

Cahindi, Joseph Francis R.	November 11, 2025
CBS 401A-IT31S3 - Network Security Final Project	Mr. San Juan

## Web Security

### **Secure Web Application Development (SECURE TASK MANAGER)**

#### **System Features**

##### **User Registration**

- Allows new users to sign up with a username, email, and password.
- Validates input fields and prevents invalid or duplicate data.
- Passwords are securely stored using hashing.
- Displays appropriate error messages for invalid or missing input.

##### **User Login**

- Authenticates registered users using username/email and password.
- Prevents unauthorized access to the dashboard.
- Includes error handling for incorrect credentials.

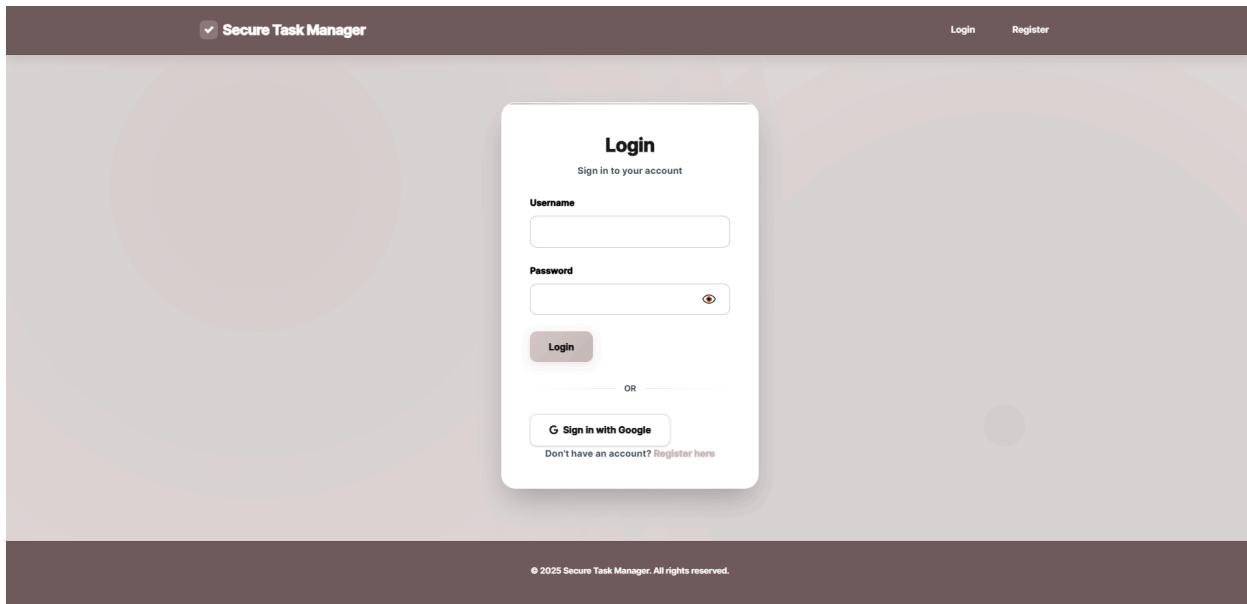
##### **Dashboard (Task Management)**

- Displays a personalized dashboard for each user.
- Enables users to create, view, update, and delete their own tasks.
- Ensures that users cannot access or modify other users' data.

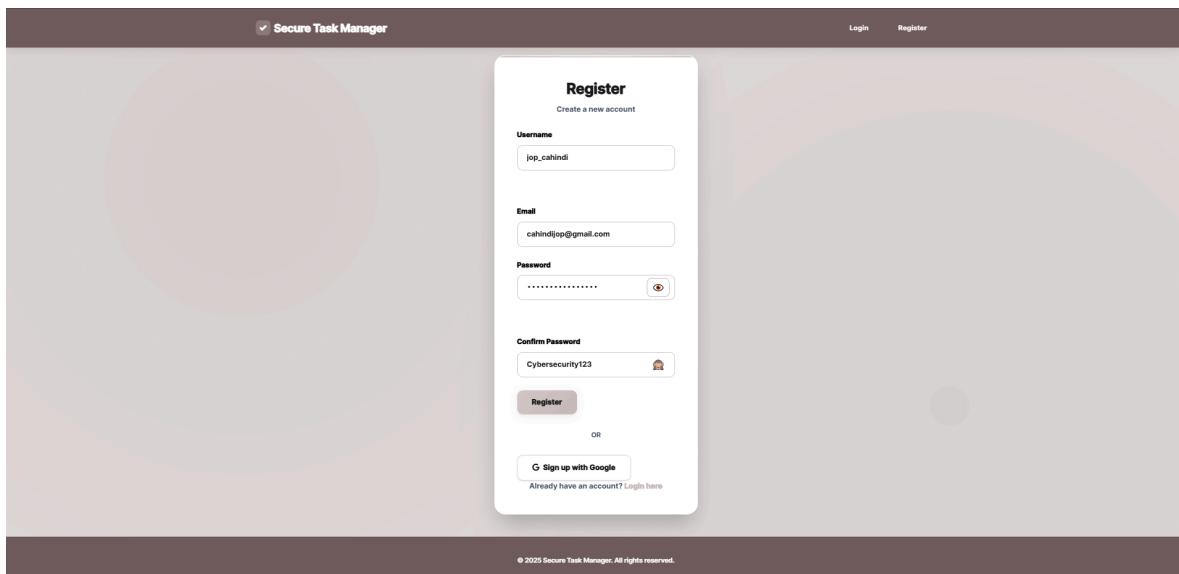
##### **Google OAuth Login**

- Provides a “Sign in with Google” feature for faster, secure authentication.
- Retrieves the user's first name and email from their Google account.
- Creates a new user account if they log in with Google for the first time.

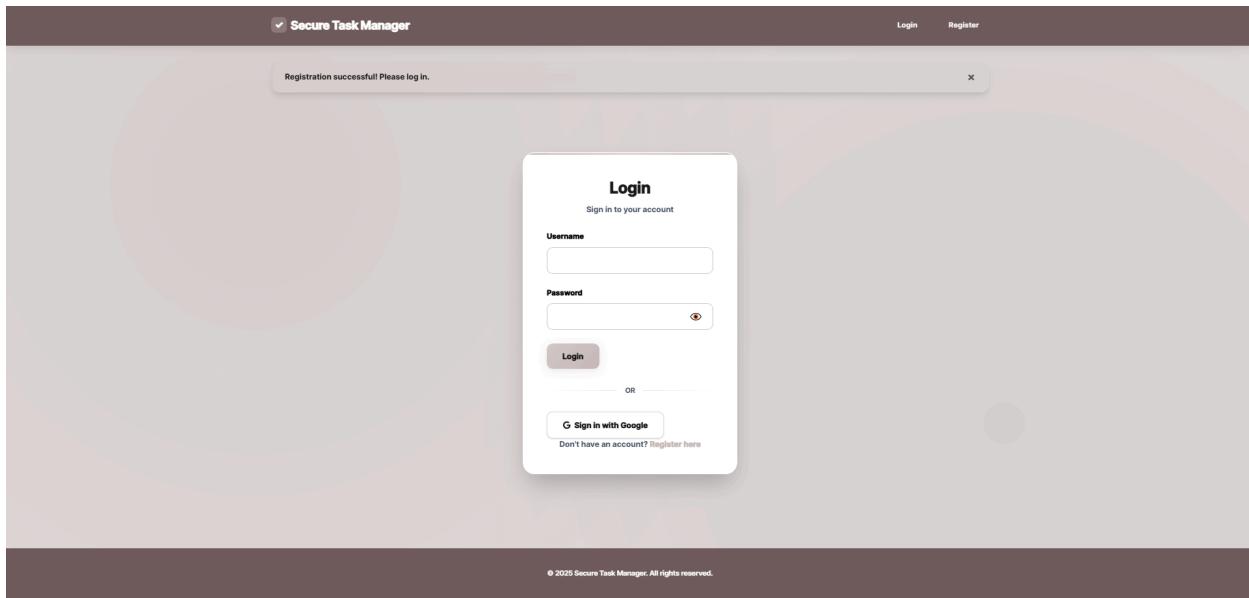
## LOGIN PAGE



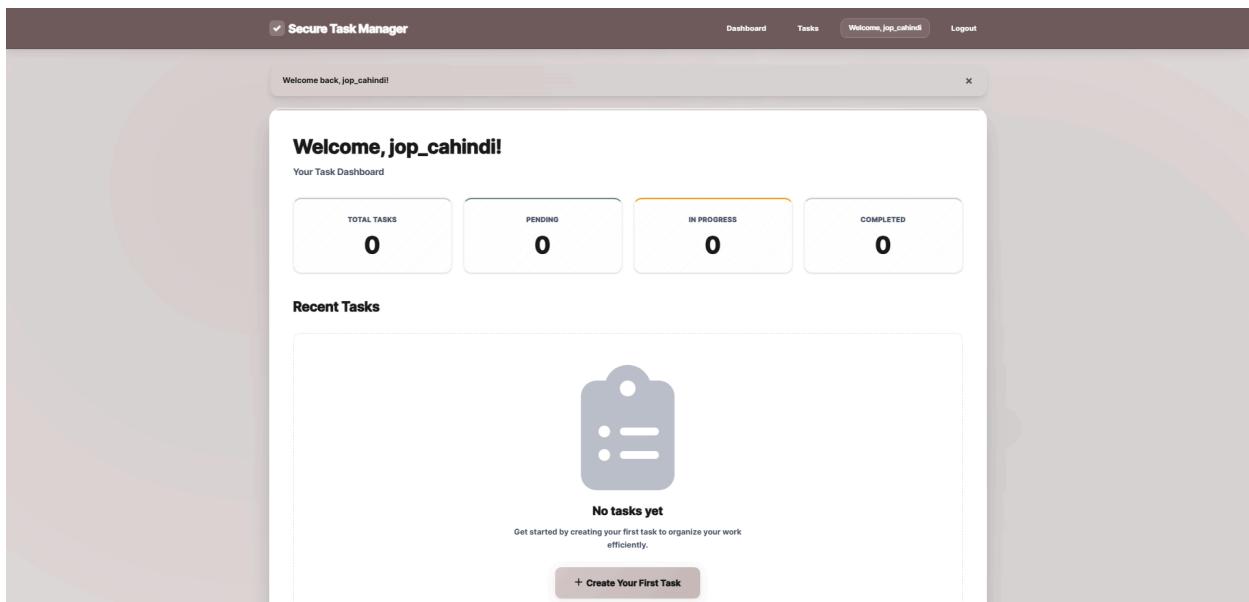
## REGISTRATION PAGE



## LOGING IN



## DASHBOARD



## CREATING A TASKS

The screenshot shows the 'Task Management' section of a web application. At the top left is the title 'Task Management'. Below it is a form titled 'Create New Task'. The form fields are: 'Task Title' (input field containing 'FINAL PROJECT PRESENTATION'), 'Description' (input field containing 'CBS FINAL PROJECT ,ADVANCE DATABASE PROJECT'), and 'Status' (dropdown menu showing 'Pending'). At the bottom of the form is a dark grey button labeled '+ Create Task'.

## TASKS CREATED

The screenshot shows the 'Your Task Dashboard' page. At the top center is the greeting 'Welcome, jop\_cahindi!'. Below it is a summary card with four boxes: 'TOTAL TASKS' (1), 'PENDING' (1), 'IN PROGRESS' (0), and 'COMPLETED' (0). Underneath is a section titled 'Recent Tasks' featuring a card for the task 'FINAL PROJECT PRESENTATION' (Status: PENDING). The card includes the description 'CBS FINAL PROJECT ,ADVANCE DATABASE PROJECT', the creation date '2025-11-11 09:15', and two buttons: '✓ Complete' and '↻ View Details'. At the bottom of this section is a dark grey button labeled '☰ Manage Tasks'.

## USERS CAN EDIT HIS/HER TASKS

The screenshot shows a user interface for a task management application. At the top, there is a dark header bar with the title "Secure Task Manager". Below the header, there are navigation links for "Dashboard", "Tasks", "Welcome, jop\_cahindi", and "Logout". A large, semi-transparent circular watermark is visible in the background.

The main content area is titled "Your Tasks". It contains a form for editing a task:

- Task Title:** FINAL PROJECT PRESENTATION
- Description:** CBS FINAL PROJECT ,ADVANCE DATABASE PROJECT
- Status:** A dropdown menu showing the following options:
  - Pending
  - Pending (selected)
  - In Progress
  - Completed
  - Cancelled

At the bottom of the page, there is a footer bar with the text "© 2025 Secure Task Manager. All rights reserved."

- Enables users to create, view, update, and delete their own tasks.
- Ensures that users cannot access or modify other users' data.

# **Network Security**

## **Network Security Audit and Penetration Testing**

### **Secure Web Application Development (SECURE TASK MANAGER)**

#### **Security Features**

##### **Input Validation**

- Ensures that all input fields meet required formats and constraints.
- Prevents entry of malicious data, special characters, or script tags.

##### **Session Management**

- Uses secure sessions to track logged-in users.
- Regenerates session IDs after login to prevent session fixation.
- Automatically expires sessions after inactivity.

##### **Secure Storage**

- Stores passwords using password\_hash() instead of plain text.
- Uses parameterized queries to prevent SQL injection.
- Ensures that sensitive data (like session tokens) are never exposed.

##### **SQL Injection Protection**

- All database queries use prepared statements.
- Tests confirm that injection attempts fail and do not leak data.

##### **CSRF Protection**

- Each form includes a CSRF token stored in the session.
- Requests without valid tokens are rejected.
- Demonstrates successful prevention of CSRF attacks.

##### **Error Handling**

- Handles invalid inputs gracefully with friendly messages.
- Prevents exposure of server or database error details to users.
- Logs errors internally for debugging without revealing system information.

## REGISTRATION TESTING INVALID USERNAME

The image displays two side-by-side screenshots of a registration form titled "Register". Both screenshots show the same fields: Username, Email, Password, and Confirm Password. The "Username" field is highlighted in both cases.

**Screenshot 1 (Left):** The "Username" field contains "user@#%". A validation message box appears below it stating: "Please match the requested format. Username must be 3-20 alphanumeric characters or underscores".

**Screenshot 2 (Right):** The "Username" field contains "'1'=1'". A validation message box appears below it stating: "Please match the requested format. Username must be 3-20 alphanumeric characters or underscores".

Both screenshots also show a "Register" button and a "G Sign up with Google" button at the bottom.

## REGISTRATION TESTING INVALID EMAILS

The image displays three screenshots illustrating invalid email validation. The central screenshot shows a modal dialog from "Secure Task Manager" with the error message "Invalid email format".

**Screenshot 1 (Left):** The "Email" field contains "test..test@example.com". A validation message box at the bottom of the page states: "Invalid email format".

**Screenshot 2 (Middle):** The "Email" field contains "Cahindi1234". A validation message box at the bottom of the page states: "Invalid email format".

**Screenshot 3 (Right):** The "Email" field is empty. A validation message box at the bottom of the page states: "Invalid email format".

All three screenshots show the same registration form fields: Username, Email, Password, Confirm Password, and a "Register" button.

## REGISTRATION TESTING INVALID PASSWORDS

The image displays three screenshots of a registration form. The first screenshot shows a modal dialog from the browser with the message "127.0.0.1:5000 says Password must contain at least one uppercase letter!" and an "OK" button. The second screenshot shows the registration page with the "Password" field containing "aaaaa". A yellow warning bubble says "Please lengthen this text to 8 characters or more (you are currently using 5 characters)". The third screenshot shows the registration page with the "Password" field containing "Aaaa". A yellow warning bubble says "Please lengthen this text to 8 characters or more (you are currently using 4 characters)". Both screenshots show the "Confirm Password" field below it.

127.0.0.1:5000 says  
Password must contain at least one uppercase letter!

OK

**Register**  
Create a new account

Username  
joseph\_cahindi

Email  
josephreynosocahindi@gmail.com

Password  
aaaaa

Confirm Password  
aaaaaaa

OR

G Sign up with Google

Already have an account? [Login here](#)

**Register**

Create a new account

Username  
joseph\_cahindi

Email  
josephreynosocahindi@gmail.com

Password  
aaaaa

Confirm Password  
aaaaaaa

OR

G Sign up with Google

Already have an account? [Login here](#)

**Register**

Create a new account

Username  
joseph\_cahindi

Email  
josephreynosocahindi@gmail.com

Password  
Aaaa

Confirm Password  
Aaaa

OR

G Sign up with Google

Already have an account? [Login here](#)

## REGISTRATION TESTING CONFIRM PASSWORDS

The image displays two screenshots of a registration form. Both screenshots show the "Confirm Password" field containing "6789password" and the "Password" field containing "12345password". A yellow warning bubble under the "Confirm Password" field says "Passwords do not match". Both screenshots show the "Password" field containing "Password1234" and the "Confirm Password" field containing "Password567". A yellow warning bubble under the "Confirm Password" field says "Passwords do not match". Both screenshots show the "Register" button at the bottom.

**Register**  
Create a new account

Username  
joseph\_cahindi

Email  
josephreynosocahindi@gmail.com

Password  
12345password

Confirm Password  
6789password

OR

G Sign up with Google

Already have an account? [Login here](#)

**Register**

Create a new account

Username  
joseph\_cahindi

Email  
josephreynosocahindi@gmail.com

Password  
Password1234

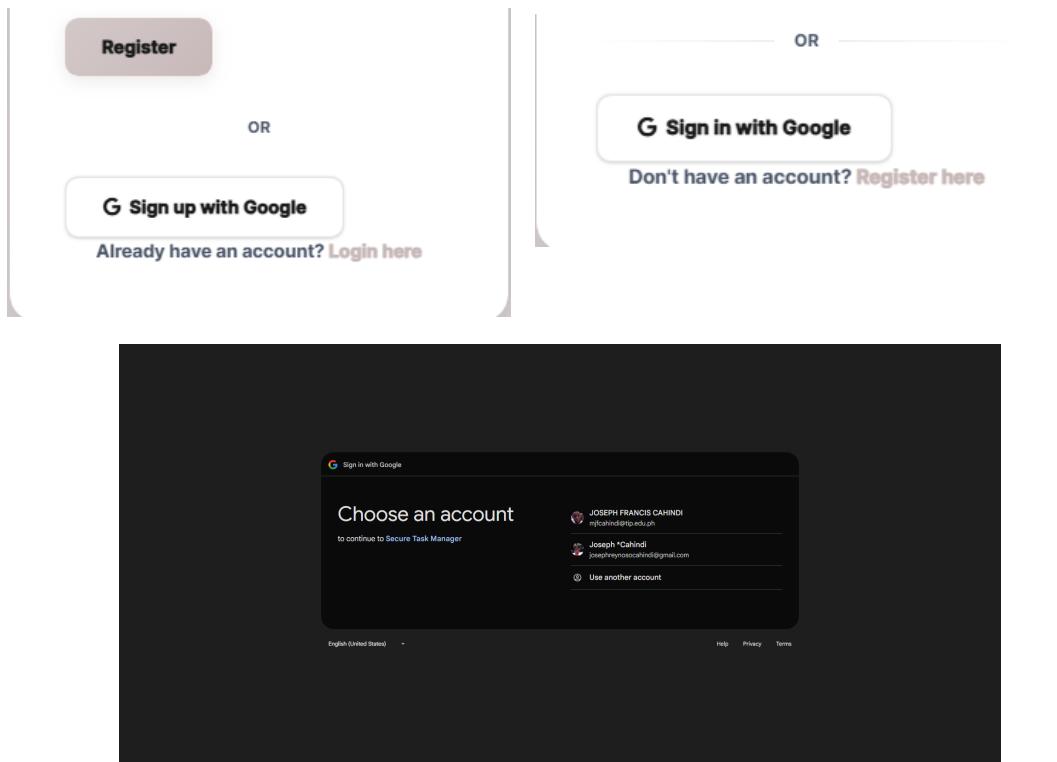
Confirm Password  
Password567

OR

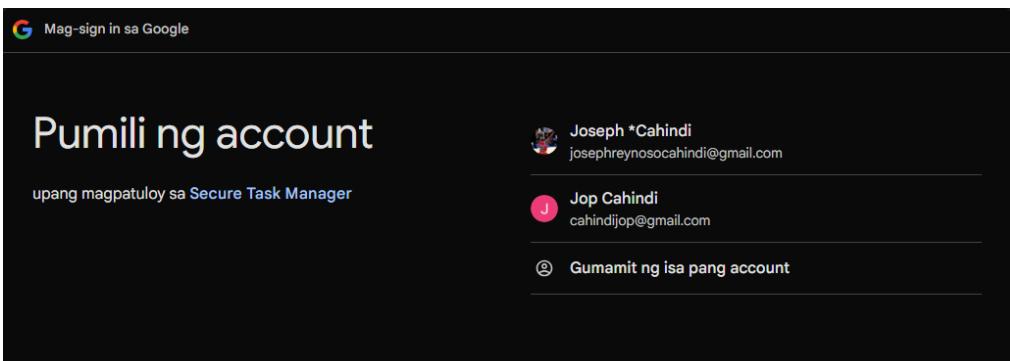
G Sign up with Google

Already have an account? [Login here](#)

## GOOGLE OAUTH REGISTRATION



**GOOGLE OAUTH REGISTRATION ([cahindijop@gmail.com](mailto:cahindijop@gmail.com)) : website will get your first name in you personal gmail account.**



A screenshot of a task manager application dashboard. The top navigation bar includes 'Secure Task Manager', 'Dashboard', 'Tasks', 'Welcome, jop!', and 'Logout'. A welcome message 'Welcome, jop!' is displayed above the main content area. The main area is titled 'Your Task Dashboard' and contains four cards showing 'TOTAL TASKS' (0), 'PENDING' (0), 'IN PROGRESS' (0), and 'COMPLETED' (0). Below this is a section titled 'Recent Tasks' which is currently empty, showing a placeholder icon of a tag with a list.

## TESTING INVALID CREDENTIALS

(login with non-existent username → Should show error)

(login with wrong password → Should show error)

(login with empty username → Should show error)

(login with empty password → Should show error)

The image displays two side-by-side screenshots of a mobile-style login application. Both screens feature a header 'Login' and a sub-header 'Sign in to your account'. The left screen shows a successful login flow: the 'Username' field contains 'Sanjuan\_Joselito', the 'Password' field contains 'Sanjuan123', and the 'Login' button is visible. Below the form are links for Google sign-in and account registration. The right screen shows an error state: the 'Username' field is empty, and the 'Password' field contains 'Sanjuan123'. A prominent red error bar at the top states 'Invalid username or password.' The 'Login' button is disabled in this state.

The image displays two side-by-side screenshots of a mobile-style login application. Both screens feature a header 'Login' and a sub-header 'Sign in to your account'. The left screen shows a validation error for the 'Username' field: it is empty, and a red callout bubble indicates 'Please fill out this field.' The 'Password' field contains 'Sanjuan1234' and is functional. The right screen shows a validation error for the 'Password' field: it is empty, and a red callout bubble indicates 'Please fill out this field.' The 'Username' field contains 'Sanjuan\_Joselito' and is functional. Below both forms are links for Google sign-in and account registration.

## SECURITY TESTING <script>alert<'XSS'></script>

### Your Tasks

The image shows a task card within a 'Your Tasks' section. The card has a header 'Security Testing' and a status indicator 'IN PROGRESS'. The main content area contains the payload '<script>alert('XSS')</script>'. At the bottom, there are creation and update timestamps: 'Created: 2025-11-11 11:30' and 'Updated: 2025-11-11 11:30'. At the very bottom are three buttons: 'Mark Complete' (grey), 'Edit' (blue), and 'Delete' (red).

## Task Management

### Create New Task

Task Title

Description

```
<script>alert('XSS')</script>
```

Status

+ Create Task

## SQL INJECTION PROTECTION

### Register

Create a new account

Username

! Please match the requested format.

Username must be 3-20 alphanumeric characters or underscores

Email

Password



Confirm Password



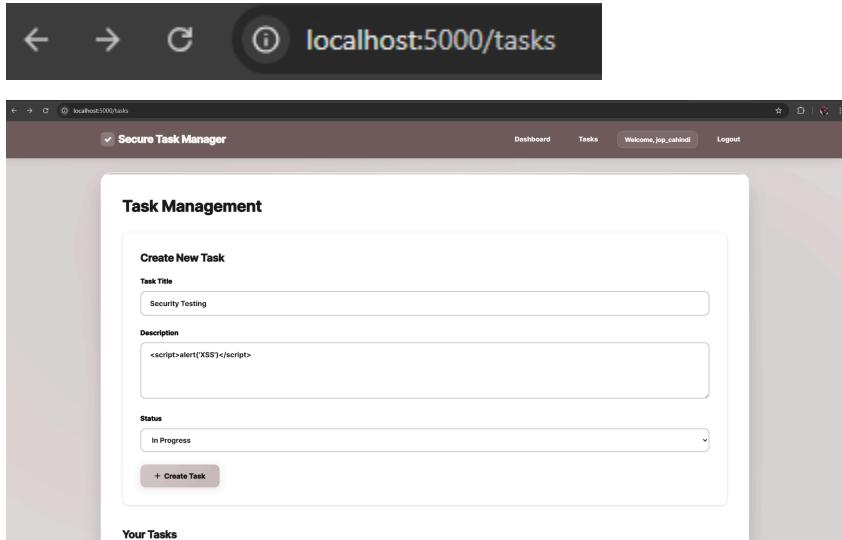
Register

OR

G Sign up with Google

Already have an account? [Login here](#)

## ERROR HANDLING



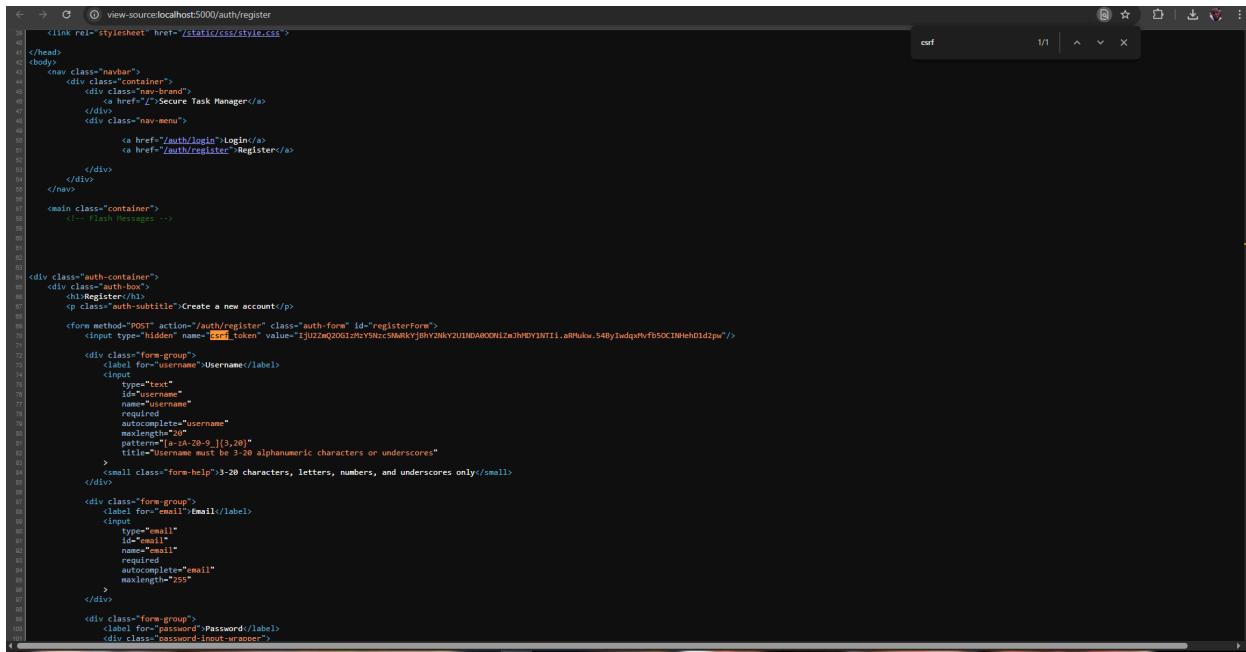
The screenshot shows a web browser window with the URL `localhost:5000/tasks` in the address bar. The page title is "Secure Task Manager". The main content is a "Task Management" form. The "Task Title" field contains "Security Testing". The "Description" field contains the XSS payload `<script>alert('XSS')</script>`. The "Status" dropdown is set to "In Progress". Below the form is a button labeled "+ Create Task". At the bottom of the page, there is a section titled "Your Tasks".



The screenshot shows a web browser window with the URL `localhost:5000/note` in the address bar. The page title is "Not Found". The main content is a message: "The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again." There are browser navigation buttons at the top.

## CSRRF PROTECTION

```
<input type="hidden" name="csrf_token" value="IjU2ZmQ20GIzMzY5Nzc5NWlkYjBhY2NkY2U1NDA0ODNiZmJhMDY1NTIi.aRMukw.54ByIwdqxMvfb5OCINHehD1d2pw"/>
```

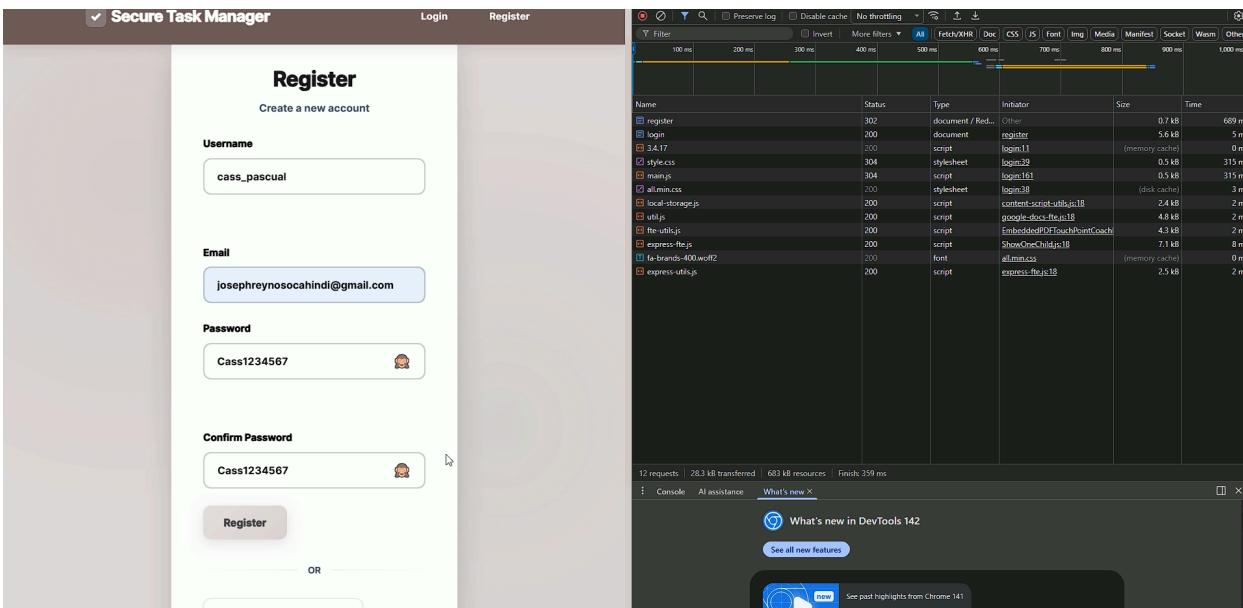


```

<link rel="stylesheet" href="/static/css/style.css">
</head>
<body>
  <nav class="navbar">
    <div class="container">
      <div class="nav-brand">
        <a href="#">Secure Task ManagerLogin</a>
        <a href="/auth/register">Register</a>
      </div>
    </div>
  </nav>
  <main class="container">
    <!-- Flash Messages -->
    <br>
    <div class="with-container">
      <div class="auth-box">
        <h3>Register</h3>
        <p>Create a new account</p>
        <form method="POST" action="/auth/register" class="auth-form" id="registerForm">
          <input type="hidden" name="_csrf_token" value="1JUZmQ20G1gHYSNzC9MrkyJ8HY2NKY2U1H0A00N1zJmHDYINT1i.oHMuKw.S4ByIwdqdvfb50CINehD1d2pw"/>
          <div class="form-group">
            <label for="username">Username</label>
            <input type="text"
                   id="username"
                   name="username"
                   required="true"
                   autocomplete="username"
                   maxlength="20"
                   pattern="[\w-]{3-20}[^_]{3-20}"
                   title="Username must be 3-20 alphanumeric characters or underscores" />
            <small>3-20 characters, letters, numbers, and underscores only</small>
          </div>
          <div class="form-group">
            <label for="email">Email</label>
            <input type="email"
                   id="email"
                   name="email"
                   required="true"
                   autocomplete="email"
                   maxlength="255" />
          </div>
          <div class="form-group">
            <label for="password">Password</label>
            <input type="password" />
          </div>
        </form>
      </div>
    </div>
  </main>
</body>

```

## CSRF TOKEN WORKING



The screenshot shows a "Secure Task Manager" application with a "Register" page open. The page has fields for "Username" (cass\_pascual), "Email" (josephreynosacahindi@gmail.com), and "Password" (Cass1234567). Below the form is a "Register" button. To the right, the Chrome DevTools Network tab is visible, displaying a list of resources loaded by the page. The resources include the main document, CSS files like style.css and all.min.css, and various JavaScript files such as login.js, register.js, and express.js.

Name	Status	Type	Initiator	Size	Time
register	302	document / Red...	Other	0.7 kB	689 ms
login	200	document	register	5.6 kB	5 ms
3.4.17	200	script	login:11	(memory cache)	0 ms
style.css	304	stylesheet	login:39	0.5 kB	315 ms
main.js	304	script	login:161	0.5 kB	315 ms
all.min.css	200	stylesheet	login:38	(disk cache)	3 ms
local-storage.js	200	script	content-script-utils:18	2.4 kB	2 ms
util.js	200	script	google-docs-fte:18	4.8 kB	2 ms
fte-util.js	200	script	EmbeddedPDFTouchPointCoach	4.3 kB	2 ms
express-fbe.js	200	script	ShowOneChild:18	7.1 kB	8 ms
fe-brands-400.woff2	200	font	all.min.css	(memory cache)	0 ms
express-util.js	200	script	express-fte:18	2.5 kB	2 ms

## **SECURITY AUDIT REPORT (ZAP)**



The screenshot shows a browser window displaying a very long XML document. The XML content is a single, continuous block of code, likely a configuration file for a network device or application. It includes numerous nested tags such as <config>, <include>, <language>, <authentication>, <authorization>, and <context>. The code is written in a standard XML syntax with attributes and values. The browser interface at the top shows the title 'Default Context Context' and the path 'File C:/Users/TITI/Downloads/Default%20Context.context'. The scroll bar on the right indicates the document is much longer than the visible area.

The screenshot shows the ZAP interface. At the top, there's a navigation bar with File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help, and a tab for 'Untitled Session - ZAP 2.16.1'. Below the navigation is a toolbar with icons for Sites, Contexts, Requests, Response, and Requester. The main window has a left sidebar titled 'Contexts' with 'Default Context' selected, and a 'Sites' section below it. The central area displays a 'Welcome to ZAP' banner with the text: 'ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. If you are new to ZAP then it is best to start with one of the options below.' Below the banner is a table of scan results:

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Std Resp. Header	Std Resp. Body
96	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/key.pem	404	NOT FOUND	5 ms	384 bytes	207 bytes
96	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/ssl_crt_1.ssa	404	NOT FOUND	3 ms	384 bytes	207 bytes
97	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/ssl_crt_2.ssa	404	NOT FOUND	2 ms	384 bytes	207 bytes
98	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/sslMd5_rsa	404	NOT FOUND	4 ms	384 bytes	207 bytes
99	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/sslMd5_dsa	404	NOT FOUND	3 ms	384 bytes	207 bytes
100	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/sslMd5_sha	404	NOT FOUND	4 ms	384 bytes	207 bytes
101	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/vbscript.jsp	404	NOT FOUND	7 ms	384 bytes	207 bytes
102	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/CHANGELOG.MD	404	NOT FOUND	5 ms	384 bytes	207 bytes
103	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/redis/available	404	NOT FOUND	4 ms	384 bytes	207 bytes
104	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/composer.json	404	NOT FOUND	4 ms	384 bytes	207 bytes
105	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/zip/test.zip	404	NOT FOUND	7 ms	384 bytes	207 bytes
106	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/xml_settings.xml	404	NOT FOUND	5 ms	384 bytes	207 bytes
107	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/server_info	404	NOT FOUND	8 ms	384 bytes	207 bytes
108	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/phpinfo.php	404	NOT FOUND	4 ms	384 bytes	207 bytes
109	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/laravel.php	404	NOT FOUND	6 ms	384 bytes	207 bytes
110	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/robots.txt	404	NOT FOUND	4 ms	384 bytes	207 bytes
111	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/_webroute/config.json	404	NOT FOUND	4 ms	384 bytes	207 bytes
112	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/_webroute/config.php	404	NOT FOUND	3 ms	384 bytes	207 bytes
113	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/_webroute/worker.boot.json	404	NOT FOUND	3 ms	384 bytes	207 bytes
114	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/_hg	404	NOT FOUND	4 ms	384 bytes	207 bytes
115	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/_tar	404	NOT FOUND	3 ms	384 bytes	207 bytes
116	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/_dcrs	404	NOT FOUND	4 ms	384 bytes	207 bytes
117	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/_Bkkeeper	404	NOT FOUND	3 ms	384 bytes	207 bytes
118	11/11/2025, 8:16:00 pm	11/11/2025, 8:16:00 pm	GET	http://localhost:5000/tasks	200	OK	4 ms	557 bytes	4,600 bytes
120	11/11/2025, 8:16:01 pm	11/11/2025, 8:16:01 pm	GET	http://localhost:5000/tasks	200	OK	4 ms	557 bytes	4,600 bytes
124	11/11/2025, 8:16:01 pm	11/11/2025, 8:16:01 pm	GET	http://localhost:5000/tasks	200	OK	4 ms	557 bytes	4,600 bytes
126	11/11/2025, 8:16:01 pm	11/11/2025, 8:16:01 pm	GET	http://localhost:5000/tasks	200	OK	5 ms	557 bytes	4,600 bytes
128	11/11/2025, 8:16:01 pm	11/11/2025, 8:16:01 pm	GET	http://localhost:5000/tasks	200	OK	4 ms	557 bytes	4,600 bytes
130	11/11/2025, 8:16:01 pm	11/11/2025, 8:16:01 pm	GET	http://localhost:5000/tasks	200	OK	4 ms	557 bytes	4,600 bytes
132	11/11/2025, 8:16:01 pm	11/11/2025, 8:16:01 pm	GET	http://localhost:5000/tasks	200	OK	3 ms	557 bytes	4,600 bytes
134	11/11/2025, 8:16:01 pm	11/11/2025, 8:16:01 pm	GET	http://localhost:5000/tasks	200	OK	5 ms	557 bytes	4,600 bytes
136	11/11/2025, 8:16:01 pm	11/11/2025, 8:16:01 pm	GET	http://localhost:5000/tasks	200	OK	4 ms	557 bytes	4,600 bytes
138	11/11/2025, 8:16:01 pm	11/11/2025, 8:16:01 pm	GET	http://localhost:5000/tasks	200	OK	3 ms	557 bytes	4,600 bytes
140	11/11/2025, 8:16:01 pm	11/11/2025, 8:16:01 pm	GET	http://localhost:5000/tasks	200	OK	5 ms	557 bytes	4,600 bytes