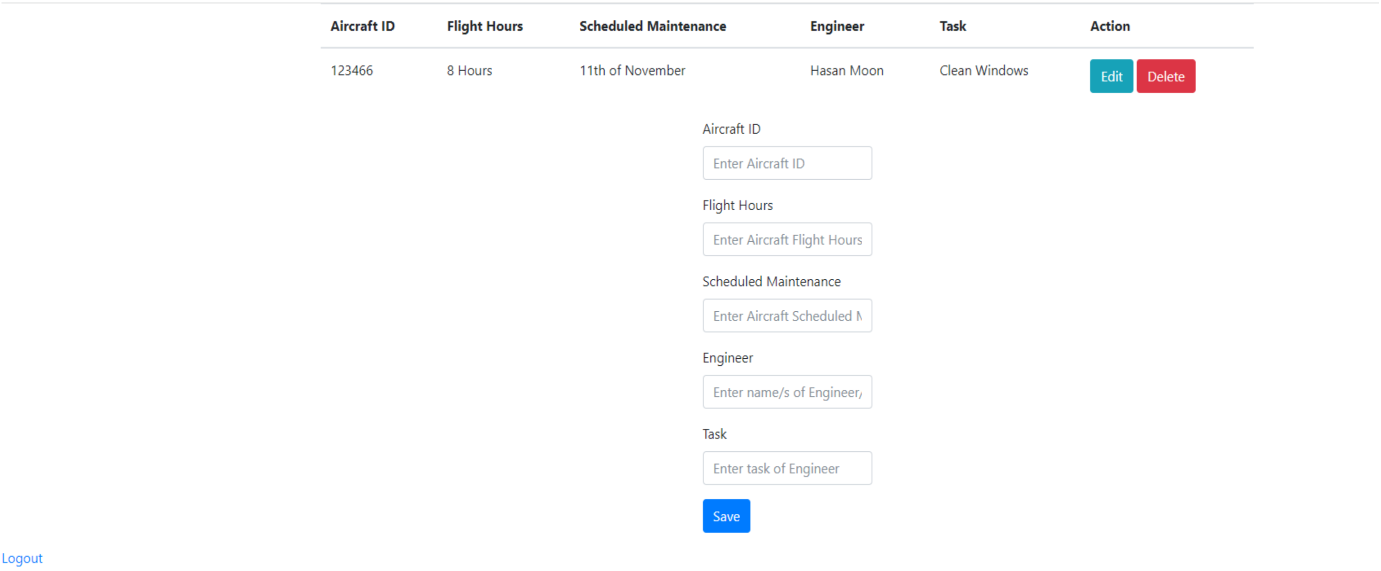
□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

□ Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None

+ Options

	id	user_id	user_name	password	date
□ Edit Copy Delete	12	6003886	Admin	Toor	2021-11-
□ Edit Copy Delete	13	777687197974	Engineer1	2b159d158343123c21cb504ae9c133db724d9cfe4e81ce62fc...	2021-11-
□ Edit Copy Delete	14	193087834	Engineer2	ee07c352628b1243569acc08b2c363bb2a370ef5e7614bdad3...	2021-11-
□ Edit Copy Delete	15	292330327	Engineer3	bc84f30b116e53ddd983d6289f2983e3dfb7a9ed22148ffe7a...	2021-11-
□ Edit Copy Delete	17	9223372036854775807	Admin2	261997a7728e21d87653c6efacfb47d8ba66e083ffae373918...	2021-11-

In a simple term, when the user put the correct username and password (correct credentials), it will allow to login (JavaScript XSS); input fields have been sanitised to protect against XSS attacks, as part of the security testing. See below:



Aircraft ID	Flight Hours	Scheduled Maintenance	Engineer	Task	Action
123466	8 Hours	11th of November	Hasan Moon	Clean Windows	Edit Delete

Aircraft ID

Enter Aircraft ID

Flight Hours

Enter Aircraft Flight Hours

Scheduled Maintenance

Enter Aircraft Scheduled M

Engineer

Enter name/s of Engineer/

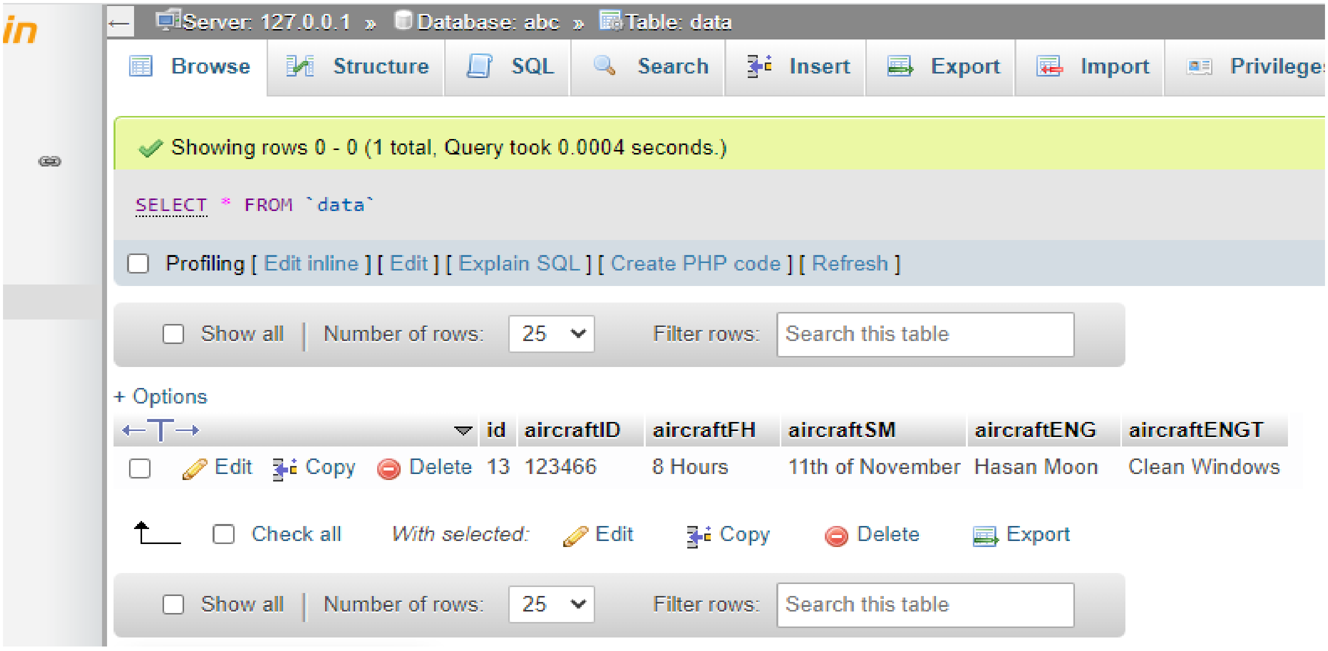
Task

Enter task of Engineer

Save

Logout

Whatever, we can see here, reflects on the Database as well. See below:



Server: 127.0.0.1 » Database: abc » Table: data
Browse
Structure
SQL
Search
Insert
Export
Import
Privileges

✓ Showing rows 0 - 0 (1 total, Query took 0.0004 seconds.)

```
SELECT * FROM `data`
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
□ Show all | Number of rows: 25 Filter rows: Search this table
+ Options

	id	aircraftID	aircraftFH	aircraftSM	aircraftENG	aircraftENGT
□ Edit Copy Delete	13	123466	8 Hours	11th of November	Hasan Moon	Clean Windows

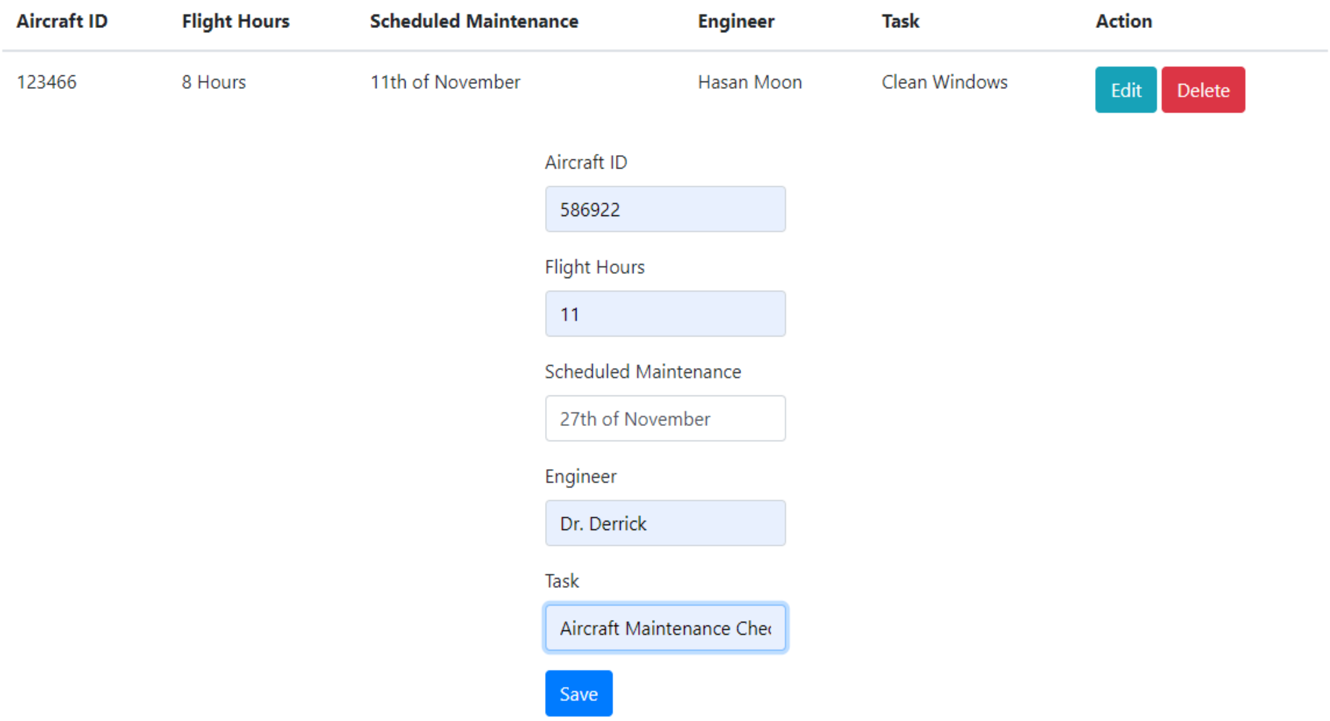
□ Check all With selected: Edit Copy Delete Export
□ Show all | Number of rows: 25 Filter rows: Search this table

[Ideas from 7032 CEM course materials, Day 1 - 5, own evaluation, and Meet Guru99 – Free Training Tutorials & Video for IT Courses. (2021). Retrieved 27 November 2021, from https://www.guru99.com/ and ReQtest: Requirements, Test Management, Bug Tracking Tool. (2021). Retrieved 27 November 2021, from https://reqtest.com/]

Deployment:

As a part of the process above, this part is significant because, in this situation, the appropriate software for the web application and the database is required for installation. And also, the source code has already been compiled, and an **admin account** has been developed.

Additionally, records were thoroughly tested by being able to read the saved records, creating new ones, and also updating and deleting existing ones See below step by step:



Aircraft ID	Flight Hours	Scheduled Maintenance	Engineer	Task	Action
123466	8 Hours	11th of November	Hasan Moon	Clean Windows	Edit Delete

Aircraft ID

586922

Flight Hours

11

Scheduled Maintenance

27th of November

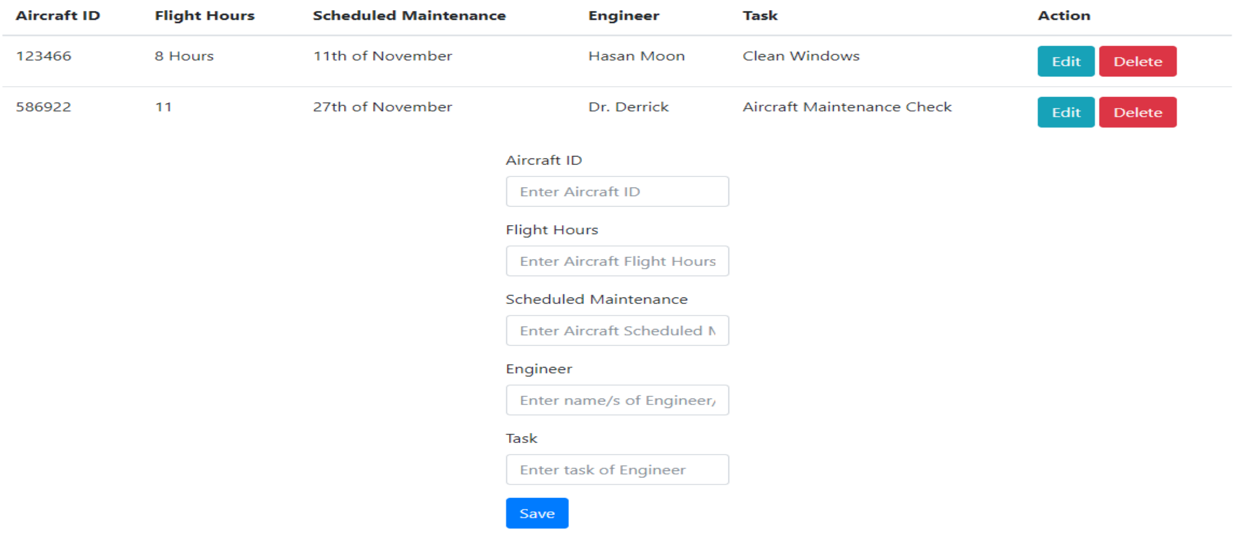
Engineer

Dr. Derrick

Task

Aircraft Maintenance Chec

After clicking the Save button, it will reflect under the previous records, and at the same time, were thoroughly tested by being able to read the saved records, creating new ones and also updating and deleting existing ones, as per the requirements. See below:



Aircraft ID	Flight Hours	Scheduled Maintenance	Engineer	Task	Action
123466	8 Hours	11th of November	Hasan Moon	Clean Windows	Edit Delete
586922	11	27th of November	Dr. Derrick	Aircraft Maintenance Check	Edit Delete

Aircraft ID

Enter Aircraft ID

Flight Hours

Enter Aircraft Flight Hours

Scheduled Maintenance

Enter Aircraft Scheduled N

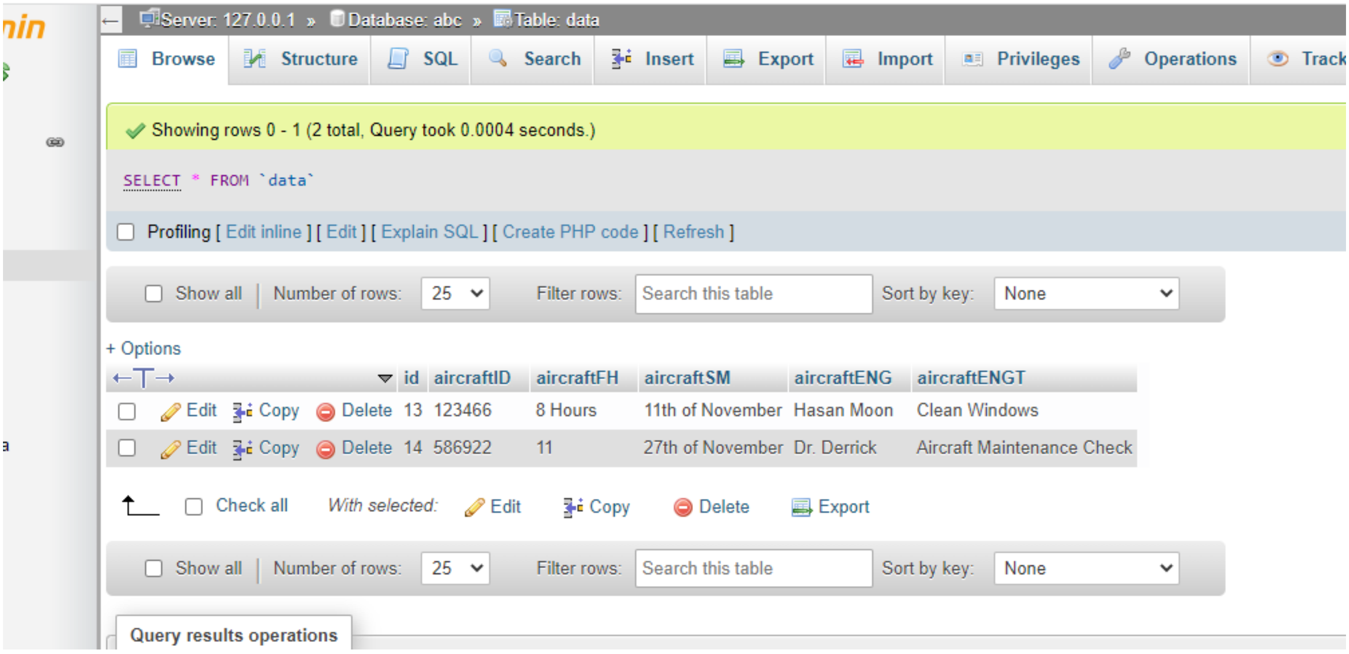
Engineer

Enter name/s of Engineer,

Task

Enter task of Engineer

However, these new records will reflect on the database as well under all the previous data. See below:


Server: 127.0.0.1 » Database: abc » Table: data
Browse
Structure
SQL
Search
Insert
Export
Import
Privileges
Operations
Track
Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None
+ Options
Check all | With selected: Edit | Copy | Delete | Export
Query results operations

✓ Showing rows 0 - 1 (2 total, Query took 0.0004 seconds.)

```
SELECT * FROM `data`
```

	id	aircraftID	aircraftFH	aircraftSM	aircraftENG	aircraftENGT
□ Edit Copy Delete	13	123466	8 Hours	11th of November	Hasan Moon	Clean Windows
□ Edit Copy Delete	14	586922	11	27th of November	Dr. Derrick	Aircraft Maintenance Check

[Ideas from 7032 CEM course materials, Day 1 - 5, own evaluation, and Desktop Management Software | Desktop Manager Solution - ManageEngine Desktop Central. (2021). Retrieved 27 November 2021, from https://www.manageengine.com/products/desktop-central/]

Feedback:

I would like to mention, propose the possible solutions if you find any errors on this website. Also, you can advise what other security measures we can take than our current security measure.

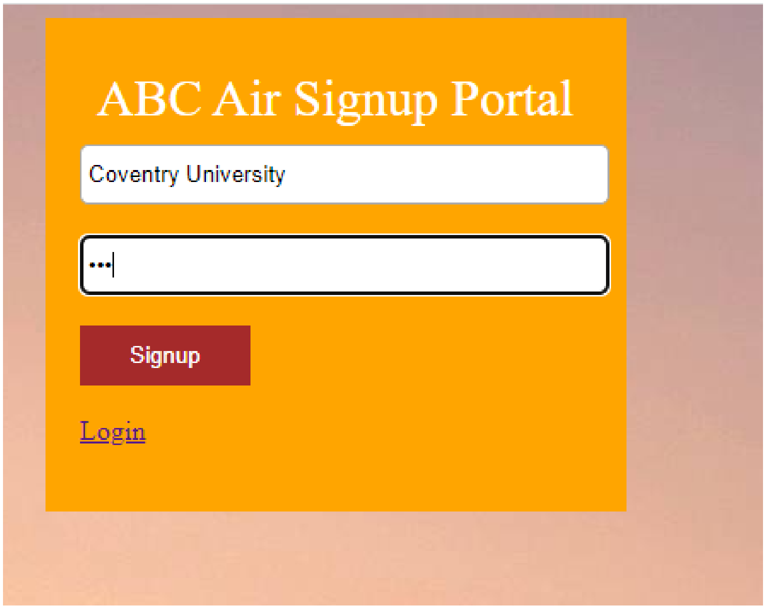
I believe this is the part where the team gathers input on the product and works through it in order to get the best output for ABC Air.

Security (security of the system)**:**

As per my prototype testing, in the signup stage security is ensured by white-listing and sanitizing both input fields using strict regular expressions as well as hashing and salting the password that is stored in the database.

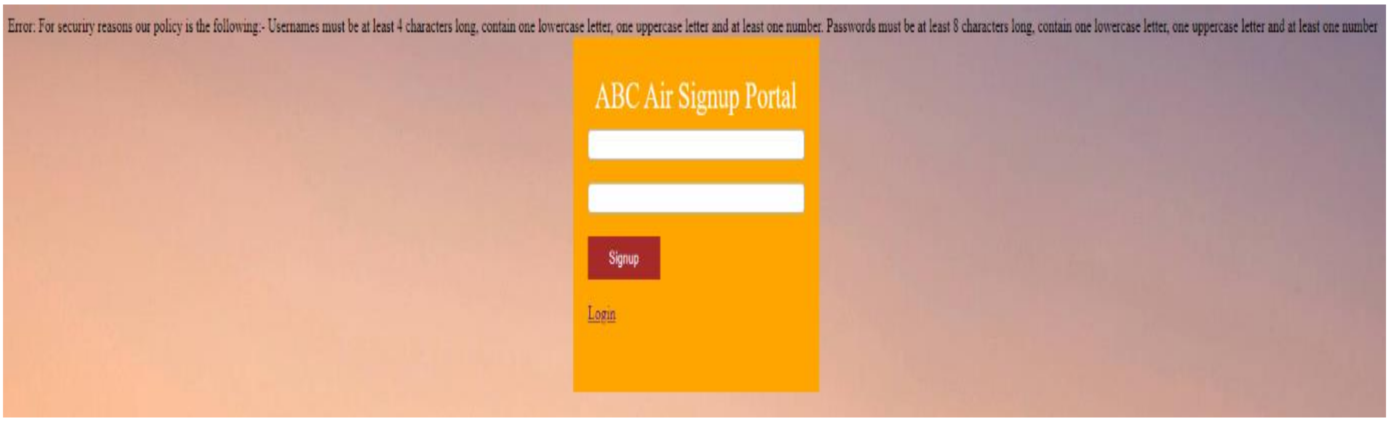
Moreover, if any user wants to be signing up a similar regular expression was applied for usernames must be at least 4 characters long, contain one lowercase letter, one uppercase letter and one number; at the same time, passwords with the only difference being that passwords must contain a minimum of eight characters long, contain one lowercase letter, one uppercase letter and at least one number.

Alongside this, by filtering out characters and strings I am mitigating against harmful code injections into the system. If a user of ABC Air fails to create an account, they will be provided specifications of the system's requirements to accept the username and password with an error; see the screenshots step by step below:

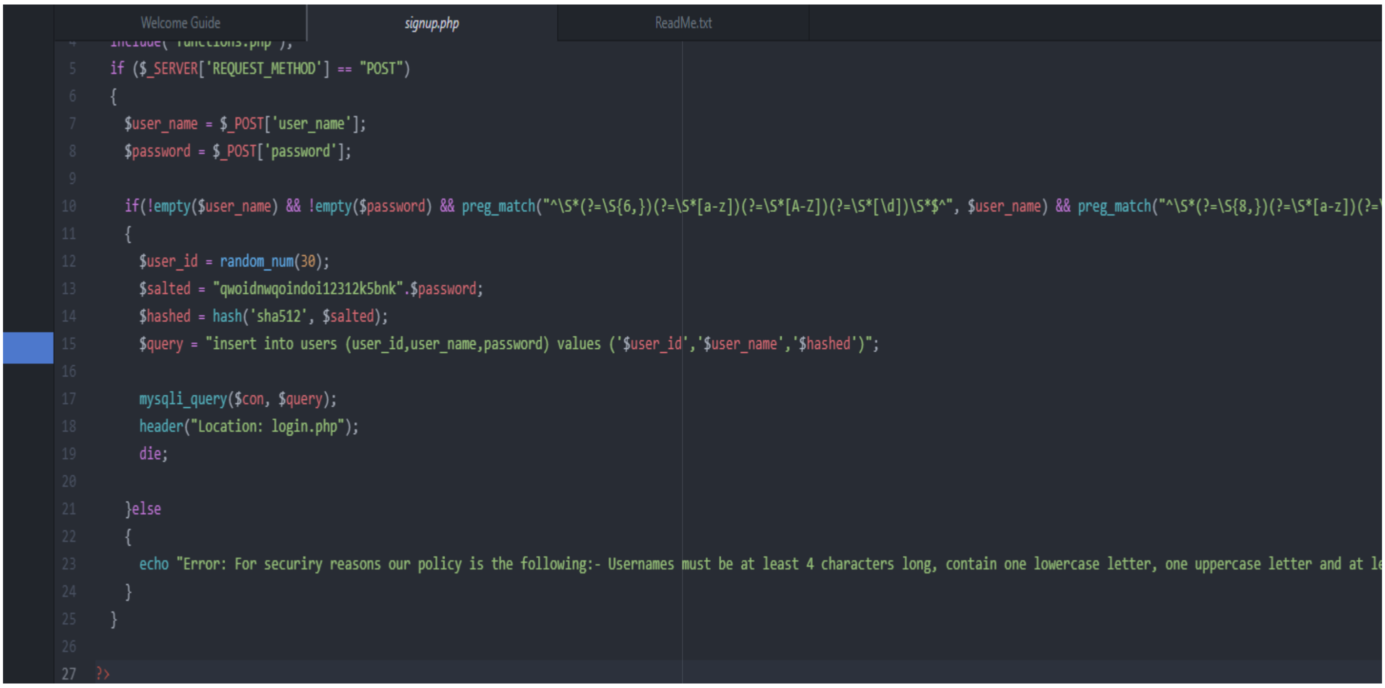


Coventry University

•••

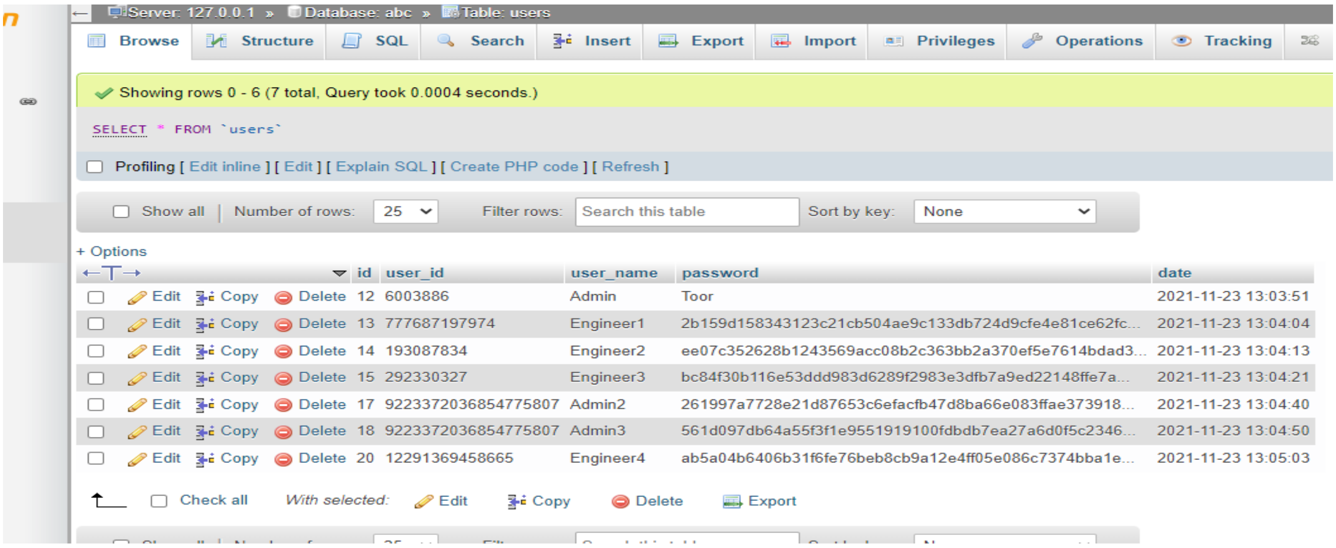


Error: For securiry reasons our policy is the following:- Usernames must be at least 4 characters long, contain one lowercase letter, one uppercase letter and at least one number. Passwords must be at least 8 characters long, contain one lowercase letter, one uppercase letter and at least one number



```php
include('functions.php');
if ($_SERVER['REQUEST_METHOD'] == "POST")
{
  $user_name = $_POST['user_name'];
  $password = $_POST['password'];

  if(!empty($user_name) && !empty($password) && preg_match("^\S*(?=\S{6,})(?=\S*[a-z])(?=\S*[A-Z])(?=\S*[\d])\S*$^", $user_name) && preg_match("^\S*(?=\S{8,})(?=\S*[a-z])(?=\
  {
    $user_id = random_num(30);
    $salted = "qwoidnwqoindoi12312k5bnk".$password;
    $hashed = hash('sha512', $salted);
    $query = "insert into users (user_id,user_name,password) values ('$user_id','$user_name','$hashed')";

    mysqli_query($con, $query);
    header("Location: login.php");
    die;

  }else
  {
    echo "Error: For securiry reasons our policy is the following:- Usernames must be at least 4 characters long, contain one lowercase letter, one uppercase letter and at le
  }
}

?>
```

As we can see here, the password is not shown in Plain Text because it is not secure to store passwords in plaintext on the database; it is not secure to store hashes of the passwords in the database due to exiting the rainbow table. If we see the screenshots, then we would see that opted to salt the password with a string of random characters then store the hash of the output in the database. See below step by step:


Server: 127.0.0.1 » Database: abc » Table: users
Browse
Structure
SQL
Search
Insert
Export
Import
Privileges
Operations
Tracking

✓ Showing rows 0 - 6 (7 total, Query took 0.0004 seconds.)

```
SELECT * FROM `users`
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
□ Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None
+ Options

	id	user_id	user_name	password	date
□ Edit Copy Delete	12	6003886	Admin	Toor	2021-11-23 13:03:51
□ Edit Copy Delete	13	777687197974	Engineer1	2b159d158343123c21cb504ae9c133db724d9cfe4e81ce62fc...	2021-11-23 13:04:04
□ Edit Copy Delete	14	193087834	Engineer2	ee07c352628b1243569acc08b2c363bb2a370ef5e7614bdad3...	2021-11-23 13:04:13
□ Edit Copy Delete	15	292330327	Engineer3	bc84f30b116e53ddd983d6289f2983e3dfb7a9ed22148ffe7a...	2021-11-23 13:04:21
□ Edit Copy Delete	17	9223372036854775807	Admin2	261997a7728e21d87653c6efacfb47d8ba66e083ffae373918...	2021-11-23 13:04:40
□ Edit Copy Delete	18	9223372036854775807	Admin3	561d097db64a55f3f1e9551919100fdbdb7ea27a6d0f5c2346...	2021-11-23 13:04:50
□ Edit Copy Delete	20	12291369458665	Engineer4	ab5a04b6406b31f6fe76beb8cb9a12e4ff05e086c7374bba1e...	2021-11-23 13:05:03

[Ideas from 7032 CEM course materials, Day 1 - 5, own evaluation, and Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions. (2021). Retrieved 27 November 2021, from https://www.synopsys.com/ and Poremba, S., Eddy, N., Eddy, N., Jennings, R., & Eddy, N. (2021). Home. Retrieved 27 November 2021, from https://securityboulevard.com/]

Security Risk Assessment:

Though it is a prototype, still I would like to focus on further security measures in this development Phase, as I would show that how it integrates with the ongoing development cycle. I will do the basic threat assessment, risk associate with the security breaches, and methodical approach to security I have been adopted, i.e. who might be interested in unauthorised access, what vector might be used, and what kind of risks associated with unauthorised access. See below:

Attackers could be outsiders or even insiders of ABC Air, they can use different methods or attack vectors for the unauthorised access to my newly built site for ABC Air, but for this, they can use the most common vectors, are Phishing, Malware, Denial of Service (DDoS) attack, Compromise Credential, Malicious insider and Web Application attacks.

If the attackers gain access to the ABC Air's system or user accounts, by gaining unauthorised access they can destroy our data, they can steal or copy our plan for another aircraft service company, they can steal ABC Air's user identities, or even, they can compromise ABC Air's system and use these for illegitimate or criminal activity, which they might do beyond our knowledge.

I would do the Risk assessment for this project, which are 4 steps, and they are, Identification, Assessment, Mitigation and Prevention.

Identification determines all critical assets of the technology for ABC Air. As a result, this diagnoses sensitive data which is created, stored or transmitted by all these assets, it creates a risk profile for each, which I have explained.

Assessment always administers an approach to assess the identified any kind of security risks for ABC Air's critical assets. After my evaluation and assessment, it determines how to effectively and efficiently allocate time and resources towards risk mitigation strategy for ABC Air.

Mitigation is the step, which defines a mitigation approach and enforces security control for each risk in ABC Air.

Prevention is the last step, which implements tools, and processes to minimise threats and vulnerabilities from occurring in ABC Air's resources.

However, with all those steps above, always I would like to have a glance at the MITRE ATT&CK framework, as this is a tool used by many cybersecurity teams to help analyse antipathetic attacks and techniques. The reason behind to glance this method is, by tracking these antipathetic methods and styles of attack, ABC Air would gain the ability to understand their cyber risk landscape from the threat actor's perspective. This method uses 3 steps, but the coping process with MITRE would be very similar to my Risk Assessments steps.

At the end of this Risk Assessments for ABC Air, there is nothing wrong if I also have a look at the OWASP Risk Assessment Framework, as it consists of Static application security testing and Risk Assessment tools, which will be able to analyse and review ABC Air's code quality and vulnerabilities without any additional setup.

[Ideas from Dr. Derrick's Feedback, 7032 CEM course materials, Day 1 - 5, own evaluation and Security Ratings & Cybersecurity Risk Management. (2021). Retrieved 4 December 2021, from https://securityscorecard.com/ and Cynet XDR | Autonomous Breach Protection. (2021). Retrieved 4 December 2021, from https://www.cynet.com/ and Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions. (2021). Retrieved 27 November 2021, from https://www.synopsys.com/ and Institute, F. (2021). Quantitative Information Risk Management | The FAIR Institute. Retrieved 4 December 2021, from https://www.fairinstitute.org/ and OWASP Foundation | Open Source Foundation for Application Security. (2021). Retrieved 4 December 2021, from https://owasp.org/]

Strengths:

I would say, each ABC Air's user data record is maintained independently and is structured to be responsive and reliable.

Furthermore, all data, including device configuration, user credentials, and logs, is encrypted and available only to the administrator; and also, web servers are used to handle all external device interfaces for the App.

Similarly, a Web Portal is available to allow our ABC Air Web App to access functions using a 128-bit SSL encrypted web browser. As we can see, the Web Portal's users are authenticated using a complex username and password combination, which I have been established in order to deter any bad activities on the website.

As I have mentioned above, user inputs are sanitised, meaning they are filtered for strings and characters to prevent the injection of harmful codes to the system; password hashing is implemented in the database. Always, after authentication, a specific session ID is designed to avoid session hijacking, and users are restricted to the functions and data that their assigned task authorises them to use.

Whenever incorrect passwords are entered on the log on tab, an error message appears demanding the correct credentials. Therefore, login updates for users require the same level of authentication as original login initialization. To my best knowledge, data is backed up regularly and safely maintained in safe offsite storage sites for recovery purposes. Examples below:

ABC Air has services working behind the scenes for the web portal to execute its set of operations. i.e.

> **Authentication** – In order to enter the Web Portal, user must first be validated with a username and a secure password; the rule I have set, which is **$query = "select * from users where user_name = '$user_name' limit 1";**
> **$result = mysqli_query($con, $query);**
>
> **Evaluating** – Regardless, all user behaviour is audited and reportable to the Administrator upon request.
>
> **Password and its Expiry Notification** – Passwords are both salted and hashed before being stored in the database. And also, rather than waiting until a user attempt to log in to the Web Portal with an outdated credential, they are informed in advance when their password is about to expire.
>
> **User's Profile** – As per the security part, a change in credentials is done every 3 months.

I am explaining more regarding the implementation of security measures to give better clarity. As I mentioned above in the **Security part** that opted to salt the password with a string of random characters then store the hash of the output in the database because a large salt value prevents precomputation attacks by attackers, including rainbow tables. It shows that each ABC Air's user password is hashed uniquely. Additionally, salts are used to safeguard passwords in ABC Air's storage.

[Ideas from Dr. Derrick's Feedback, 7032 CEM course materials, Day 1 - 5, own evaluation, and Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions. (2021). Retrieved 27 November 2021, from https://www.synopsys.com/ and Poremba, S., Eddy, N., Eddy, N., Jennings, R., & Eddy, N. (2021). Home. Retrieved 27 November 2021, from https://securityboulevard.com/ and Rainbow table - Wikipedia. (2021). Retrieved 4 December 2021, from https://en.wikipedia.org/wiki/Rainbow_table and Salt (cryptography) - Wikipedia. (2021). Retrieved 4 December 2021, from https://en.wikipedia.org/wiki/Salt_(cryptography)

Weakness:

It is better to mention the weakness as per the security measure, as this will make more sense to all. The weakness of the Web Application is the lack of a "captcha" when registering a new user for ABC Air. The unavailability of "captcha" while signing up could allow automated bots to carry out credential stuffing attacks.

In any case, if user credentials are compromised, the attacker can log in from any location. This unusual login attempt should be identified, logged and the user must be notified. Additionally, a whitelisted IP range must be allowed to login and an unrecognized IP address must be denied access.

[Ideas from 7032 CEM course materials, Day 1 - 5, own evaluation, and reCAPTCHA | Google Developers. (2021). Retrieved 27 November 2021, from https://developers.google.com/recaptcha]

Possible solutions for the issues discovered:

At this point, as the development and testing were done manually by a team of one-person further improvements include a bigger team with a variety of different web-related backgrounds working on the project. Alongside this, the use of web vulnerability scanners and tools like SQLmap should find their use within the project to automate the vulnerability assessment process in order to patch the remaining security holes present on the ABC Air website.

Moreover, as we know this is a Prototype for ABC Air, but still, we can use a multilayer approach to its security, i.e. Two Factor Authentication (2FA) is another process in order to deter unauthorised access to ABC Air's site. Additionally, if we could be used CAPTCHAs in order to restrict usage by bots, it can prevent poll skewing by ensuring that each entry is entered by a human.

[Ideas from Dr. Derrick's Feedback, 7032 CEM course materials, Day 1 - 5, own evaluation and from Auth0: Secure access for everyone. But not just anyone. (2021). Retrieved 4 December 2021, from https://auth0.com/ and Cyber Security Leader | Imperva, Inc. (2021). Retrieved 4 December 2021, from https://www.imperva.com/]

Formal Methods:

At this point, and before explaining legal considerations, I would like to go through the Formal Methods of this project.

However, before going ahead, and delivering this by Flow charts, Wireframe, Petri Net, I would like to say there are a few major benefits from the Agile methodologies are,

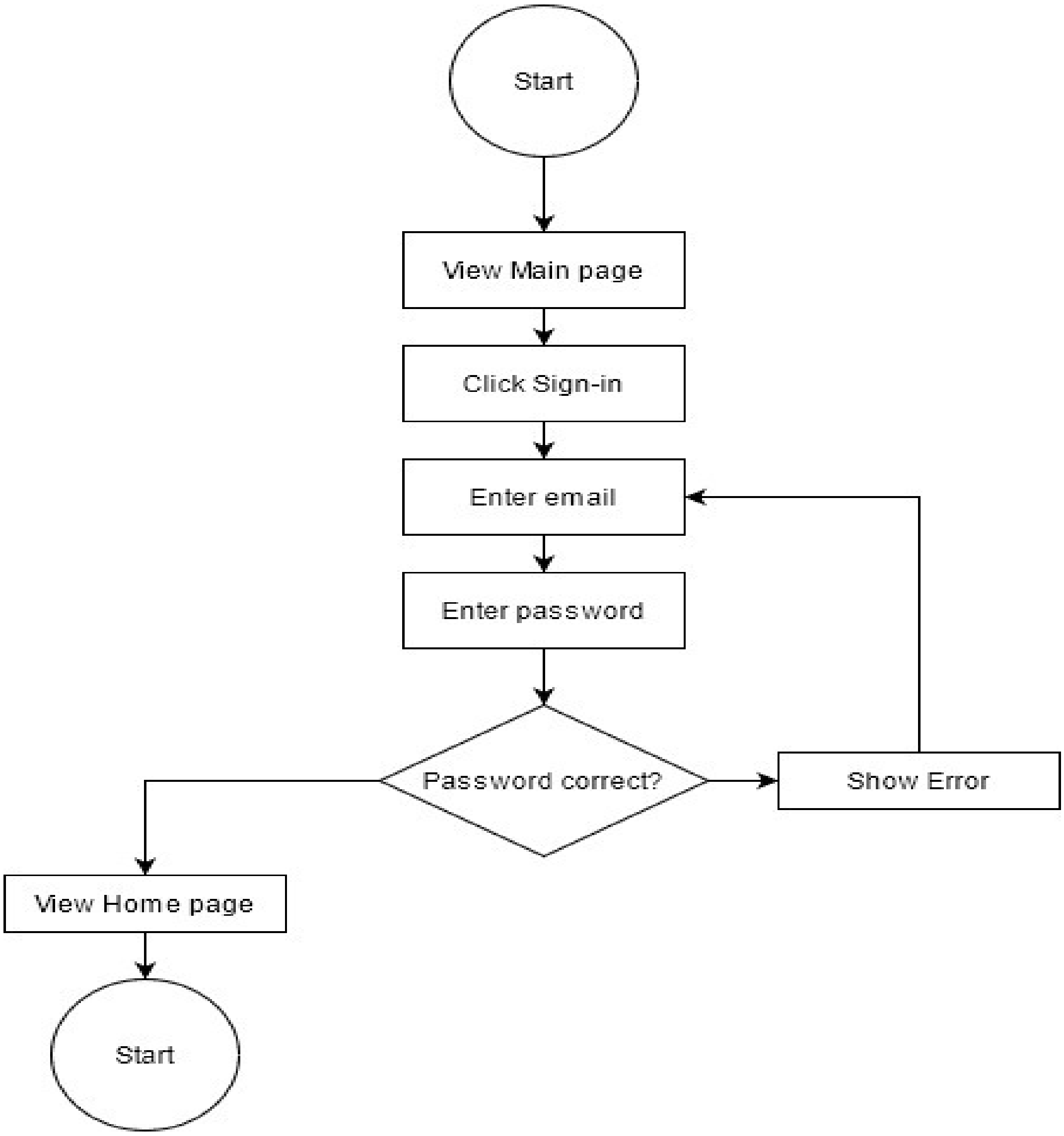
This method is a faster development process,
This is a high-quality product,
It increased Project Control,
Its reduction of Risk,
And it increased customer satisfaction.

Alongside this, using this method, retrospectively helps terms to review their types of work, improve themselves continuously. As I mentioned, in retrospect, I can uncover major and recurring security issues, which can be resolved and can avoided in the future.

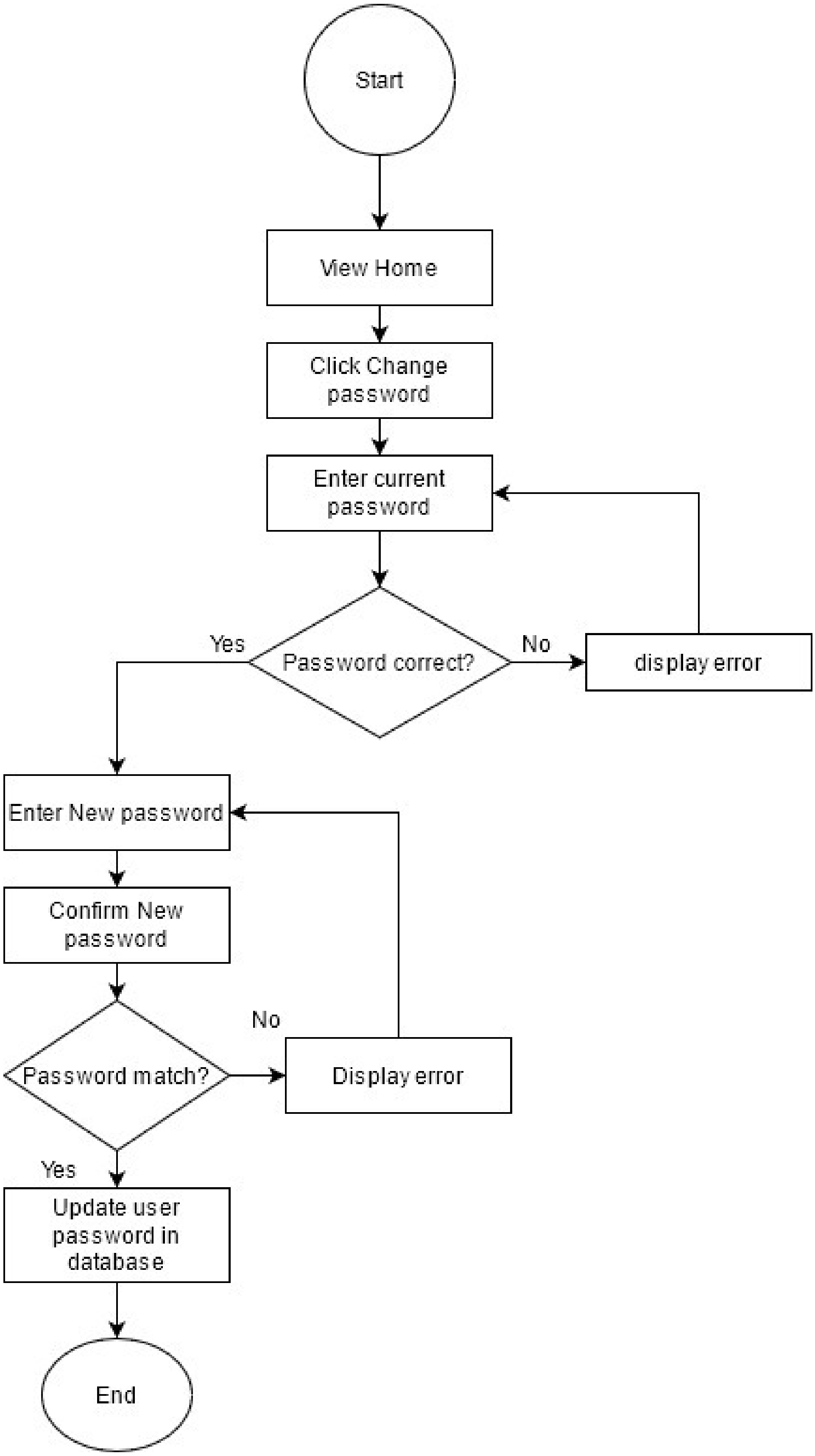
[Ideas from Dr. Derrick's Feedback, 7032 CEM course materials, Day 1 - 5, own evaluation and from Distributed Agile Teams | Self Organized Squad of IT Experts - Bridge Global. (2021). Retrieved 4 December 2021, from https://www.bridge-global.com/

See below:

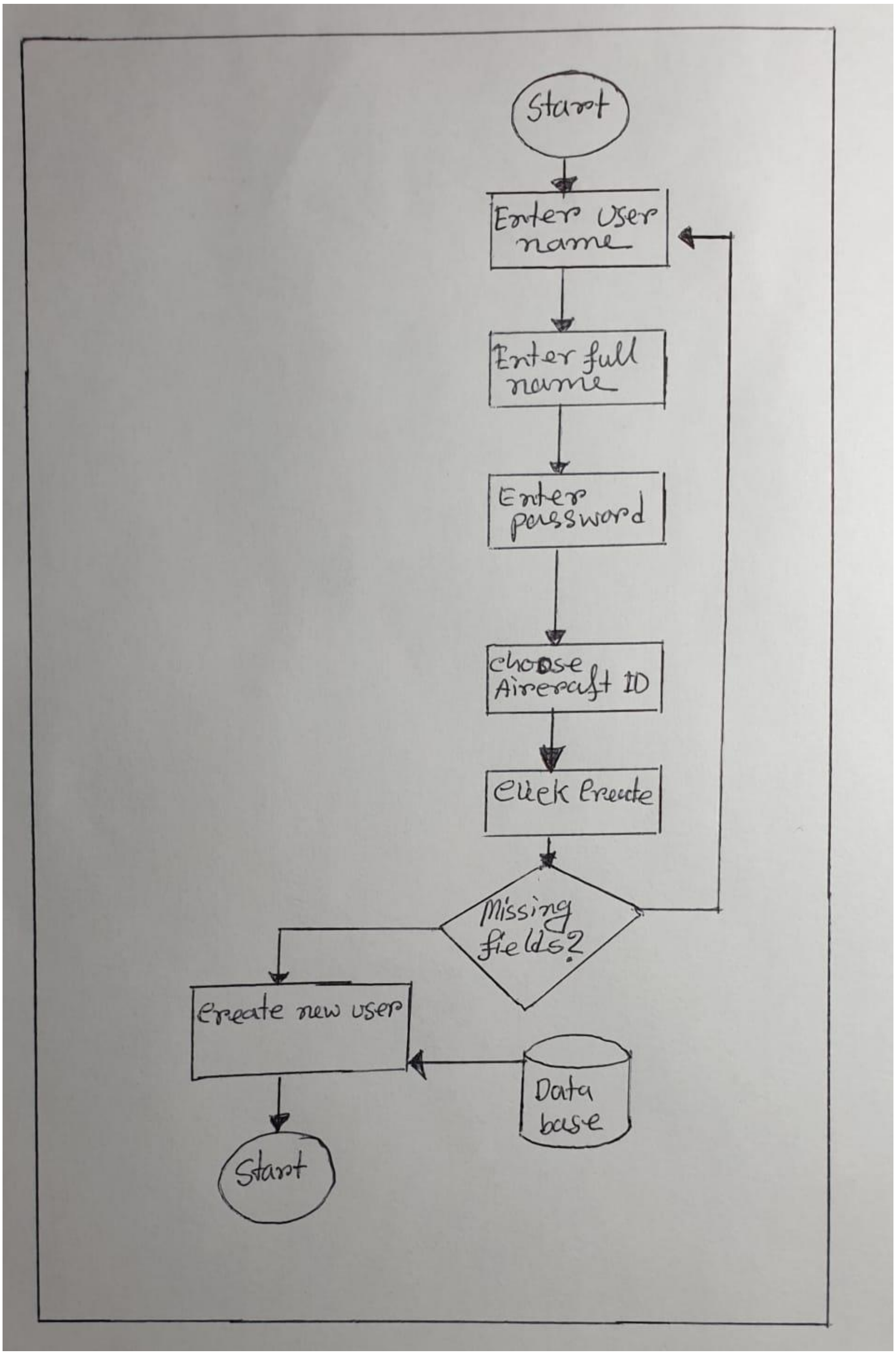
Showing the login process:



Updating user password:

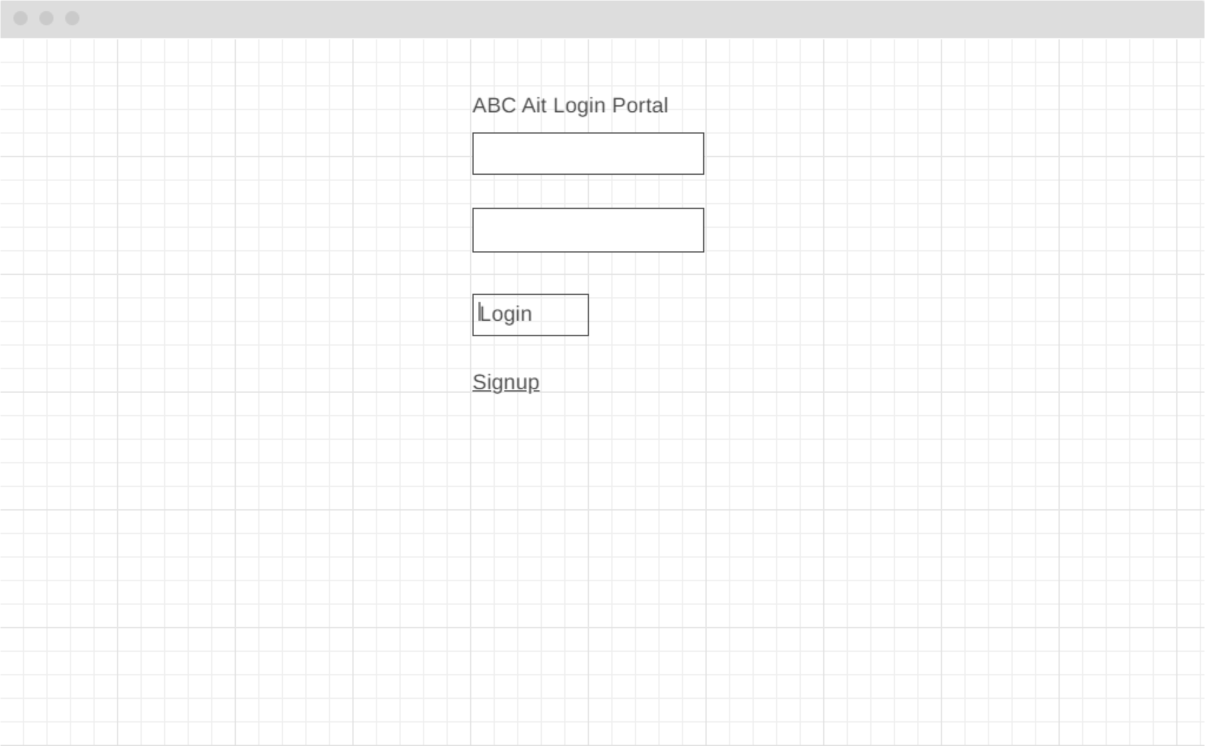


Create a new user:

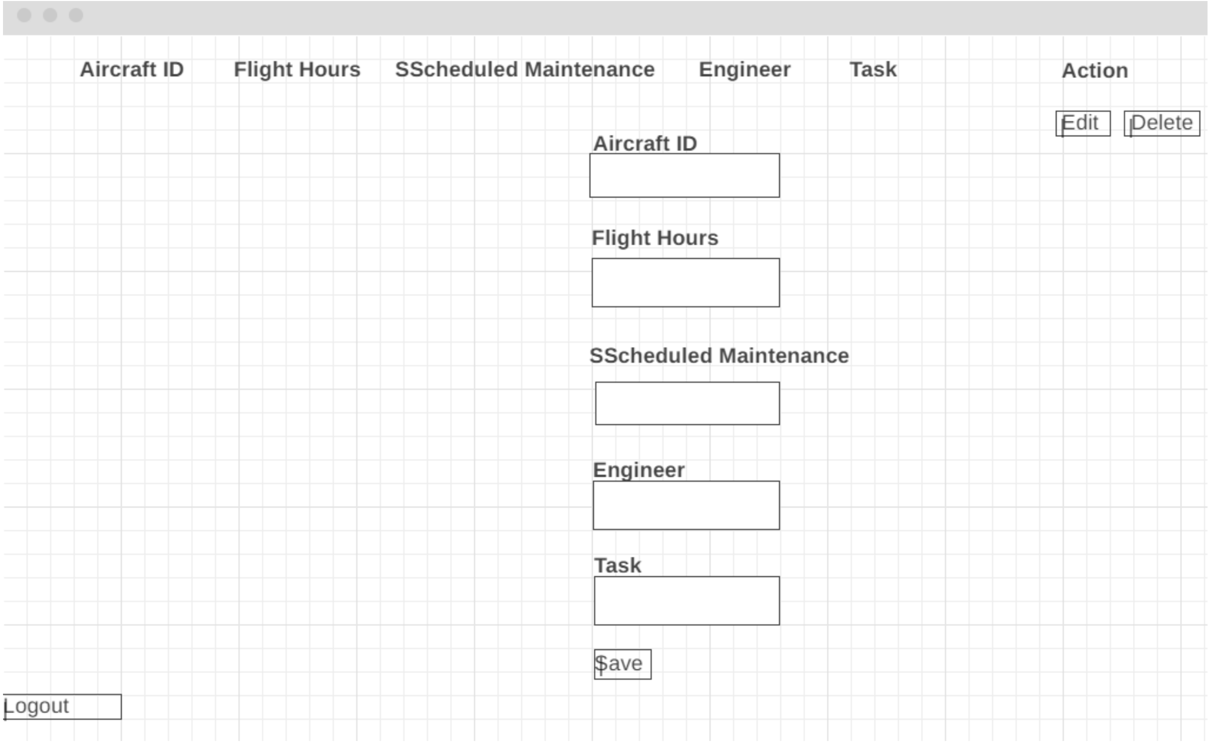


Wireframe, below:

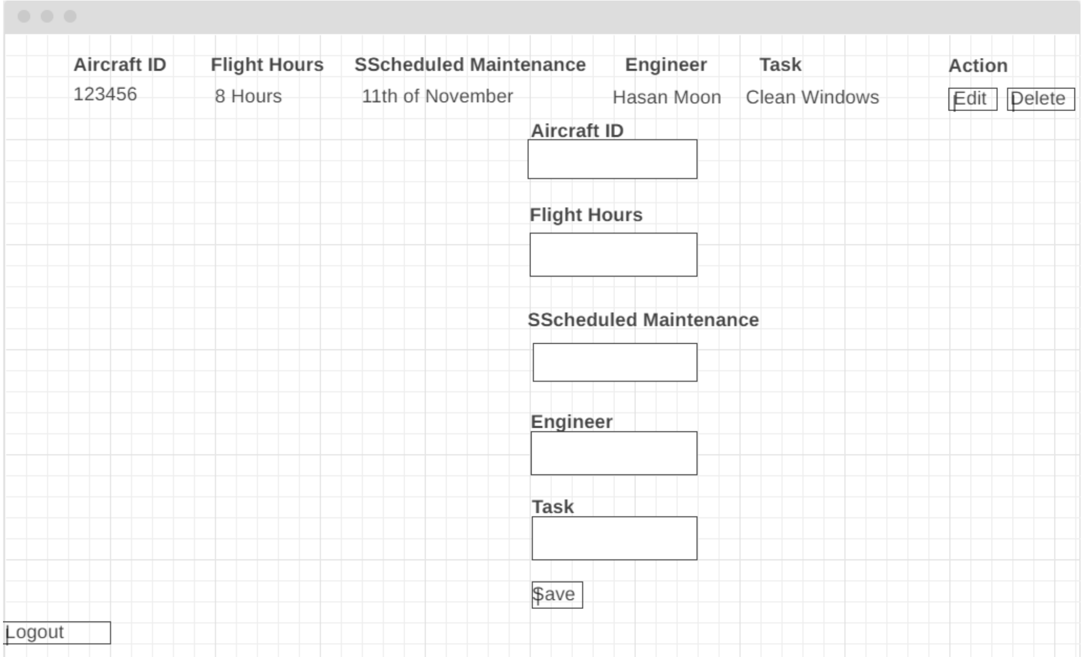
Wireframe login page:



Admin Dashboard page:



After inputting all of the information, as per ABC Air’s requirements:



Aircraft ID	Flight Hours	SScheduled Maintenance	Engineer	Task	Action
123456	8 Hours	11th of November	Hasan Moon	Clean Windows	Edit Delete

Aircraft ID

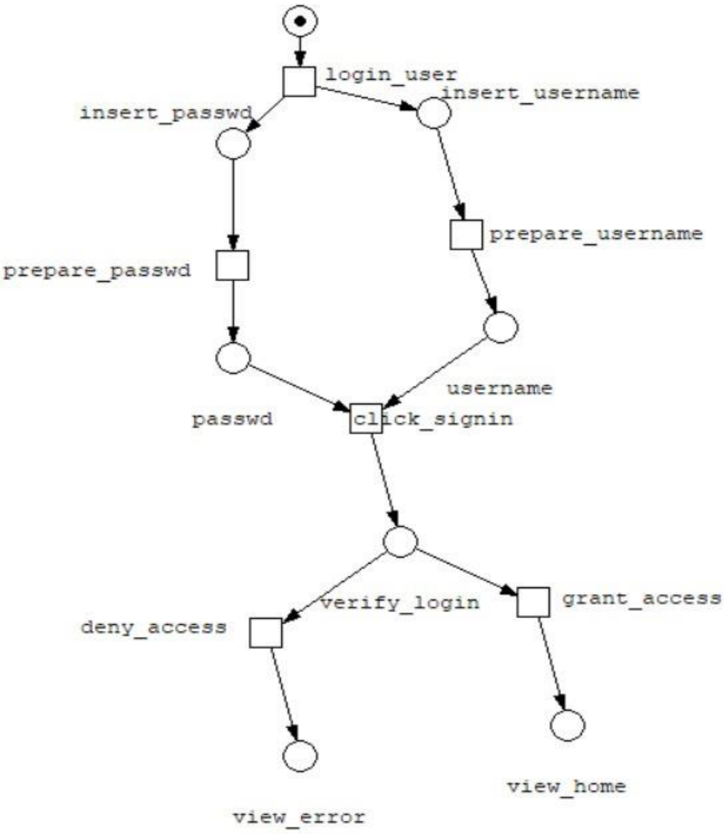
Flight Hours

SScheduled Maintenance

Engineer

Task

Petri Net:



[Ideas from 7032 CEM course materials, Day 1 - 5, own evaluation, and (2021). Retrieved 27 November 2021, from https://softwarehut.com/ and [Petri net - Wikipedia. (2021). Retrieved 27 November 2021, from https://en.wikipedia.org/wiki/Petri_net]

Legal Considerations:

This is one of the most important parts of this project, the Web App must conform with existing regulations, as we have outlined certain requirements to keep the webapp and the company on the right side of the law. Those laws are below:

The companies act 2006: For this requires entities to disclose certain information about who they are on their websites. This could include company names and addresses and non-electronic means to contact the business.

[Ideas from 7032 CEM course materials, Day 1 - 5, own evaluation, and Save Time and Improve your Marks with CiteThisForMe, The No. 1 Citation Tool. (2021). Retrieved 27 November 2021, from https://www.citethisforme.com/apa/source-type]

Accessibility: In this Cyberage, everyone that needs the website must be able to use it, and if it is not then you might be in violation of the Equality Act 2010.

[Ideas from 7032 CEM course materials, Day 1 - 5, own evaluation, and Equality Act 2010: guidance. (2021). Retrieved 27 November 2021, from https://www.gov.uk/guidance/equality-act-2010-guidance]

General Data Protection Regulation (GDPR) 2018: As per UK's implementation of the General Data Protection Regulation (GDPR) has been considered in ABC Air's Web App, as it is legislation affecting all British and European citizens and it talks about that how their personal information is used and stored.

This data and information must be protected from abuse and use on the internet, and users must be informed of data privacy breaches. Therefore, the websites must maintain the integrity of their user's records.

As such, consent forms are also given to ABC Air's users when they first come or before their signing up process. Their data is collected and stored on the ABC Air server securely and in a correct manner of GDPR.

The basis on those above, the user of ABC Air has the right to request whatever information ABC Air hold on them as well as make a request for their information to be completely erased and deleted from ABC Air's servers.

In order to do this, a data protection officer (DPO) can be employed to oversee data privacy within the organization and serve as data controls for ABC Air's users.

[Ideas from 7032 CEM course materials, Day 1 - 5, own evaluation, and Data protection. (2021). Retrieved 27 November 2021, from https://www.gov.uk/data-protection]

Encryption: For ABC Air, the information entered by a user is transmitted over the HTTPS protocol instead of HTTP, and it always should be like that.

Respecting Copyright: Like others, this particular Web App have a "Copyright, which is an amendment to the **Copyright Act 2021**. All websites and their content are automatically copyright protected as long as they are original works and including the text will prevent anyone from copying the content. This means ABC Air uses licensed and copyright images in the process, protecting the Web App's copyright.

[Ideas from 7032 CEM course materials, Day 1 - 5, own evaluation, and How copyright protects your work. (2021). Retrieved 27 November 2021, from https://www.gov.uk/copyright]

Conclusion:

The design and development (a functional secure system), I have done for ABC Air small aircraft service company, which will help them to mitigate the threats of the above risks. However, the best practices should be started as soon as they (ABC Air) become operational, by doing the best practice and following the methodology and Governance, it can run its daily business in order to protect from evil eyes.

[Ideas from Dr. Derrick's Feedback and Dr. Christo's Feedback from IDR and Ethical Hacking module]

References

[1] (2021). Retrieved 27 November 2021, from https://blog.devapo.pl/

[2] (2021). Retrieved 27 November 2021, from https://softwarehut.com/

[3] (2021). Retrieved 27 November 2021, from https://www.aha.io/software/develop-agile?utm_campaign=Global_-_Paid_Search_-_Google_-_Develop&utm_content=Develop_-_Agile_-_Exact&utm_source=google&utm_medium=paid%20search&gclid=EAIaIQobChMIl9Grvbe59AIVXOrtCh3nXAnHEAAYAiAAEgI5N_D_BwE

[4] (2021). Retrieved 27 November 2021, from https://www.rroij.com/

[5] 07606704, G. (2021). Crowd Testing QA for Web and Mobile | Global App Testing. Retrieved 27 November 2021, from https://www.globalapptesting.com/

[6] Agile SDLC | Software Development Life Cycle - Javatpoint. (2021). Retrieved 27 November 2021, from https://www.javatpoint.com/agile-sdlc

[7] Agile software development - Wikipedia. (2021). Retrieved 27 November 2021, from https://en.wikipedia.org/wiki/Agile_software_development

[8] Biggest Online Tutorials Library. (2021). Retrieved 27 November 2021, from https://www.tutorialspoint.com/index.htm

[9] ClickUp Blog. (2021). Retrieved 27 November 2021, from https://clickup.com/blog/

[10] Confidently secure apps you build and manage with Veracode. (2021). Retrieved 27 November 2021, from https://www.veracode.com/

[11] Data protection. (2021). Retrieved 27 November 2021, from https://www.gov.uk/data-protection

[12] Desktop Management Software | Desktop Manager Solution - ManageEngine Desktop Central. (2021). Retrieved 27 November 2021, from https://www.manageengine.com/products/desktop-central/

[12] Digital Transformation and Enterprise Software Modernization | Micro Focus. (2021). Retrieved 27 November 2021, from https://www.microfocus.com/en-us/home

[13] Docs.servicenow.com. 2021. *Product Documentation* | *ServiceNow*. [online] Available at: <https://docs.servicenow.com/> [Accessed 27 November 2021].

[14] Encryption - Wikipedia. (2021). Retrieved 27 November 2021, from https://en.wikipedia.org/wiki/Encryption

[15] Equality Act 2010: guidance. (2021). Retrieved 27 November 2021, from https://www.gov.uk/guidance/equality-act-2010-guidance

[16] Home - iObeya. (2021). Retrieved 27 November 2021, from https://www.iobeya.com/

[17] How copyright protects your work. (2021). Retrieved 27 November 2021, from https://www.gov.uk/copyright

[18] Infosec Resources - IT Security Training & Resources by Infosec. (2021). Retrieved 27 November 2021, from https://resources.infosecinstitute.com/

[19] Konstant Infosolutions Pvt. Ltd. 2021. *Top Mobile App Development Company in India, USA - Konstantinfo*. [online] Available at: < https://www.konstantinfo.com/> [Accessed 27 November 2021].

[20] Meet Guru99 – Free Training Tutorials & Video for IT Courses. (2021). Retrieved 27 November 2021, from https://www.guru99.com/

[21] Owasp.org. 2021. [online] Available at: <https://owasp.org/www-pdf-archive/Jim_Manico_(Hamburg)_-_Securiing_the_SDLC.pdf> [Accessed 27 November 2021].

[22] Petri net - Wikipedia. (2021). Retrieved 27 November 2021, from https://en.wikipedia.org/wiki/Petri_net

[23] Poremba, S., Eddy, N., Eddy, N., Jennings, R., & Eddy, N. (2021). Home. Retrieved 27 November 2021, from https://securityboulevard.com/

[24] reCAPTCHA | Google Developers. (2021). Retrieved 27 November 2021, from https://developers.google.com/recaptcha

[25] ReQtest: Requirements, Test Management, Bug Tracking Tool. (2021). Retrieved 27 November 2021, from https://reqtest.com/

[26] ResearchGate | Find and share research. (2021). Retrieved 27 November 2021, from https://www.researchgate.net/

[27] Save Time and Improve your Marks with CiteThisForMe, The No. 1 Citation Tool. (2021). Retrieved 27 November 2021, from https://www.citethisforme.com/apa/source-type

[28] ScienceDirect.com | Science, health and medical journals, full text articles and books. (2021). Retrieved 27 November 2021, from https://www.sciencedirect.com/

[29] Senior software development teams for digital products. (2021). Retrieved 27 November 2021, from https://relevant.software/

[30] Software Development Life Cycle (SDLC) | Snyk. (2021). Retrieved 27 November 2021, from https://snyk.io/learn/sdlc-software-development-life-cycle/?utm_medium=Paid-Search&utm_source=google&utm_campaign=nb_ba_cnas&utm_content=sdlc&utm_term=software%20development%20life%20cycle&gclid=Cj0KCQiAy4eNBhCaARIsAFDVtI2-ZBr2AXAXTcrJc5qj4_idaFwP6gge9AWfFT_Lqykk4IlRL6fiDUkaAo89EALw_wcB

[31] Sweeney, M. (2021). Agile vs Waterfall: Which Method is More Successful? - Clearcode Blog. Retrieved 27 November 2021, from https://clearcode.cc/blog/agile-vs-waterfall-method/

[32] Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions. (2021). Retrieved 27 November 2021, from https://www.synopsys.com/

[34] The A2 Posting : Website Speed Optimization Tips, News & Info. (2021). Retrieved 27 November 2021, from https://www.a2hosting.com/blog/

[35] tsoHost: UK Hosting Services and Complex Server Solutions. (2021). Retrieved 27 November 2021, from https://www.tsohost.com/

[36] Stack Overflow - Where Developers Learn, Share, & Build Careers. (2021). Retrieved 28 November 2021, from https://stackoverflow.com/

[37] What is Security Analysis?. (2021). Retrieved 4 December 2021, from https://www.doc.ic.ac.uk/~ajs300/security/what.htm

[38] *Ideas from Dr. Derrick's Feedback, 7032 CEM course materials, Day 1 - 5, own evaluation and Security Ratings & Cybersecurity Risk Management. (2021). Retrieved 4 December 2021, from https://securityscorecard.com/ and Cynet XDR | Autonomous Breach Protection. (2021). Retrieved 4 December 2021, from https://www.cynet.com/ and Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions. (2021). Retrieved 27 November 2021, from https://www.synopsys.com/ and Institute, F. (2021). Quantitative Information Risk Management | The FAIR Institute. Retrieved 4 December 2021, from https://www.fairinstitute.org/ and OWASP Foundation | Open Source Foundation for Application Security. (2021). Retrieved 4 December 2021, from https://owasp.org/*

[39] Rainbow table - Wikipedia. (2021). Retrieved 4 December 2021, from https://en.wikipedia.org/wiki/Rainbow_table and Salt (cryptography) - Wikipedia. (2021). Retrieved 4 December 2021, from https://en.wikipedia.org/wiki/Salt_(cryptography)

[40] *[Ideas from Dr. Derrick's Feedback, 7032 CEM course materials, Day 1 - 5, own evaluation and from* Auth0: Secure access for everyone. But not just anyone. (2021). Retrieved 4 December 2021, from https://auth0.com/ and Cyber Security Leader | Imperva, Inc. (2021). Retrieved 4 December 2021, from https://www.imperva.com/]

[41] *[Ideas from Dr. Derrick's Feedback, 7032 CEM course materials, Day 1 - 5, own evaluation and from Distributed Agile Teams | Self Organized Squad of IT Experts - Bridge Global. (2021). Retrieved 4 December 2021, from https://www.bridge-global.com/*