# SecureED.

*User manual*

# Abstract

SecureED. is a webapp that simulates a university registration system. It is an updated version of SecureED v. 1.0 (https://github.com/onniegit/SecureEd-1.0). It is intended to show several common software vulnerabilities in an educational setting, and to demonstrate the correct way to address these vulnerabilities. The software also resets itself to its initial settings following a session, allowing users to try various things without worrying about destroying their installation.

This document contains the manual of how to use SecureED. The rest of the document is ordered as follows: Chapter 1 describes the system requirements. Chapter 2 contains an explanation of how to start the program. Chapter 3 describes how to utilize asymmetric encryption. Chapter 4 includes instructions for Professors to enter grades. Chapter 5 includes instructions for Students to search for and enroll in courses. Chapter 6 includes instructions for admins to add, search and edit non-admin user accounts. Chapter 7 provides user credentials.

This document describes functionality of SecureED. v. 2.0, dated 23 April 2022.

# TABLE OF CONTENTS


1 Requirements ..... 1
1.1 System Requirements ..... 1
2 Getting Started ..... 2
2.1 Installation ..... 2
2.2 Start-up ..... 2
2.3 Log In ..... 6
2.4 Forgot Password ..... 7
2.5 Log Out ..... 10
2.6 Closing the Program ..... 11
3 Asymmetric Encryption ..... 12
3.1 Importing the certificate ..... 12
3.2 Deleting the certificate ..... 14
3.3 Creating your own self-signed certificate ..... 16
4 Faculty ..... 18
4.1 Dashboard ..... 18
4.2 Enter Grades ..... 18
4.2.1 Description ..... 18
4.2.2 CSV Format ..... 18
4.2.3 Instructions ..... 19
5 Students ..... 20
5.1 Dashboard ..... 20
5.2 Course Search ..... 20
5.2.1 Description ..... 20
5.2.2 Instructions ..... 20
5.3 Course Enroll ..... 22
5.3.1 Description ..... 22
5.3.2 Instructions ..... 22
6 Administrators ..... 24
6.1 Dashboard ..... 24
6.2 Create Account ..... 24
6.2.1 Description ..... 24
6.2.2 Instructions ..... 24

6.3 User Search ..... 26
6.3.1 Description ..... 26
6.3.2 Instructions ..... 26
6.4 Edit Account ..... 28
6.4.1 Description ..... 28
6.4.2 Instructions ..... 28
7 User Credentials ..... 30

# 1 REQUIREMENTS

## 1.1 SYSTEM REQUIREMENTS

SecureED. is written in HTML, CSS, Javascript, and PHP, and was built and tested on Google Chrome v100 – thus, Chrome is the recommended browser. Otherwise, all libraries are included in the installation folder. Screen resolutions above 1920x1080, and aspect ratios greater than 16:9, are untested, and thus unsupported.

# 2 GETTING STARTED

## 2.1 INSTALLATION

Unzip the file to the folder of your choice. All of the necessary libraries and certificates are included – no setup is required.

## 2.2 START-UP

SecureED. is portable, thus self-contained. To start the webserver, please do the following:

1. Navigate to the root folder of your installation.
2. Execute startup.bat, located in the SecureEd-master folder.

Figure 2.1 Startup

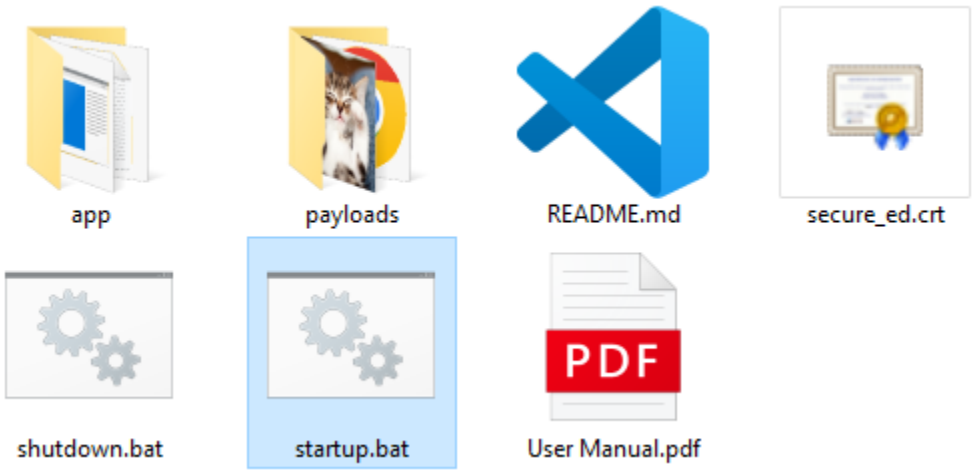
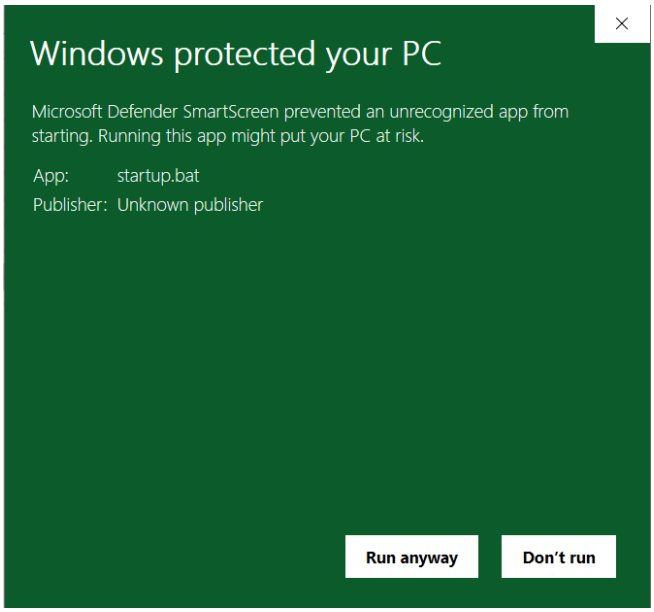


Figure 2.2 Windows Defender Run anyway




The first time you run startup.bat, Windows Defender may warn you that the app is unrecognized and may put your PC at risk. To proceed, click Run anway.

Figure 2.3 Prompt to shut down the server

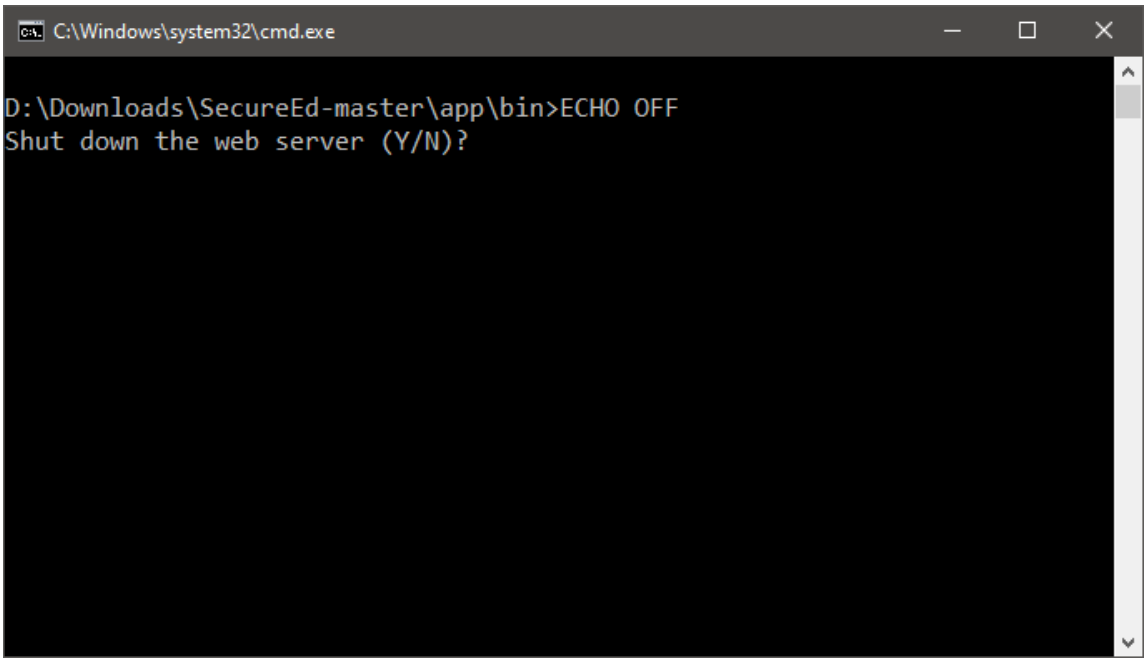
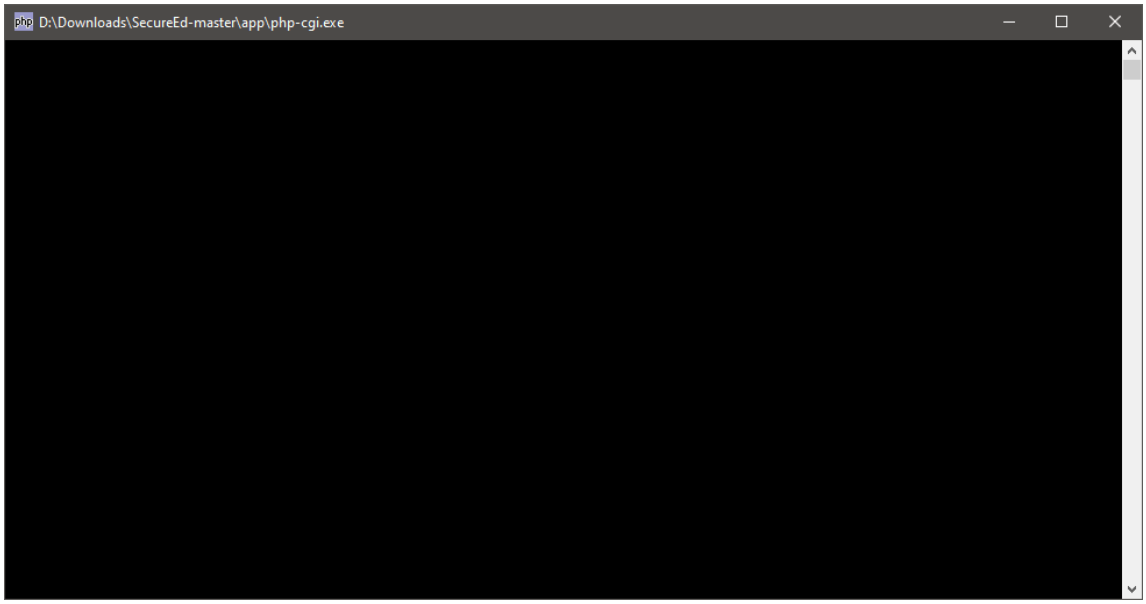
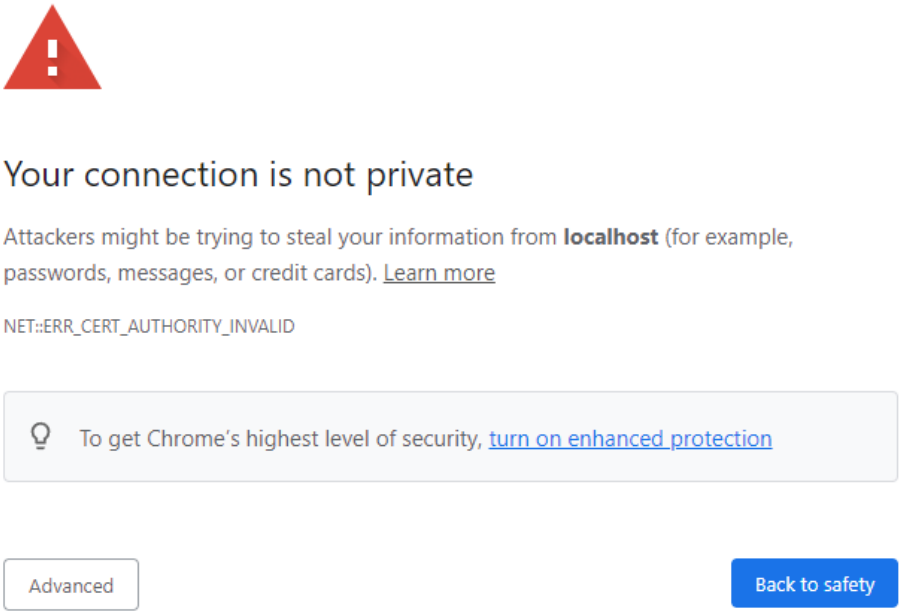



Figure 2.4 Common Gateway Interface executable

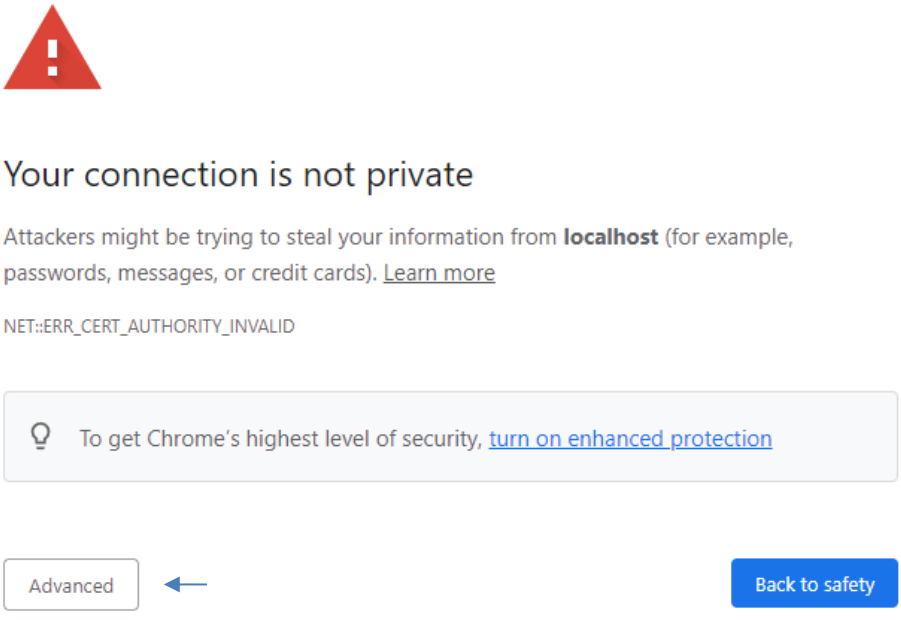



Your default browser will be opened, and you will be presented with a login screen. Note that a command prompt and an executable will open in the background – **DO NOT CLOSE THESE** until you want to end your session! After shutting down the server**,** your session will be terminated, and all data will be reset to their default values when the application is restarted.

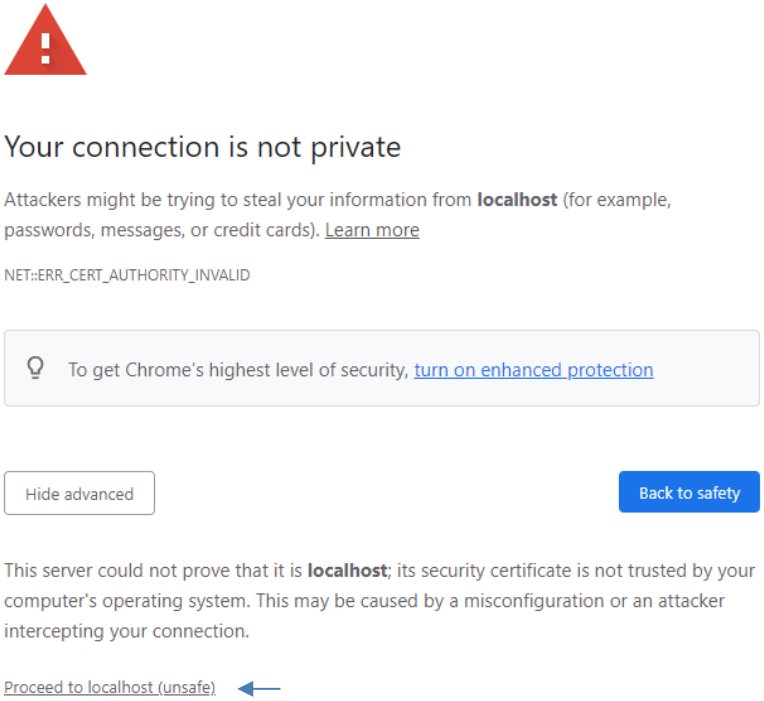
When the page opens your browser may display a page similar to this:



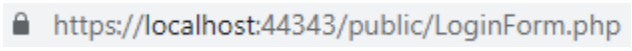

In order to resolve this, you may either import SecureED's certificate in your root store (see section 3.1) or you may ignore this warning by selecting "Advanced":



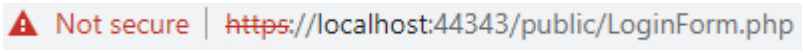
And selecting “Proceed to localhost (unsafe)”:




If you have followed the instructions from section 3.1, your browser should have opened the Log In page, and the address bar should look like this:




Otherwise, your browser will continue to warn you that the site is “not secure”:




## 2.3 Log In

Enter a username and password into the spaces provided, and then press “Submit”.

Figure 2.5 Login Form

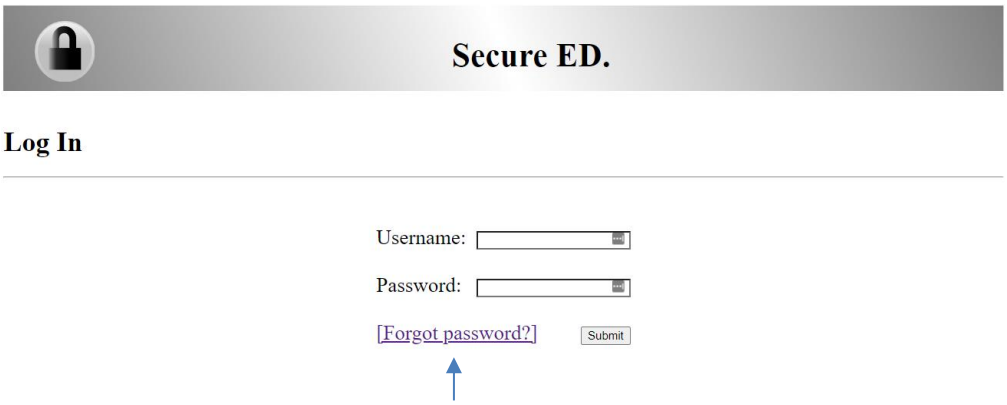
*Note: If you have forgotten your credentials, please select "Forgot password?". See the next section for information regarding how to recover your password.*

## 2.4 FORGOT PASSWORD

In order to recover a lost password:

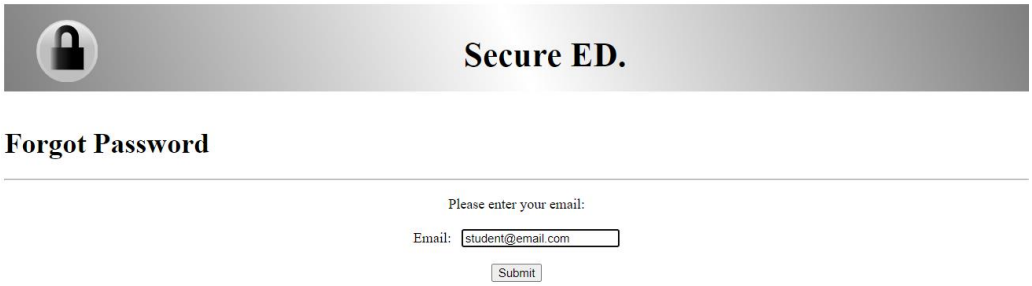
1. Click "Forgot Password?" on the Log In page.

Figure 2.6 Link to Forgot Password on Log In page



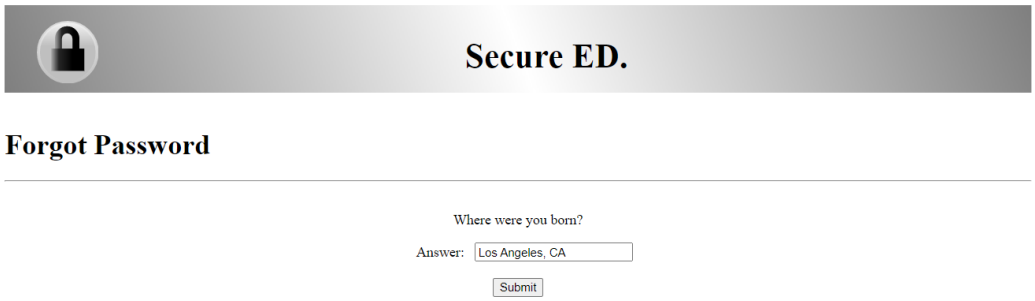

2. On the next page, please enter your email in the provided field, and select "Submit".

Figure 2.7 Forgot Password page




3. You will then be asked the security question associated with that account.

Figure 2.8 Forgot Password security question




4. Enter the correct answer, and you will be taken to a page that will allow you to change your password. Your new password must be between 8 and 20 characters and contain at least one capital letter, one lowercase letter, one number, and one of the following specials symbols: ! @ # $ % ^ & *

Figure 2.8 Forgot Password password change

*Note: Be sure that the contents of the New Password and the Confirm Password fields match!*

## 2.5 LOG OUT

After you have successfully logged in, you may log out at any time. To do so, click on the “Log Out” button on the top pane of any page.

Figure 2.9 Logout

## 2.6 CLOSING THE PROGRAM

When you are ready to end your session, exit your browser and shut down the web server by entering 'Y' in the command prompt or running shutdown.bat (found in the same folder as startup.bat). The program will reset itself to its default values the next time you run startup.

Figure 2.10 Prompt to shut down the server

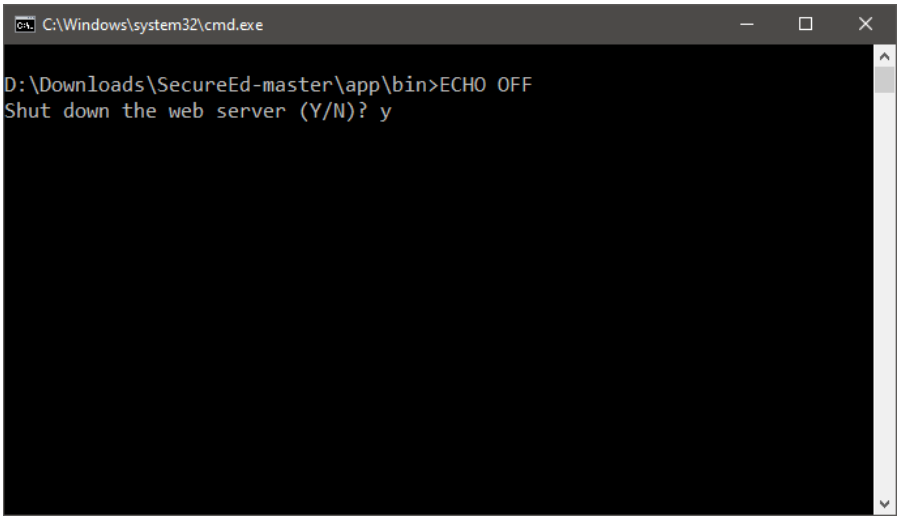
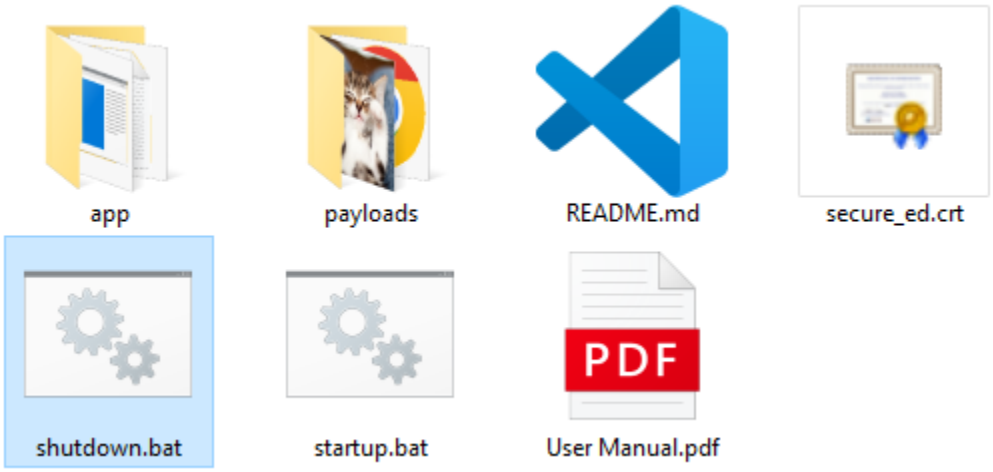



Figure 2.11 Shutdown




*Note: If you shut down the web server from the command prompt, the executable php-cgi.exe will continue to run, and can now be closed manually.*

# 3 ASYMMETRIC ENCRYPTION

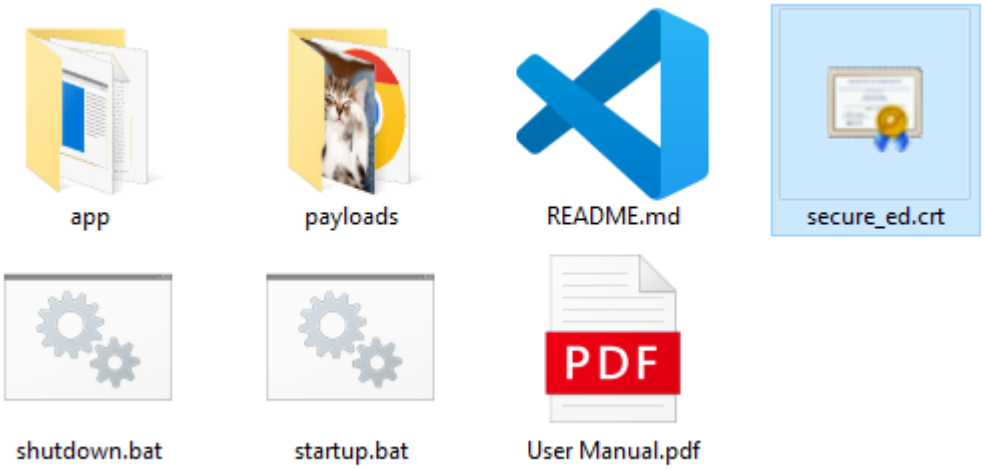
## 3.1 IMPORTING THE CERTIFICATE

SecureED utilizes asymmetric encryption (also known as public-key cryptography) to secure network traffic between the client and the server. SecureED provides both the private key and the public key (also known as a certificate) to do this.

By default, your operating system will not trust SecureED's certificate, and it must be imported into your Trusted Root Certification Authorities store. To import the certificate, please do the following:

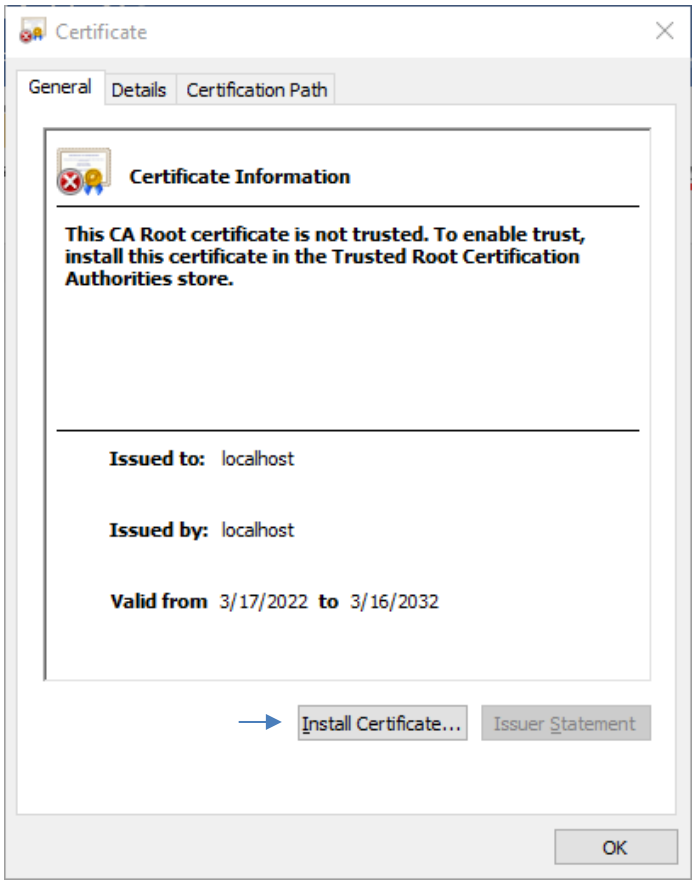
1. Double-click the certificate, located in the SecureEd-master folder.

Figure 3.1 SecureED Certificate



2. Select “Install Certificate…”

Figure 3.2 Selecting Install Certificate




3. Follow the instructions in the Certificate Import Wizard
    a. Select “Current user”. Click next.
    b. Select “Place all certificates in the following store” Click “Browse”.
    c. Select “Trusted Root Certification Authorities”. Click “OK”. Click “Next”
    d. Click “Finish”.
    e. If you are prompted with a security warning, click “yes”
    f. Click “yes”.

If you were directed to this section from section 2.1, please restart your browser (In Chrome, do this by typing chrome://restart in the address bar). Alternatively, shut down the server (see section 2.6) and restart the application (see section 2.2).

*Note: After 3/16/2032, SecureED’s certificate will have expired and your browser will warn you that the site is “not secure” because of this!*

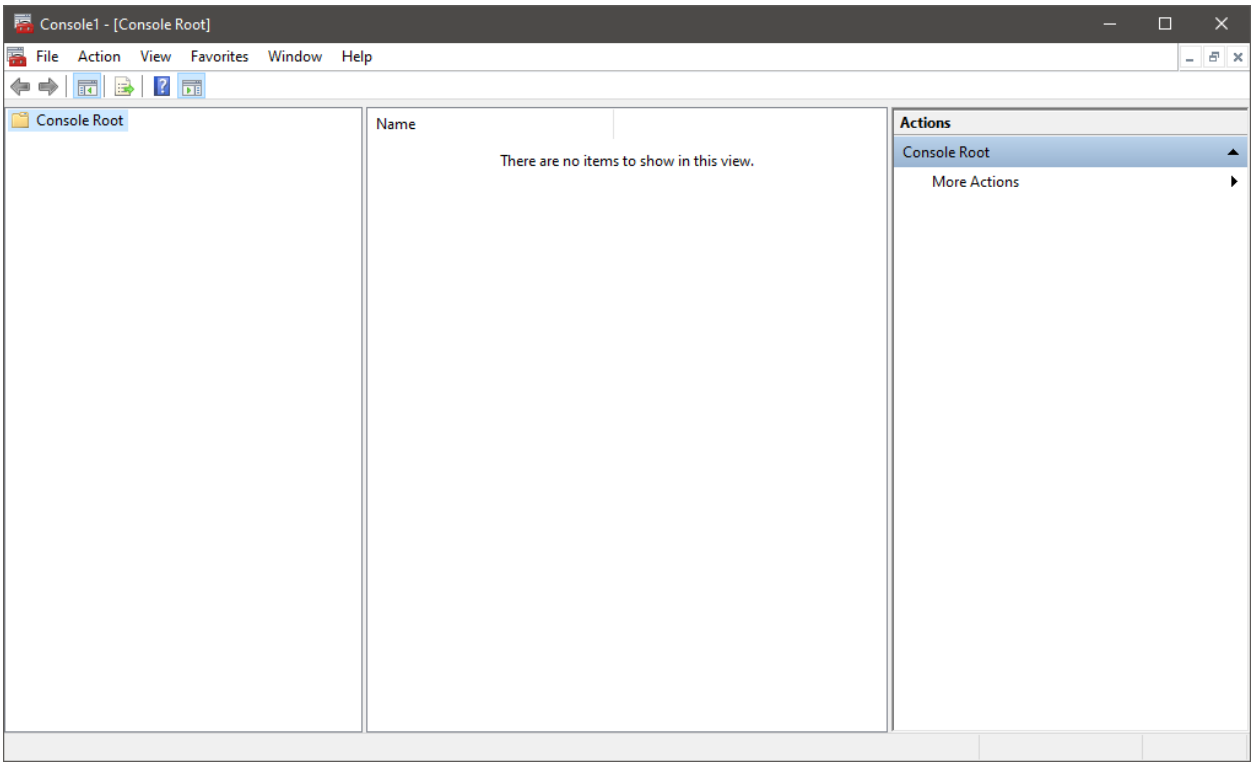
## 3.2 DELETING THE CERTIFICATE

When you are done using SecureED, you may want to delete its certificate from your operating system. To delete the certificate:

1. Click the ‘search’ button on your taskbar.
2. Type ‘mmc’
3. Run the program ‘Microsoft Management Console’

You should see a program that looks like this:

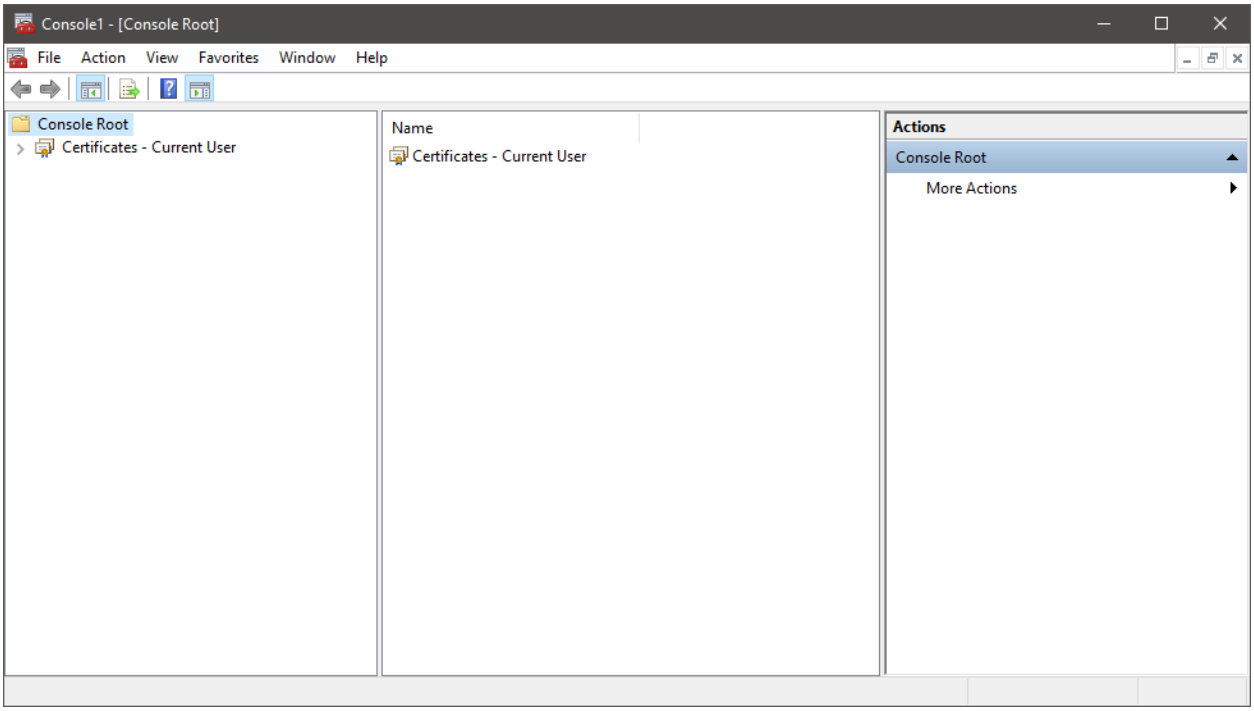
Figure 3.3 Microsoft Management Console




4. In the console, click ‘File’, then ‘Add/Remove Snap-in…’.
5. In the ‘Available snap-ins’, select ‘certificates’.
6. Click ‘Add’.
7. Select ‘My user account’. (If you imported SecureED’s certificate under ‘local machine’, select ‘computer account’ instead).
8. Click ‘Finish’.
9. Click ‘OK’.

The console should now look like this:

Figure 3.4 Certificates added to the console




10. Double-click ‘Certificates – Current User’ (or ‘Certificates (Local Computer)’).
11. Double-click ‘Trusted Root Certification Authorities’.
12. Double-click ‘Certificates’.
13. Find SecureED’s certificate.

It should look like this:

14. Right-click and delete SecureED’s certificate.
15. Click ‘yes’.
16. Click ‘yes’.

**DO NOT DELETE OTHER SYSTEM CERTIFICATES.** These are other certificates that you operating system trusts.

SecureED’s certificate can be identified by its Thumbprint (sha1):

1fd2df58f4563b5b5ba3b59a967bb37f23edef7d

If the certificate has this value as its thumbprint, then it is safe to delete.

*Note: After you delete the certificate, your browser will begin to warn you that the site is "not secure".*

## 3.3 CREATING YOUR OWN SELF-SIGNED CERTIFICATE

When creating a website, you may want to create your own self-signed certificate. These types of certificates are useful in development environments and internal networks because they are easy to make and cost no money to create.

To create a self-signed certificate, you will need to use a program. Here, we will use a popular program for creating certificates called OpenSSL

OpenSSL can be downloaded here:

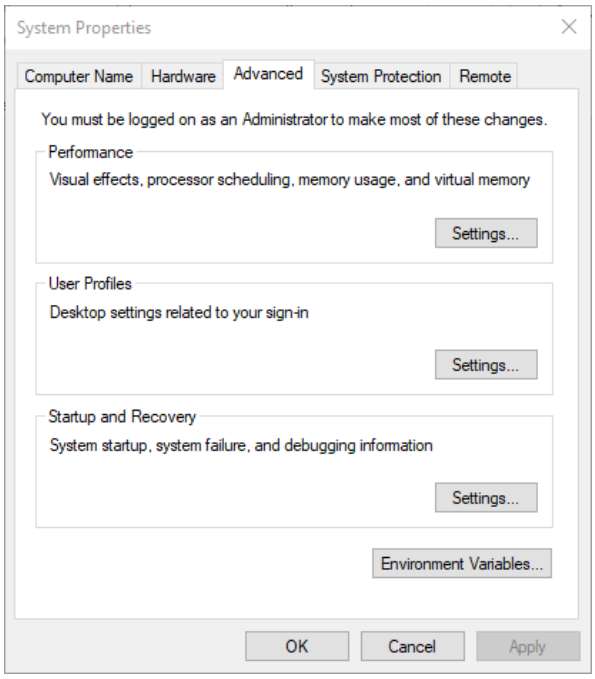
https://slproweb.com/products/Win32OpenSSL.html

Once OpenSSL is installed you will want to add it to the Windows environment variables.

1. Click 'search' on the taskbar.
2. Type 'environment variables'.
3. Click 'Edit the system environment variables' in control panel.

You should see the control panel

Figure 3.5 Environment Variables




4. Click ‘Environment variables’.
5. Under ‘System variables’, double-click ‘Path’.
6. Click ‘New’.
7. Add the path to openssl.exe that you just installed.
8. Click ‘OK’ and close the control panel.

You should now have an installation of OpenSSL that you can use in cmd.

1. Click ‘search’ on the taskbar.
2. Type ‘cmd’.
3. Run the Windows Command Prompt.
4. Enter the command:

    openssl version

To see if you have a valid installation of OpenSSL .

5. You can now use OpenSSL commands to create your own self-signed certificates. SecureED’s self-signed certificate was created with the following commands:

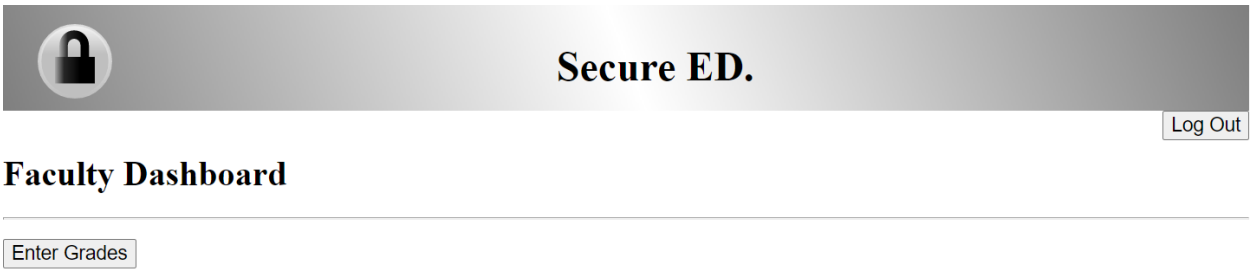
    openssl req -newkey rsa:2048 -nodes -keyout secure_ed.key -out secure_ed.csr

    openssl x509 -signkey secure_ed.key -in secure_ed.csr -req -days 3652 -extfile v3.ext -out secure_ed.crt -days 3652

# 4 FACULTY

## 4.1 DASHBOARD

Figure 4.1 Faculty Dashboard




## 4.2 ENTER GRADES

### 4.2.1 DESCRIPTION

The Enter Grades functionality allows a faculty member to add final grades to a course, using a .csv (comma-separated values) file.

### 4.2.2 CSV FORMAT

Uploaded files must be comma separated text values, in the following format:

USER_ID,GRADE
USER_ID,GRADE
USER_ID,GRADE
…

e.g.:

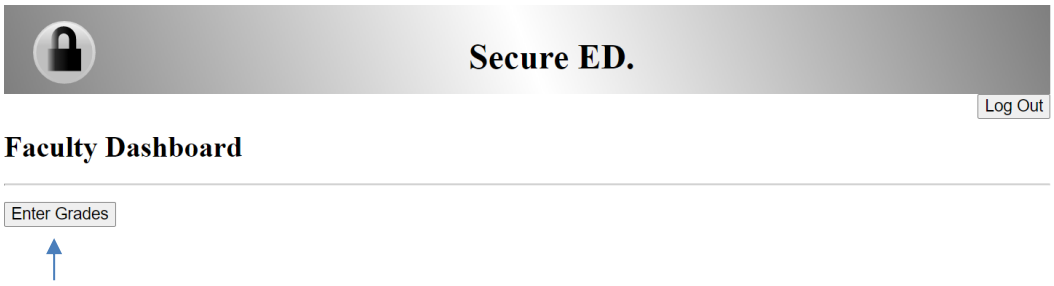
927066652,A
927190481,F
927201552,C
927237023,B
927369978,D
927410321,F
927512079,A
927535222,A
927565074,B
927600214,C
927620146,A

927671464,F
927694539,C
927790514,B

### 4.2.3 INSTRUCTIONS

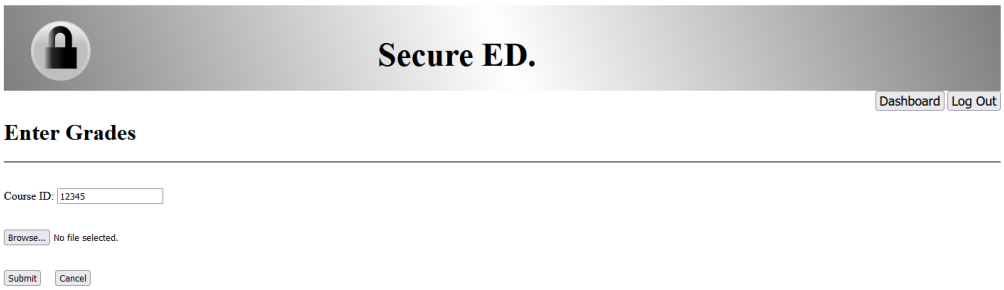
1. From the Dashboard, select “Enter Grades”.

Figure 4.2 Enter Grades selection




2. On the following page, enter the Course ID (CRN).

Figure 4.3 Enter Grades page

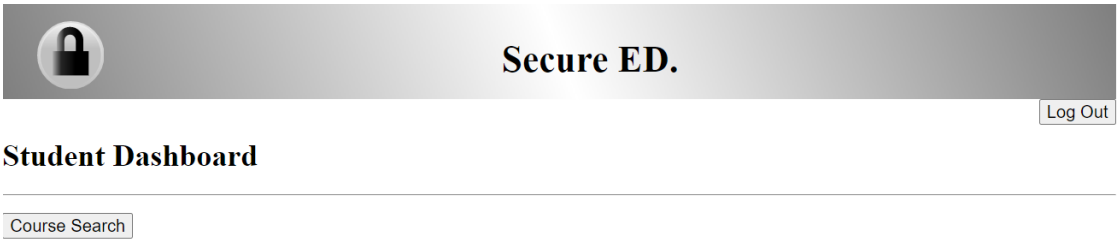



3. Select “Browse”.
4. Select a .csv file from your computer (see 3.2.2 for correct formatting).
5. Select submit to upload the file.

# 5 STUDENTS

## 5.1 DASHBOARD

Figure 5.1 Student Dashboard




## 5.2 COURSE SEARCH

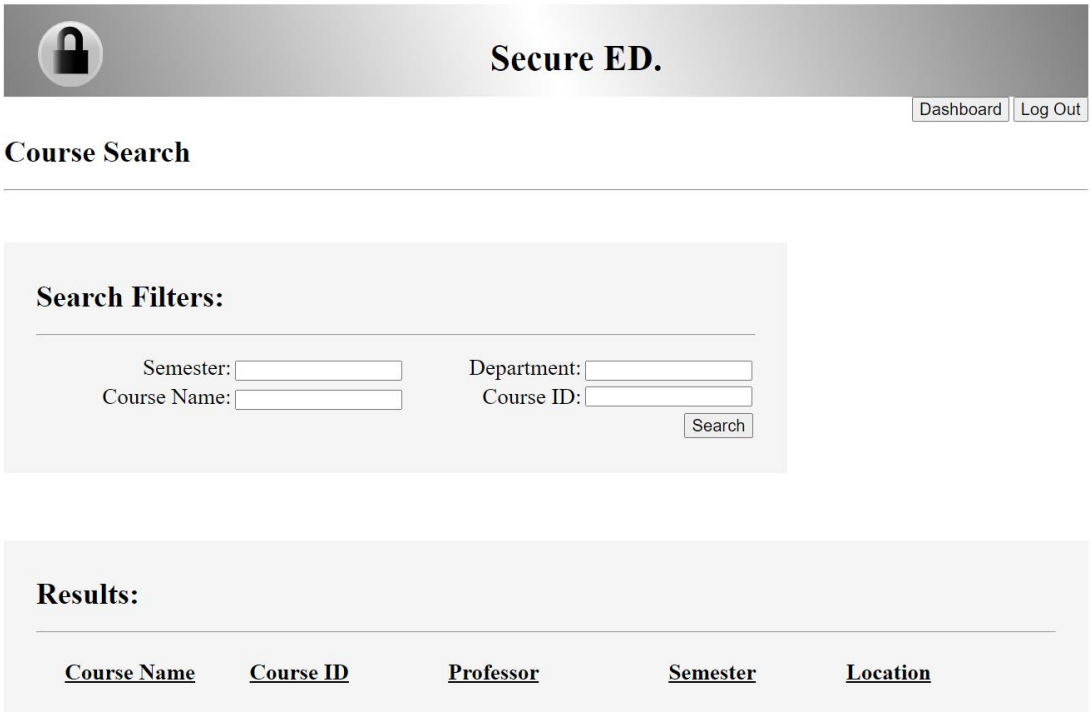
### 5.2.1 DESCRIPTION

Course search allows students to find current, past and future courses.

### 5.2.2 INSTRUCTIONS

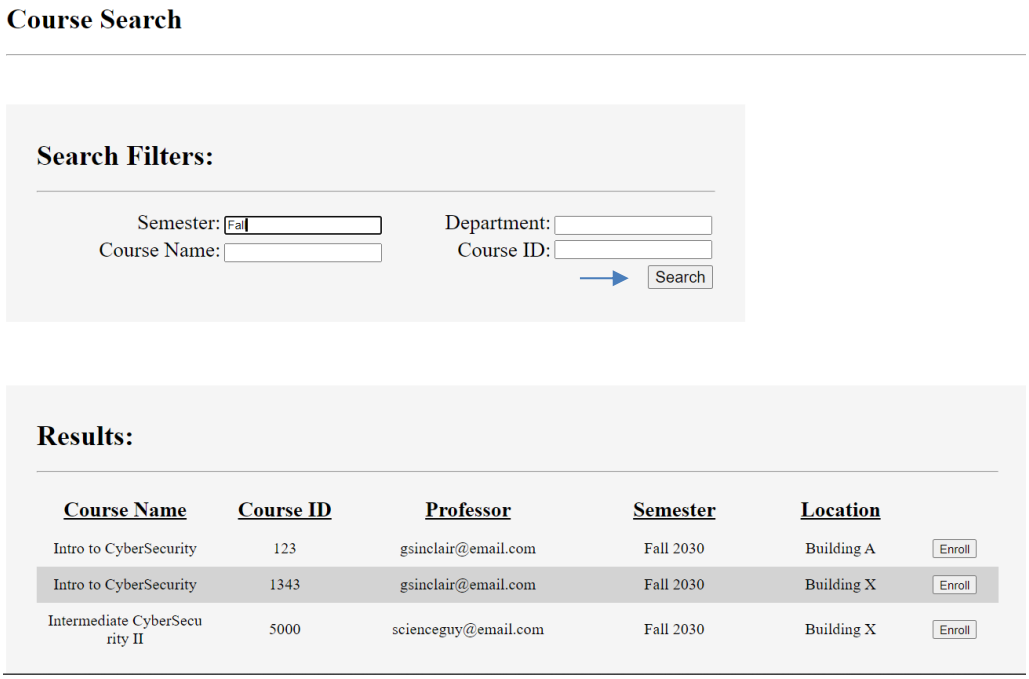
1. From the Dashboard, select “Course Search”.
2. On the following page, enter information relevant to the course you may be interested in.

Figure 5.2 Course Search page



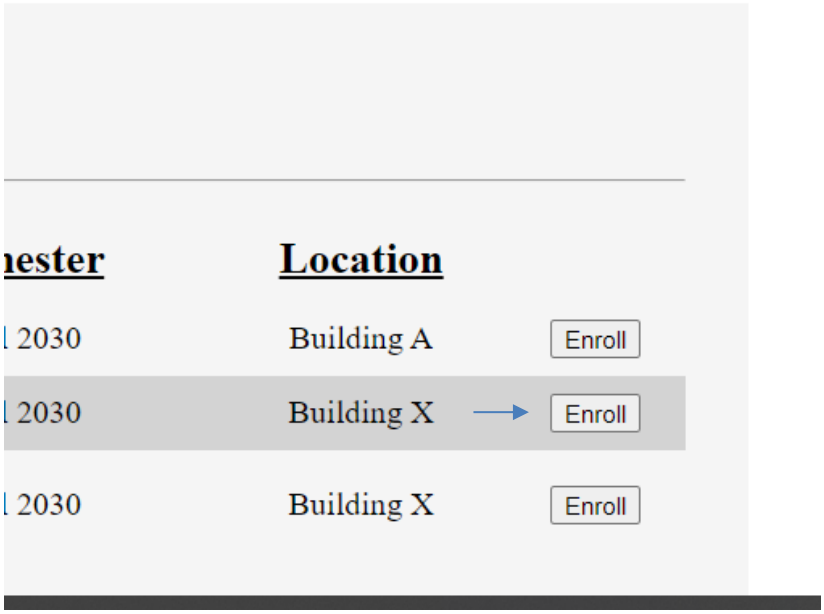
3. Select search.

Figure 5.3 Filtering and searching for courses



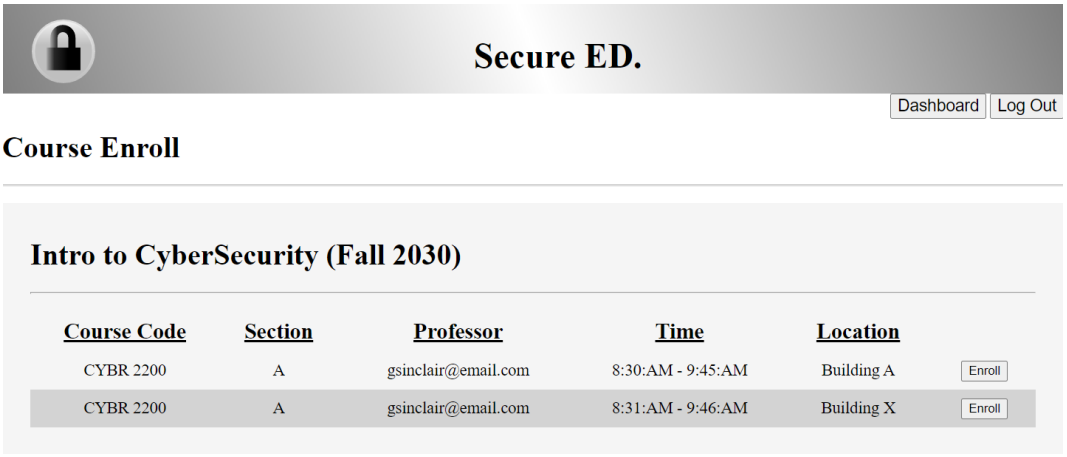

4. For a list of sections, select enroll.

Figure 5.4 Selecting a course to enroll in



5. You will be presented with a list of sections to browse.

Figure 5.5 Enrolling in a section of a course




*Note: If you don't wish to enroll at this time, you can always select "Dashboard" to return to your landing page without enrolling in a class!*

## 5.3 COURSE ENROLL

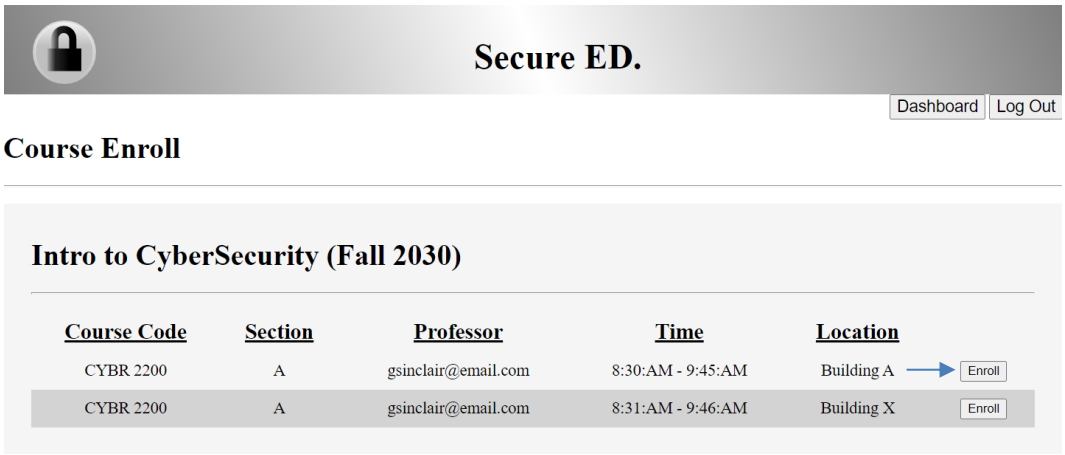
### 5.3.1 DESCRIPTION

After finding a course using Course Search, a student can enroll in a section of the course.

### 5.3.2 INSTRUCTIONS

1. Find a course per the instructions in 4.2.2.
2. Select "Enroll" to bring up a list of sections.
3. Select "Enroll" next to the section you wish to enroll in.

Figure 5.6 Course enroll

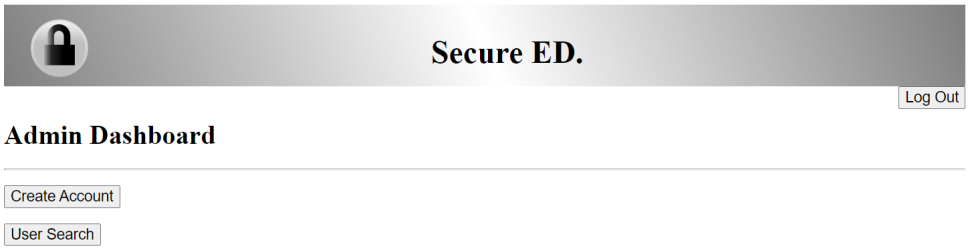



You will automatically be returned to your dashboard.

# 6 ADMINISTRATORS

## 6.1 DASHBOARD

Figure 6.1 Admin Dashboard




## 6.2 CREATE ACCOUNT

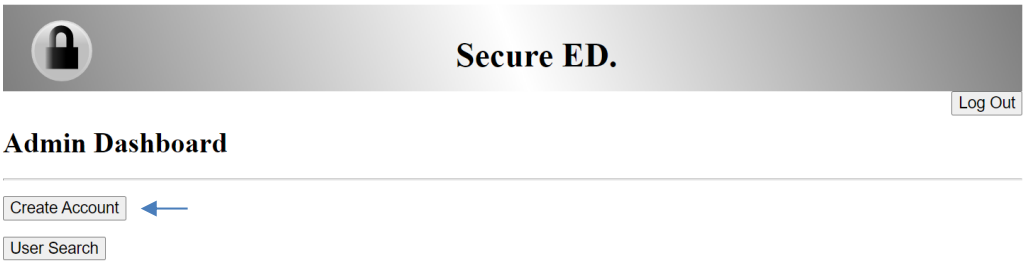
### 6.2.1 DESCRIPTION

Allows the administrator account to create new accounts for new users. This is the only way to create a new account!

### 6.2.2 INSTRUCTIONS

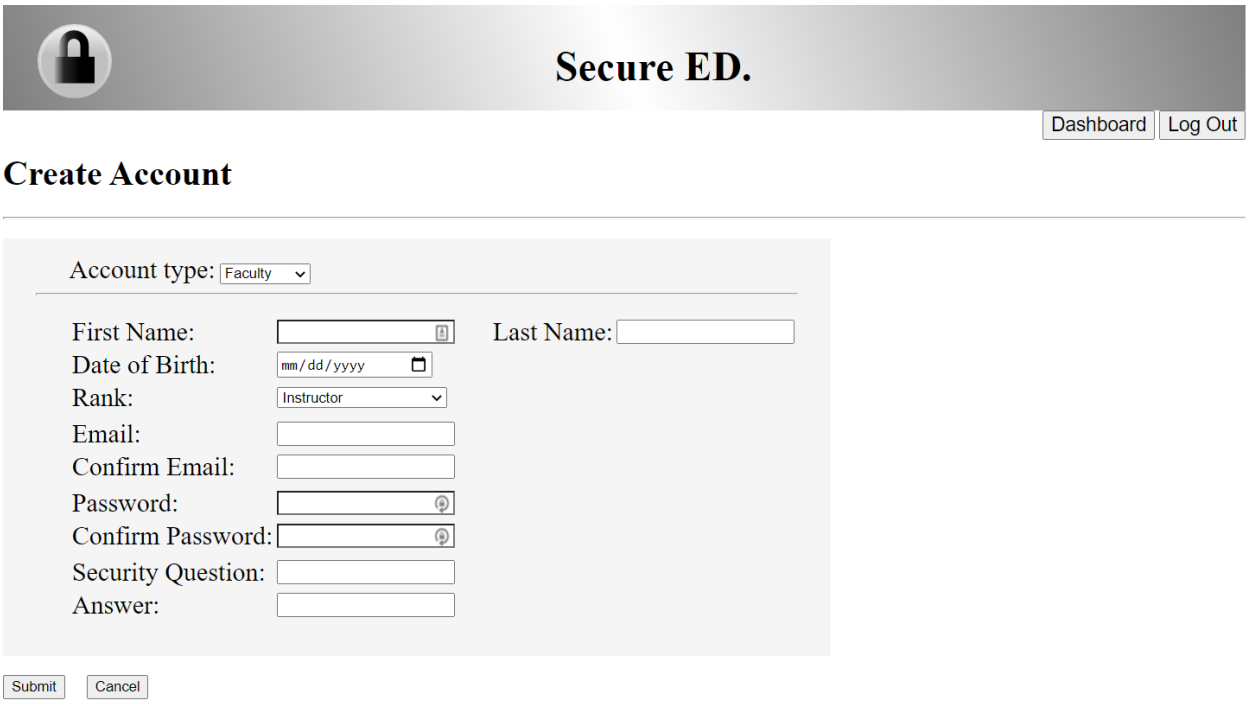
1. From the Dashboard, select “Create Account”.

Figure 6.2 Create Account selection



2. On the following page, select the account type.
*Note: Admin accounts cannot be created!*

Figure 6.3 Create Account page




3. Enter the user's:
- First and Last Name
- Date of Birth
- Rank (faculty) or Year (students)
- Email
- Password
- Security Question
- Answer (to Security Question)

4. Confirm the user's e-mail and password, and re-enter them in their respective confirmation fields.

5. Select "Submit".

## 6.3 USER SEARCH

### 6.3.1 DESCRIPTION

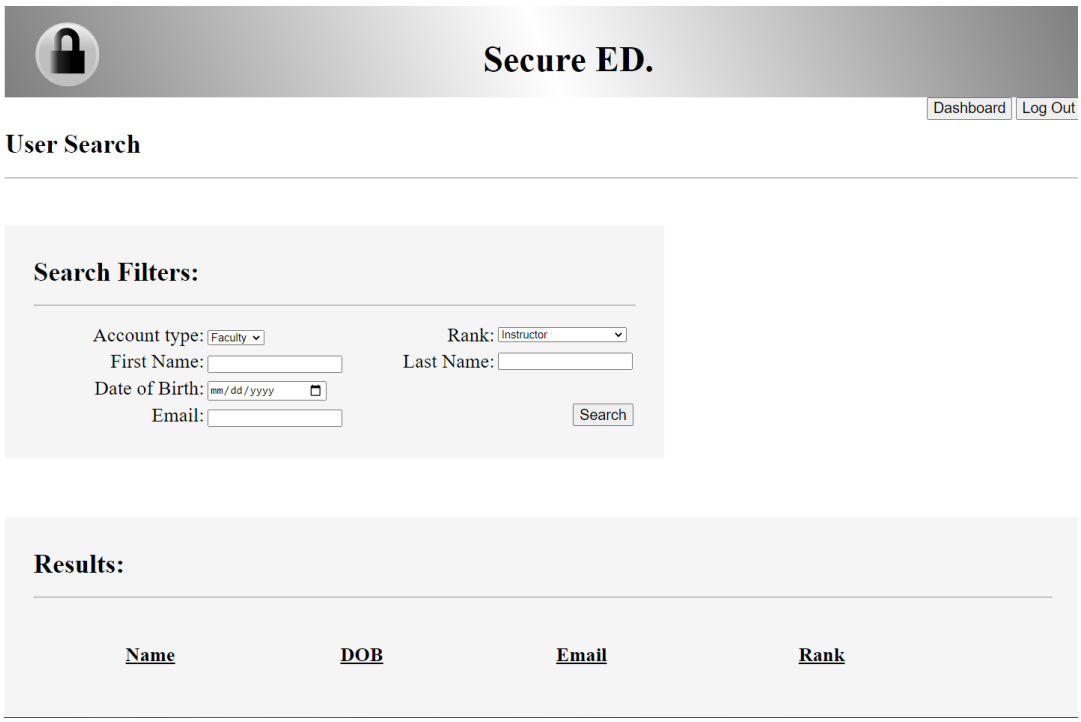
Allows administrators to search for users using filters.

### 6.3.2 INSTRUCTIONS

1. From the Dashboard, select “User Search”.

2. Select an account type, and a Rank (faculty) or Year (students).
   *Note: These two fields are mandatory!*

Figure 6.4 User Search page




3. Enter any more relevant information into the fields provided.

4. Select “Search”.

Figure 6.5 Filter and search for users

A list of matching accounts will appear below.

## 6.4 EDIT ACCOUNT

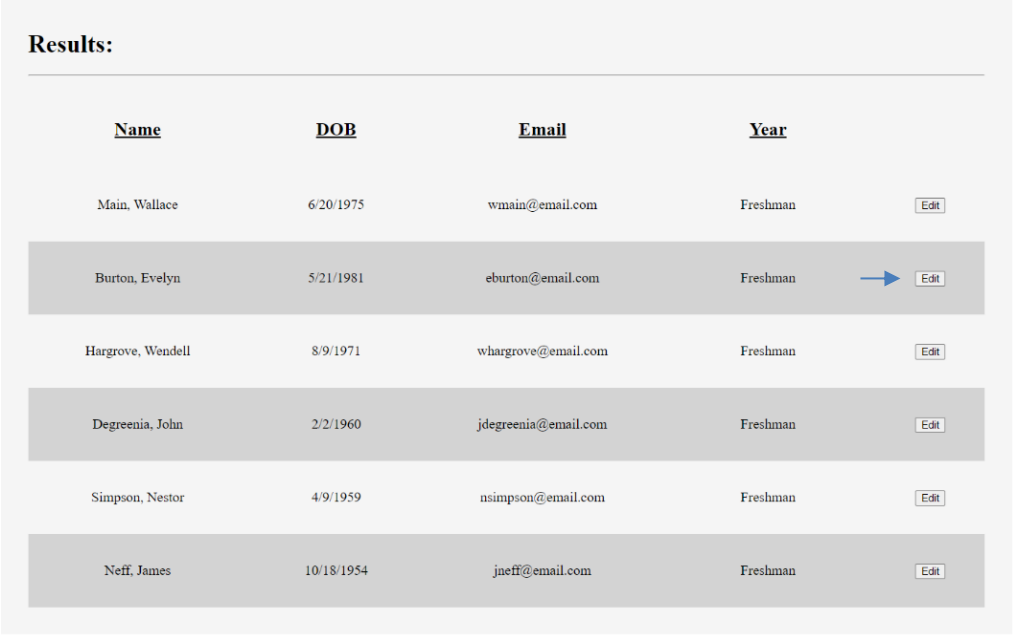
### 6.4.1 DESCRIPTION

Allows an administrator to edit a non-administrator account.

### 6.4.2 INSTRUCTIONS

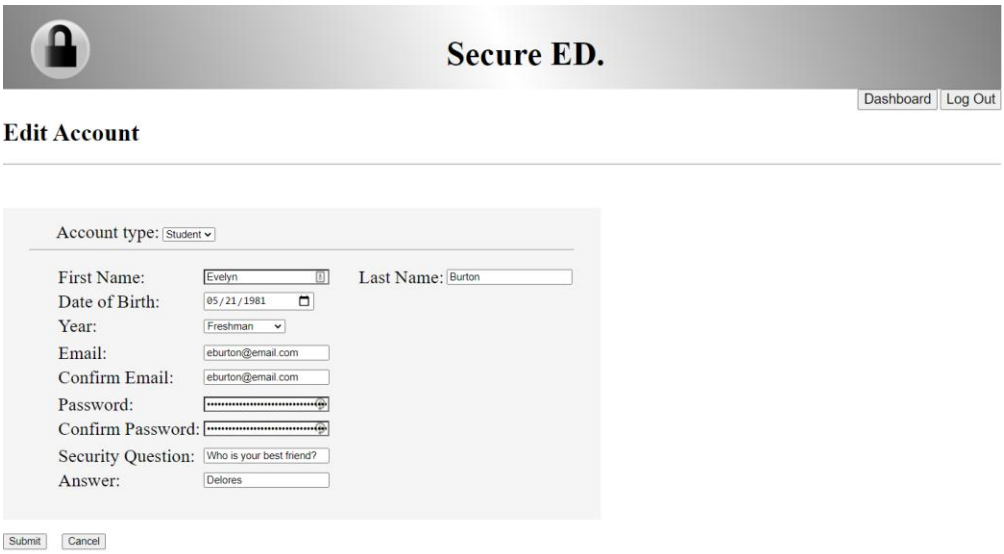
1. Find a user per the instructions in 5.3.2.
2. Select “Edit” to the right of the user’s information.

Figure 6.6 Edit Account selection




3. Make any desired changes to the prepopulated data in the fields provided.

Figure 6.7 Entering information for a new account




*Note: Don't forget to confirm any changes to the e-mail or password!*

4. Select "Submit".

# 7 USER CREDENTIALS

Figure 7.1 User Credentials

| Account Type | Username | Password | Security Question | Security Answer |
|---|---|---|---|---|
| Faculty | scienceguy@email.com | Password2! | Favorite Relative? | Charity Nye |
| Student | student@email.com | Password5! | Where were you born? | Los Angeles, CA |
| Admin | admin@email.com | Password1! | How many siblings do you have? | 0 |