

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Modifications** | **Date** | **Members Who Modified** |
| 1 | Skeleton document/Contents | 12/7 | Pierre Lucceus |
| 2 | First draft | 12/8 | Galen Yanofsky |
| 3 | Update Login  Security Recommendation | 12/10 | Pierre Lucceus |
| 4 | Finish Software Overview | 12/14 | Galen Yanofsky |
| 5 | Finish Logging Out | 12/14 | Pierre Lucceus |
| 6 | Finish User Type:  Employee View | 12/14 | Galen Yanofsky |
| 7 | Update Security Recommendation and Troubleshooting | 12/14 | Galen Yanofsky |
| 8 | Update User Manual Contents | 12/15 | Galen Yanofsky |
| 9 | Insert Page Numbers/  Match table of contents | 12/15 | Galen Yanofsky  Pierre Lucceus |
| 10 | Update User view | 12/15 | Pierre Lucceus |
| 11 | Admin View (CRUD) | 12/15 | Pierre Lucceus |

**Contents Page**

1. **Revision Table 1**
2. **Table Of Contents 2**
3. **About This Document 3**
   1. Intended audience
   2. System requirements
4. **Software Overview 4**
   1. Human Resources Web Application
5. **User Type: Employee 7**
   1. **Logging in as an Employee**
      1. Entering credentials
   2. **Employee View 8**
      1. View own record
      2. Change own demographics
6. **User Type: Administrator 10**
   1. **Logging in as an Administrator** 
      1. Entering credentials
   2. **Administrator View 11**
      1. Searching for an employee record.
      2. Searching for employees by salary range.
      3. Updating employee’s record
      4. Creating a new record
      5. Deleting a record
7. **Logging Out 17**
   1. Logging out
8. **Security Recommendations 18**
   1. **Threats** 
      1. Social Engineering
      2. Credentials Theft
      3. Phishing
9. **Troubleshooting and Support 19**
   1. Troubleshooting
   2. Tech support

**1. About This Document:**

Human Resources Management Systems are used by businesses all over to combine a number of necessary HR functions into an easy-to-use utility. This type of software ensures that everyday business practices can be carried out with ease and as part of a standardized routine. Technological advancements in the past decade have enhanced many components of our lives and Human Resources is definitely one of those things. The first human resource management systems were primitive and often-times boasting single functionality. Today, customers have a wide variety of options to choose from based on their business goals and the unique role that human resources plays within their organizations.

The following document is an overview and instructional guide for the Human Resources Web Application for CMSC495-7981, created by Group 1. The software project is the culmination of 8 weeks of planning, creating documentation, designing, programming, and testing to ensure the set requirement specifications are met.

**a. Intended Audience**

The Human Resource Web Application is an intuitive and secure software application for managing employee accounts and employee information. The application is intended for human resources and businesses of varying size. It is scalable based on data requirements and the application infrastructure (front-end, back-end, database) is completely contained within the AWS cloud.

**b. System Requirements:**

* 1024x768 resolution or higher.
* HTML5 supported web browser:
  + Google Chrome
  + Microsoft Edge
  + Firefox
  + Internet Explorer
  + Safari
* CPU: 1.6 GHz or faster
* RAM: 1GB(32-bit) or 2GB(64-bit)

The above listed requirements are minimum system requirements that are required by most web browsers for full functionality. The application is web-accessible, meaning that the software components are not installed on the user's system. Each time the application is accessed by the user, the content is loaded via the web browser and presented to the user.

**2. Software Overview:**

The Human Resources Web Application consists of a server that hosts three frontend web pages and a backend which is comprised of a database. As stated above, the web application is designed to run on top of any HTML5 supported web browser. The three frontend web pages that comprise the application are the login web page, the user view web page, and the admin view web page. All of these components are packaged in a functional web application that is easy to use. When the application receives user input, corresponding PHP scripts convert the frontend data into structured SQL queries that returns table-format data back to the user. The following is a chronological breakdown of the the web application processes.

1. **Human Resources Web Application**

* **Browser launch:**
  1. The user launches the web application from a browser.
  2. The browser pulls the front end pages and associated scripts from the specified directory.
  3. The user is presented with the login page.
* **Authentication and login page:**
  1. The user supplies a credential pair to the system.
  2. Depending on the credentials provided (user/admin), the corresponding page is presented to the user.
  3. Prepared PHP and SQL statements authenticate the user supplied credentials with the backend database.
  4. If user supplies incorrect credentials, the web application will return a message to the user notifying them of this.
  5. Both regular and admin views allow the user different permissions.
* **Different User Views:** The user has the ability to login as either type of user upon starting the web application.
  1. **Admin view:**
     1. The admin view is displayed to the user in the case that the correct admin credentials are supplied to the web application. Select credential pairs are designated admin credential pair.
     2. The admin view allows the user to update, add, and delete employee information. The page will interface with the backend SQL database which dynamically displays data via HTML for the user’s front end.
     3. **Update Record:** After the user enters the appropriate information, the button is clicked, and the update record function modifies an existing record within the database. A PHP prepared statement carries out the specified update.
     4. **Create Record:** The administrator user enters in the specific record information that will be added to the backend database. The button is clicked and a prepared PHP statement carries out the create record operation.
     5. **Delete Record:** The deletion function will permanently remove a record from the backend database. The administrator user enters enters specified information to carry out the operation. All data for the record Is tied to the respective entries primary key. The button is clicked and a prepared PHP statement carries out the deletion operation.
  2. **User view:**
     1. The user view is displayed to the user in the case that the correct regular user credentials are supplied to the web application.
     2. The user view is very limited when juxtaposed with the functionality of the admin view page.
     3. The user view allows the logged in user read and very restricted write permissions. Specifically, the user view allows a user to read their respective demographic information field which is pulled from the backend database.
     4. The write capability allows the logged in user to either add or remove demographic information to ensure that the database reflects their most current information.
     5. If an employee moves, or experiences a life event that would change their information, then the user has the ability to change this.
* **Logging Out**
  1. At any point during the application process the user has the option to log out and terminate the application.
  2. The user can perform this action at any time by either clicking the designated logout button or exiting the browser. Both options will terminate the application.
* **AWS Cloud Components**
  1. **EC2:** Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers.[[1]](#footnote-0) The Human Resources Web Application is hosted on t2micro ec2 Ubuntu instance. The t2micro is AWS’ smallest offering for a cloud solution. The public DNS address for the application is:

[**http://ec2-52-90-44-3.compute-1.amazonaws.com/**](http://ec2-52-90-44-3.compute-1.amazonaws.com/)

* 1. **RDS:** Amazon Relational Database Service provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups.[[2]](#footnote-1) The backend database is contained within RDS.
  2. **VPC:** Amazon Virtual Private Cloud provisions a logically isolated section of the AWS Cloud where a user can launch AWS resources in a virtual network that they define.[[3]](#footnote-2) The entirety of the Human Resources Web Application is hosted through this service.

**3. User Type: Employee**

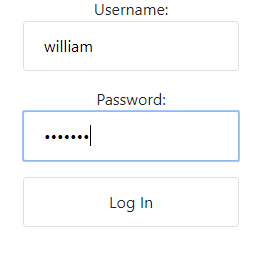
As described above in the software overview, the user view has very simple functionality. Once authenticated with the correct credentials, the user is forwarded to the Employee View. On this page the user is able to view their respective employee information that is stored in the backend database.

**a. Logging in as an Employee**

First, launch an HTML5 compatible browser. In the following example, Google Chrome is used. To do this, double-click the Google Chrome Icon. Then, enter the public DNS name of the URI where the instance and web application are hosted. Below shows the specific URI entered into the address bar of the Chrome browser.



The browser then displays the authentication page. To authenticate as the employee user, the specific test credentials are used.



The test credentials used above are as listed below:

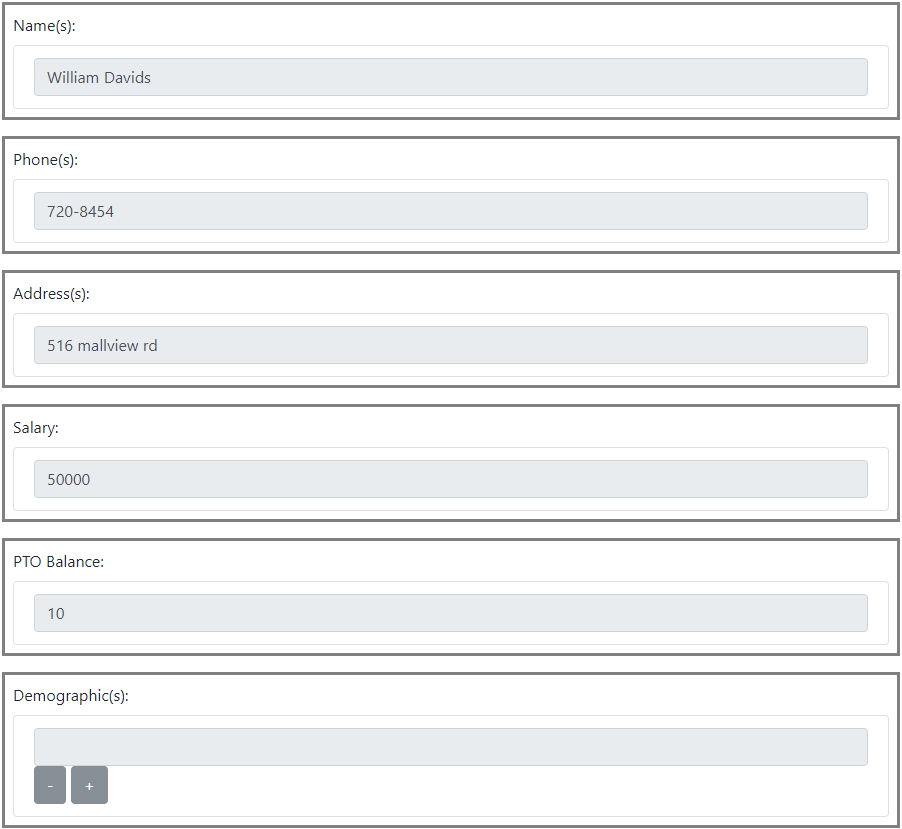
**Username:** william

**Password:** cmsc495

**b. Employee View**

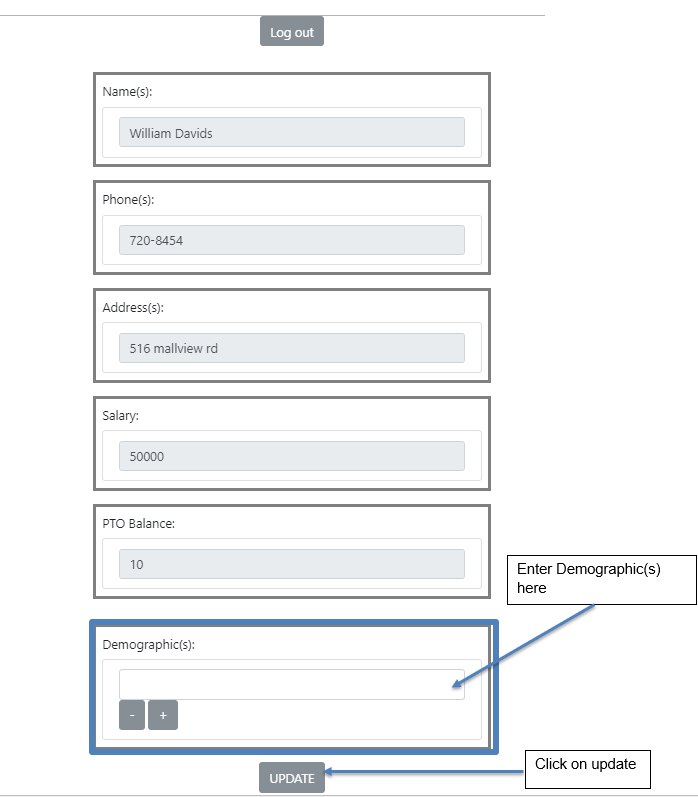
* + 1. View own record

When the user successfully logs in, the employee view is displayed.



* + 1. **Change Own Demographics**

On this page, the user has the ability to read all of their associated employee information that is subsequently stored in the backend SQL database. The user also has the ability to change their **Demographic**  information and have it reflected in the backend SQL database. Once the information is entered, the user can click the update button to commit the changes.



**3. User Type: Administrator**

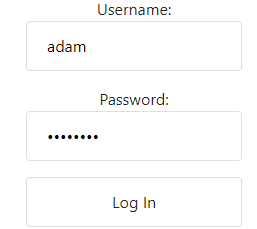
For the Human Resources Web Application, the administrator is the privileged user. The user that is logged on as the administrator has many more permissions than the employee type user. As explained in the Software Overview, once logged in, the administrator is able to perform the following functions:

* **View All Records:** Queries database to display all records to the admin user.
* **View Specific Record:** Queries database to display a specific record to the admin user.
* **Create Record:** Creates a record in the backend database.
* **Delete Record:** Deletes a record in the backend database.
* **Update Record:** Updates a record in the backend database.

**a. Logging in as an Administrator**

First, launch an HTML5 compatible browser. In the following example, Google Chrome is used. To do this, double-click the Google Chrome Icon. Then, enter the public DNS name of the URI where the instance and web application are hosted. Below shows the specific URI entered into the address bar of the Chrome browser.

  
The browser then displays the authentication page. To authenticate as the administrator user, the specific test credentials are used.



The test credentials used above are listed below:

**Username:** adam

**Password:** password

**b) Administrator View**

Once the admin user is authenticated, the user is presented with the administrator view. The administrator view is comprised of 3 components. The entire administrator view is below:

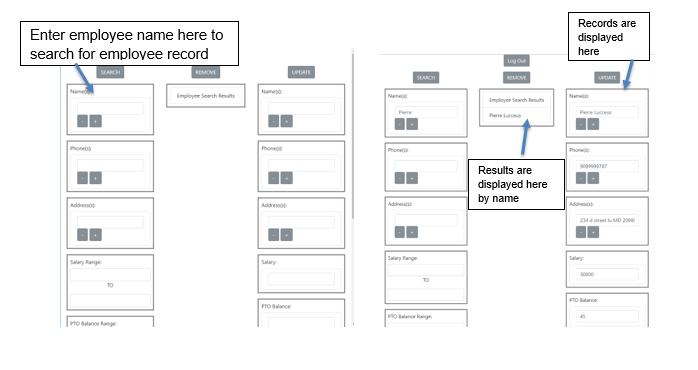


Each of these fields can be viewed or edited depending on what is trying to be accomplished. The administrator user also has the ability to create a new record which will be added to the backend database. The backend database is written in SQL and each button maps to a specific SQL operation to perform the individual function. The left portion of the view is for searching employee records. The right portion of the view is for updating employee records. The fields that are listed include:

* Name(s)
* Phone(s)
* Address(s)
* Salary Range
* PTO Balance Range
* Demographic(s)
* Note(s)

**i) Searching for an Employee Record.**

1. Enter Employee name in the name box
2. Press search
3. The employee name is displayed
4. Record/information displayed on the left

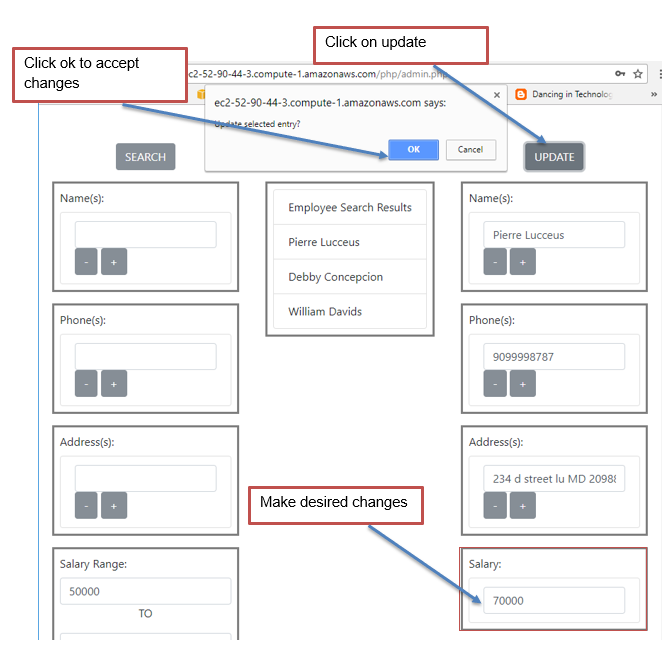


**ii) Searching for Employees by Salary range.**

1. Enter the values
2. Press search
3. All employees names are displayed
4. Click on the desired Employee to see record



**iii) Updating Employee’s Record**



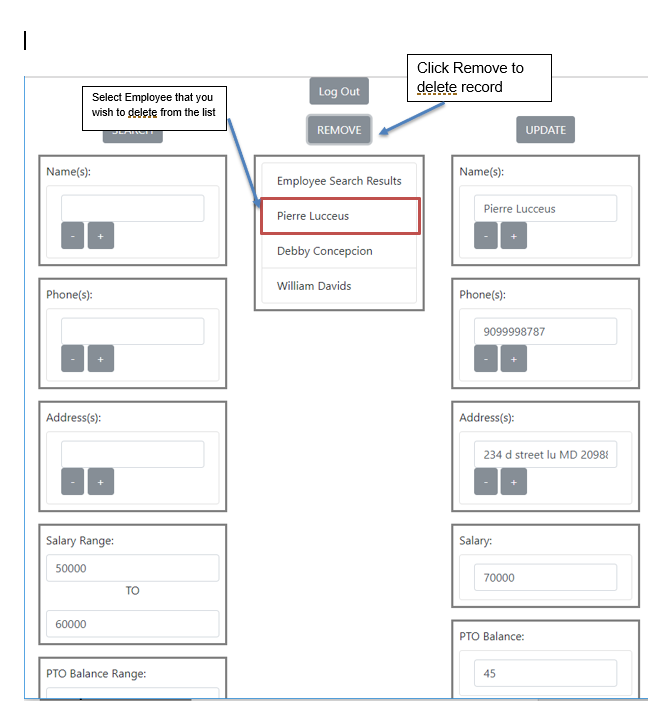
**iv) Creating a new record**

1. Enter Employee’s information in the left fields
2. Click on Add
3. Employee’s record is created
4. To view record refer to Searching Employee Record



**v) Deleting a record**

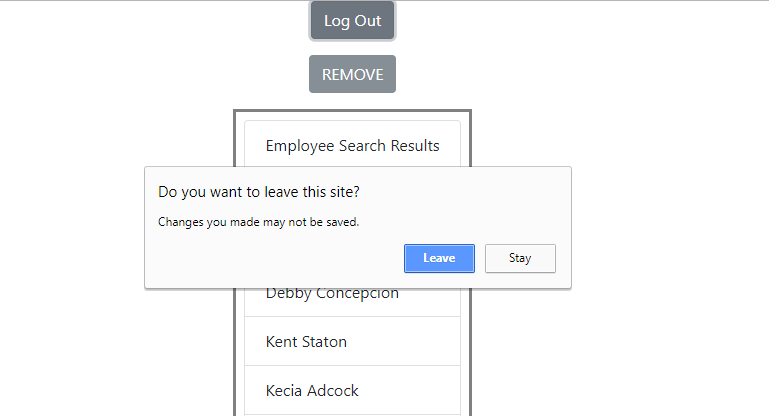
1. Select Employee that you wish to delete from the list
2. Click Remove to delete record

****

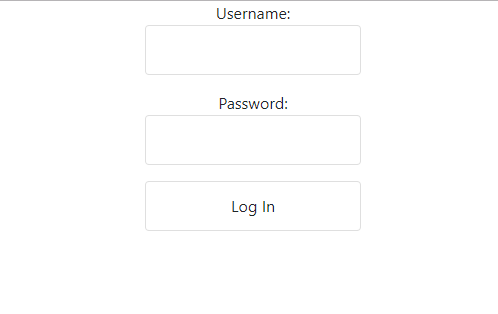
**5. Logging Out**

To logout of the application, click on the logout button on the upper right hand corner of the user view page.





Once Logged Out, the user is directed back to login page.



**6.** **Security Recommendations**

**a. Threats**

This application was designed with security in mind and was thoroughly tested for various security vulnerabilities and against different types of attacks. In order for the application to be truly secure, the user must be aware of attacks vectors that you may be exposed to:

**i.** **Social Engineering**

* Users must be aware of attackers manipulating them in order to extract confidential information. In the case of this web application, user credentials may be the target of extraction. Never discuss or share your credentials with anyone. Technical support will never ask you for password information. Consider it a red flag if someone does so.

**ii.** **Credentials Theft**

* There are many different ways that attackers and thieves can steal user credentials. The user must be pay close attention to how they operate in the online environment. Tactics that result in credential theft include: fraudulent emails, fake or malicious landing pages, viruses, and malware. Always access your account directly and from a trusted host.

**iii.** **Phishing**

* Attackers often use email to gather (Phishing) information to steal user credentials and sensitive information. Be aware of messages from unknown sources and unusual requests from unfamiliar individuals.

**7. Troubleshooting and Support**

**a. Troubleshooting:**

**i. Unable to log in:**

* Account is locked due to excess failed login attempts. Contact Administrator.
* Caps-Lock may be enabled. Disable Cap-Locks and try again.
* Wrong user type. Make sure user type corresponds to user-provided credentials. To login as an employee, the user must choose employee credentials. To login as an admin, the user must specify admin credentials. Username and password must match stored credential sets.

**ii. No response:**

* Server is down. Try again later.
* No internet connection. Check your internet connection and try again.
* Browser is not supported. Ensure that you are using a compatible browser. Refer to System Requirements.

**b. Technical Support:**

* **Contact Group 1 Through Class Discussion.**

1. https://aws.amazon.com/ec2/ [↑](#footnote-ref-0)
2. https://aws.amazon.com/rds/ [↑](#footnote-ref-1)
3. https://aws.amazon.com/vpc/ [↑](#footnote-ref-2)