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.

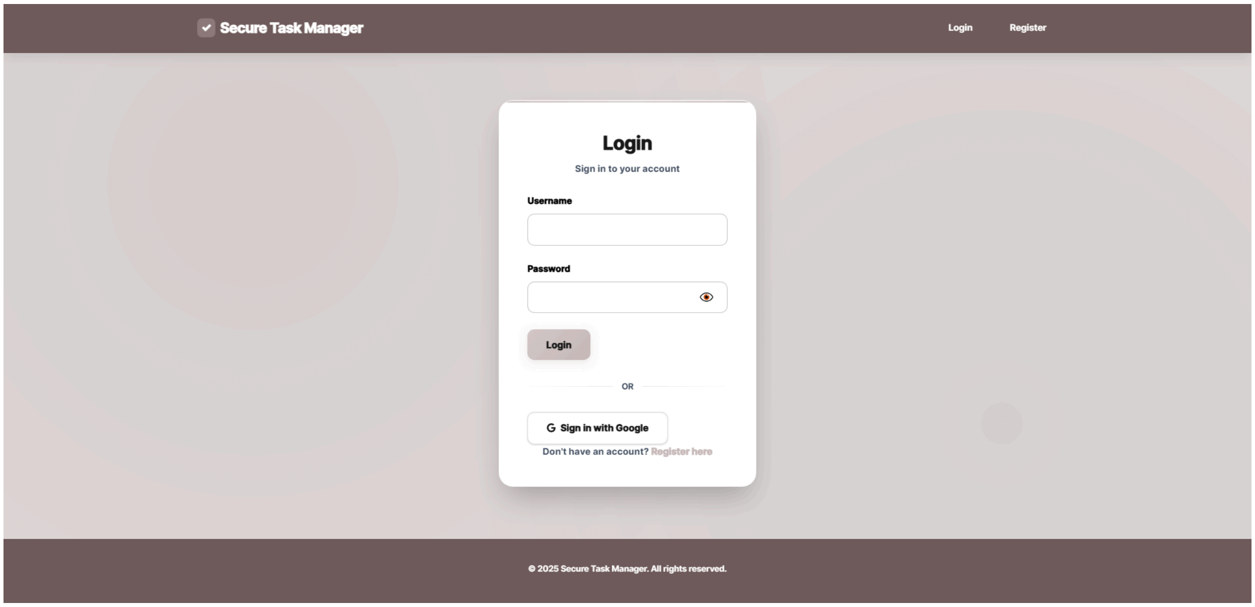
Dashboard (Task Management)

-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



Login

Sign in to your account

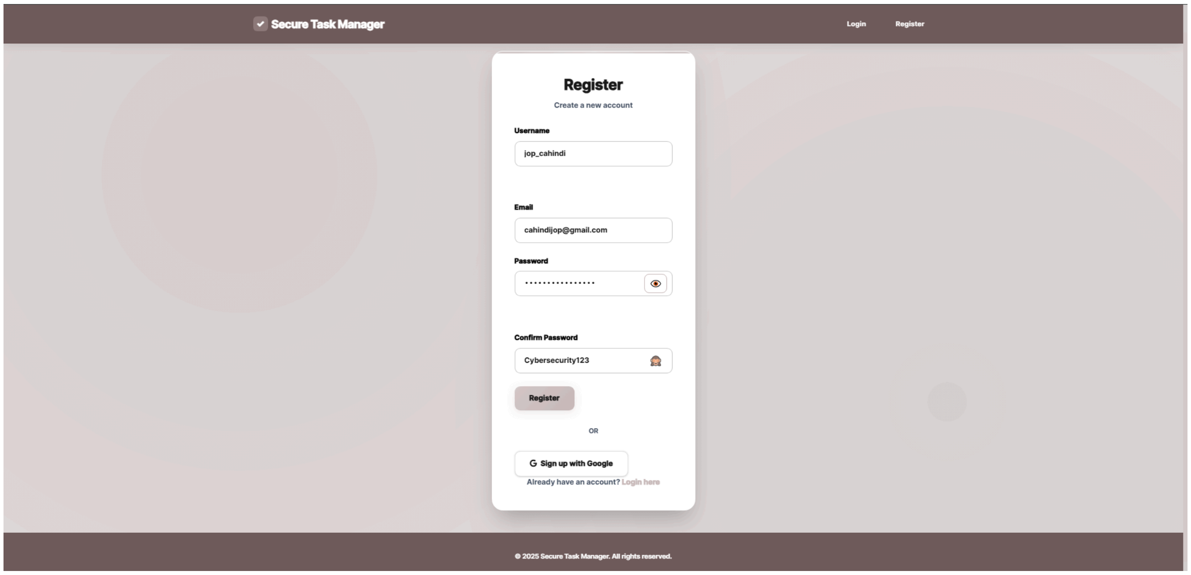
Username

Password

Don't have an account? Register here

© 2025 Secure Task Manager. All rights reserved.

REGISTRATION PAGE



Register

Create a new account

Username: jop_cahindi

Email: cahindijop@gmail.com

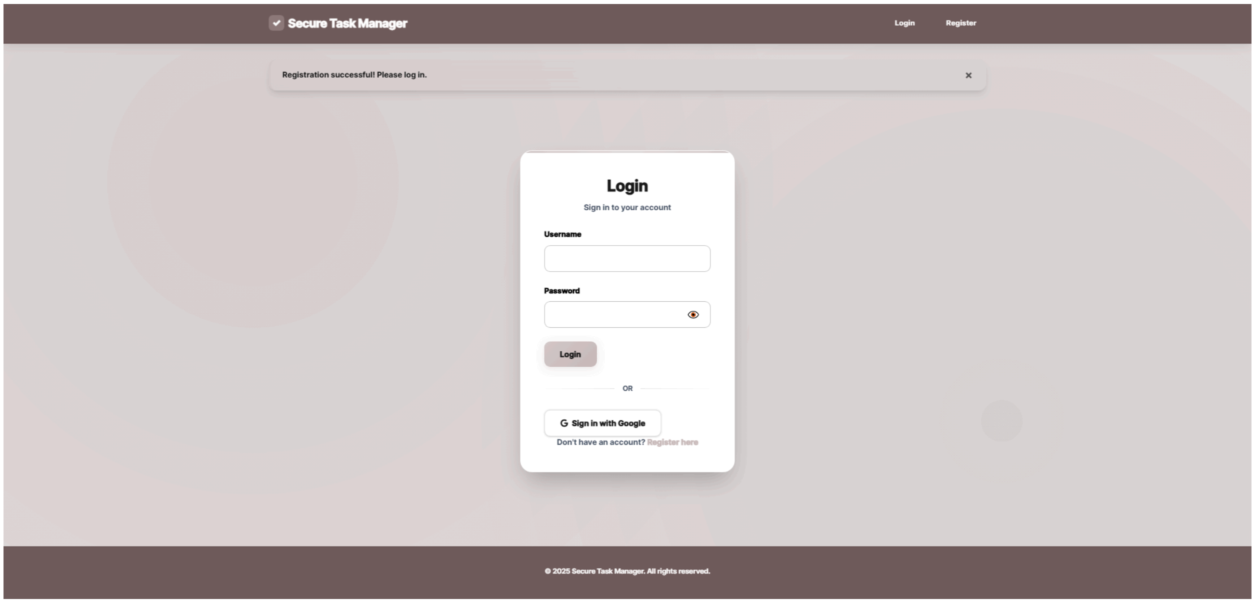
Password: ••••••••••••••••

Confirm Password: Cybersecurity123

Already have an account? Login here

© 2025 Secure Task Manager. All rights reserved.

LOGING IN



Registration successful! Please log in. ×

Login

Sign in to your account

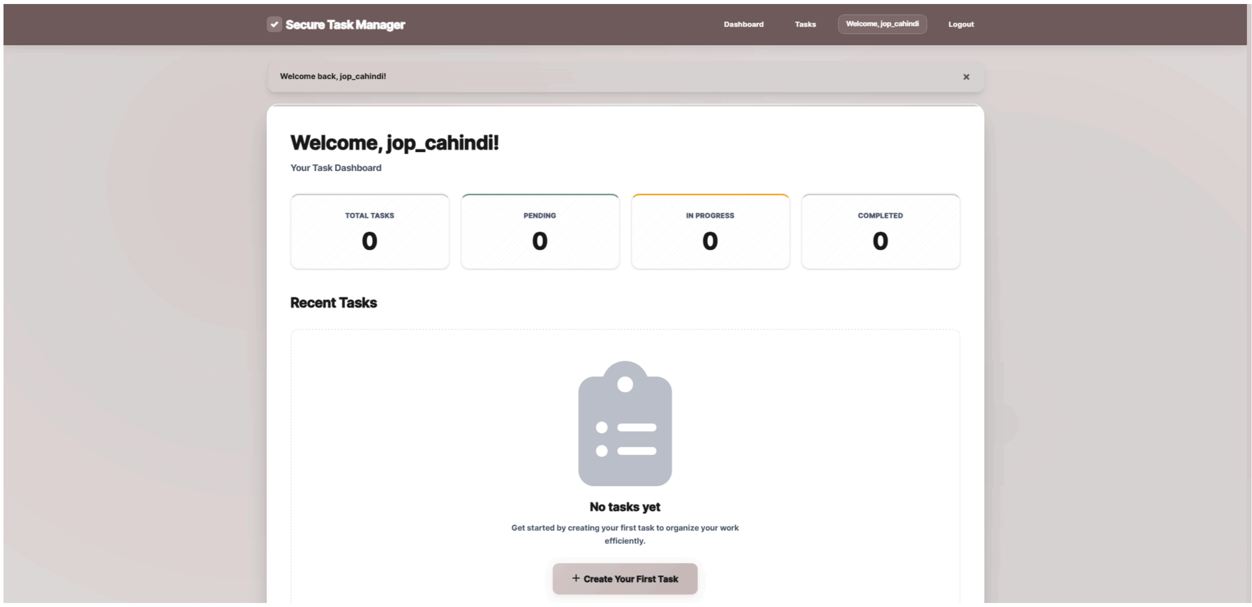
Username

Password

Don't have an account? Register here

© 2025 Secure Task Manager. All rights reserved.

DASHBOARD



Welcome back, jop_cahindi! ×

Welcome, jop_cahindi!

Your Task Dashboard

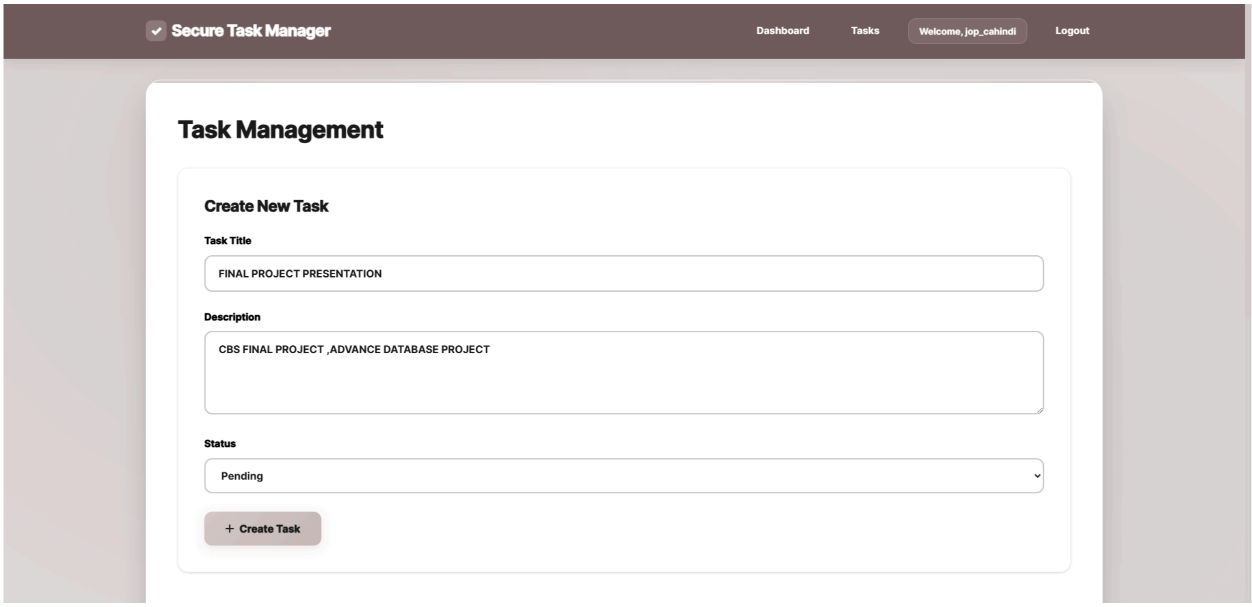
TOTAL TASKS	PENDING	IN PROGRESS	COMPLETED
0	0	0	0

Recent Tasks

No tasks yet

Get started by creating your first task to organize your work efficiently.

CREATING A TASKS



Task Management

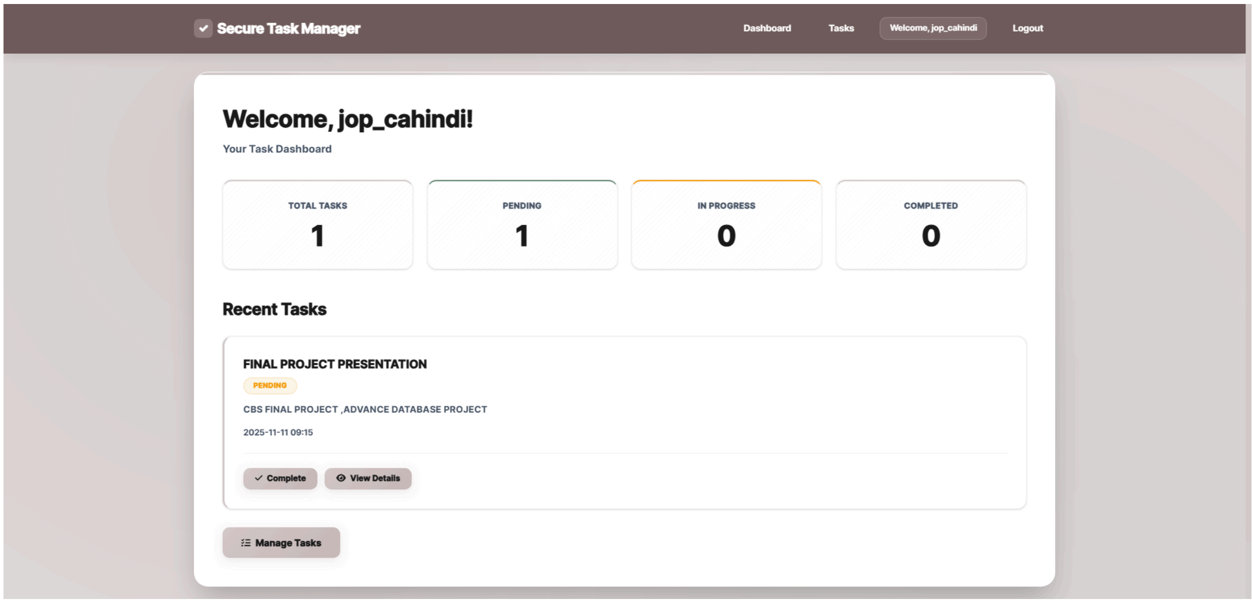
Create New Task

Task Title: FINAL PROJECT PRESENTATION

Description: CBS FINAL PROJECT ,ADVANCE DATABASE PROJECT

Status: Pending

TASKS CREATED



Welcome, jop_cahindi!

Your Task Dashboard

TOTAL TASKS	PENDING	IN PROGRESS	COMPLETED
1	1	0	0

Recent Tasks

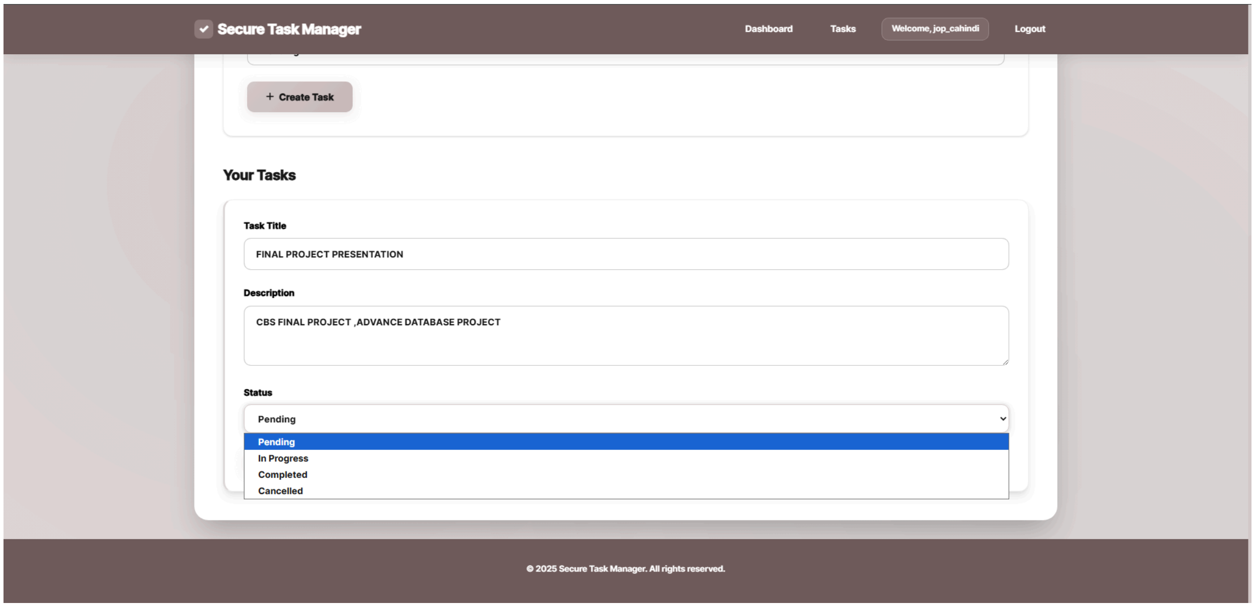
FINAL PROJECT PRESENTATION

PENDING

CBS FINAL PROJECT ,ADVANCE DATABASE PROJECT

2025-11-11 09:15

USERS CAN EDIT HIS/HER TASKS



Your Tasks

Task Title

FINAL PROJECT PRESENTATION

Description

CBS FINAL PROJECT ,ADVANCE DATABASE PROJECT

Status

Pending

- 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.

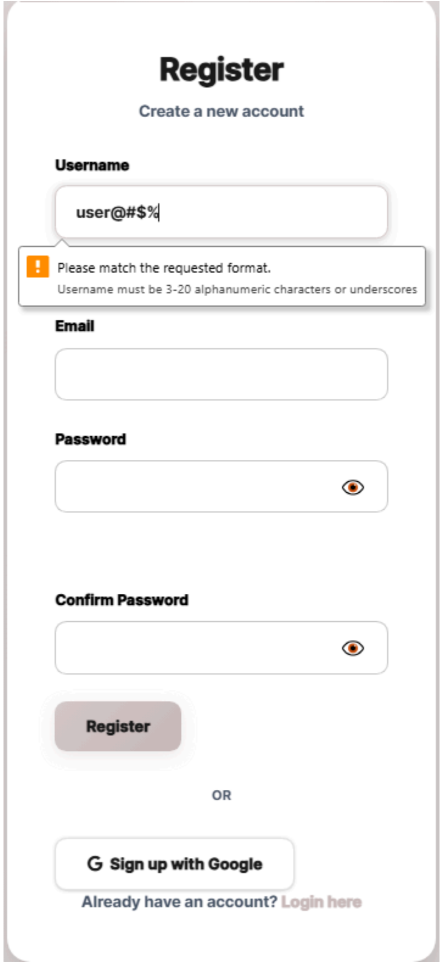
CSRF Protection

-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 USERNAMES



Register

Create a new account

Username

user@#$%

Please match the requested format.

Username must be 3-20 alphanumeric characters or underscores

Email

Password

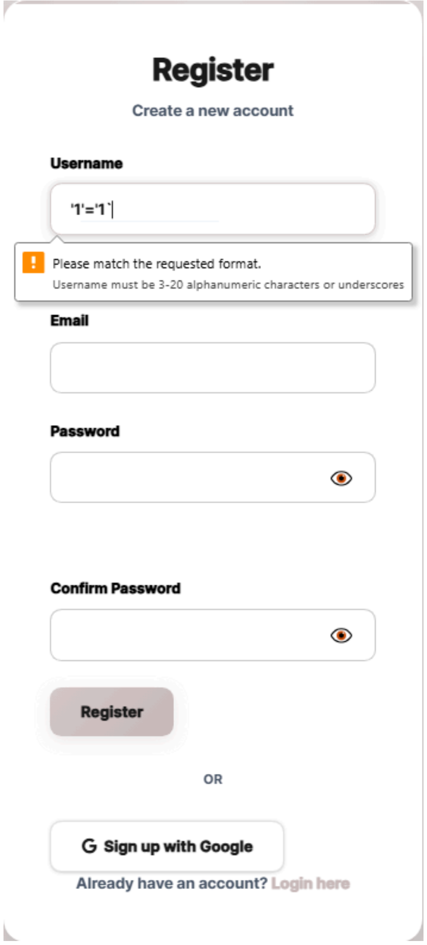
Confirm Password

Register

OR

Sign up with Google

Already have an account? Login here



Register

Create a new account

Username

'1'='1'

Please match the requested format.

Username must be 3-20 alphanumeric characters or underscores

Email

Password

Confirm Password

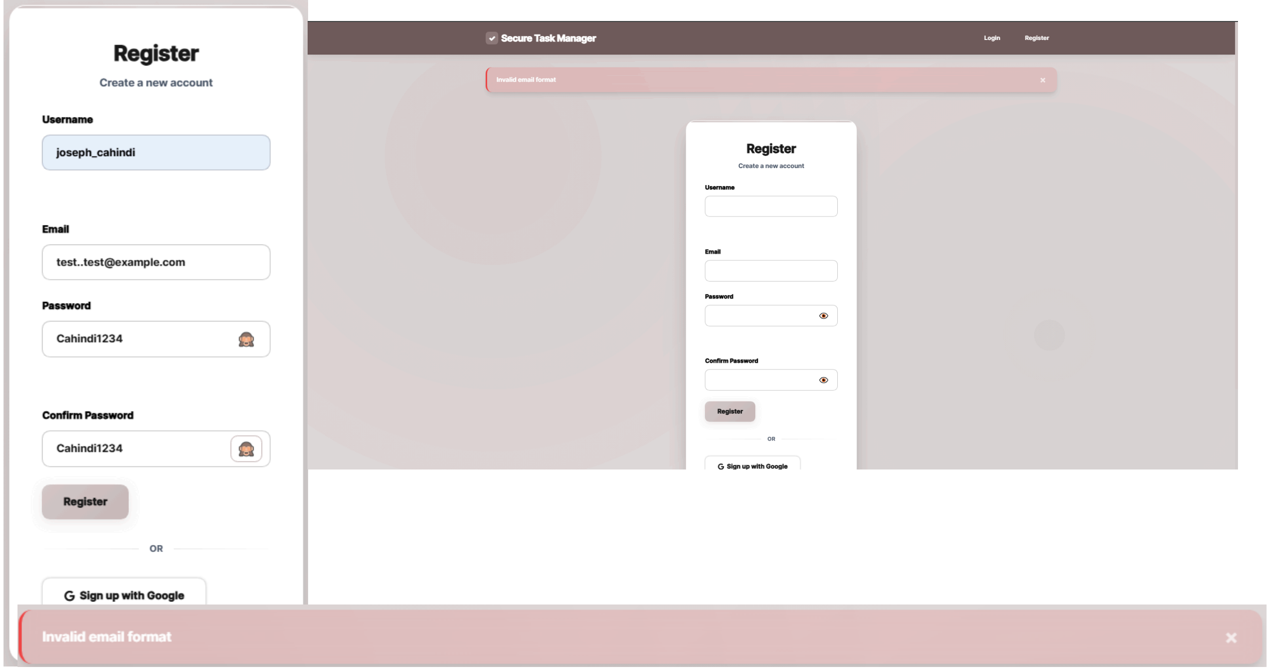
Register

OR

Sign up with Google

Already have an account? Login here

REGISTRATION TESTING INVALID EMAILS



Register

Create a new account

Username

joseph_cahindi

Email

test..test@example.com

Password

Cahindi1234

Confirm Password

Cahindi1234

Register

OR

Sign up with Google

Secure Task Manager

Login

Register

Invalid email format

Register

Create a new account

Username

Email

Password

Confirm Password

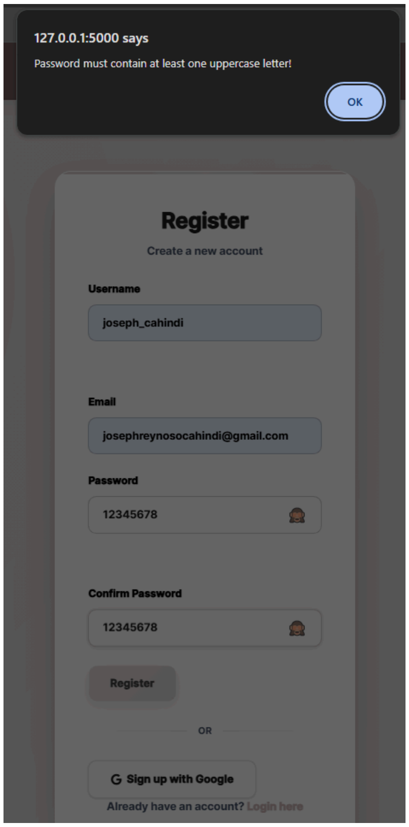
Register

OR

Sign up with Google

Invalid email format

REGISTRATION TESTING INVALID PASSWORDS



127.0.0.1:5000 says

Password must contain at least one uppercase letter!

Register

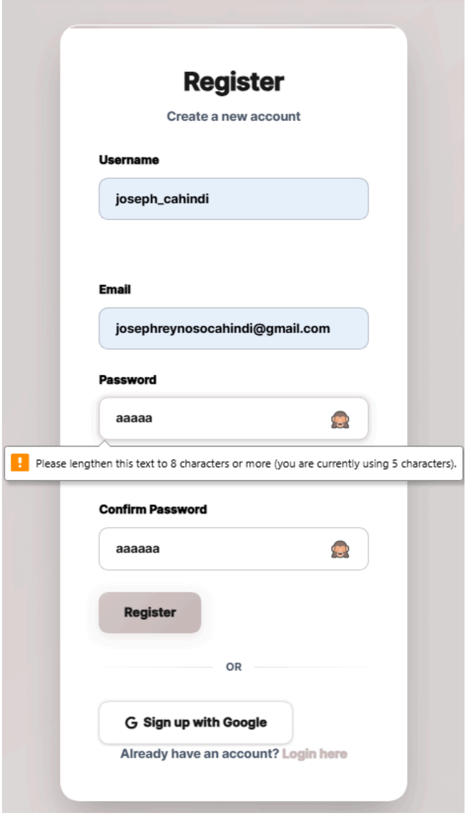
Create a new account

Username: joseph_cahindi

Email: josephreynosocahindi@gmail.com

Password: 12345678

Confirm Password: 12345678



Register

Create a new account

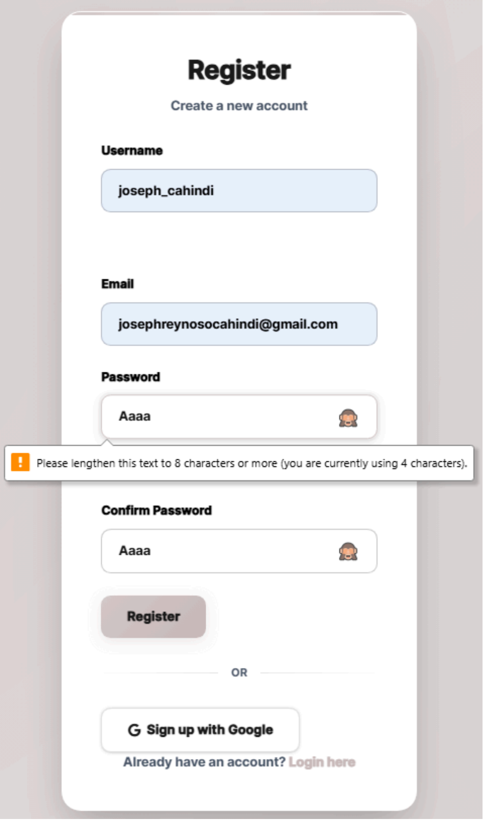
Username: joseph_cahindi

Email: josephreynosocahindi@gmail.com

Password: aaaaa

Please lengthen this text to 8 characters or more (you are currently using 5 characters).

Confirm Password: aaaaaa



Register

Create a new account

Username: joseph_cahindi

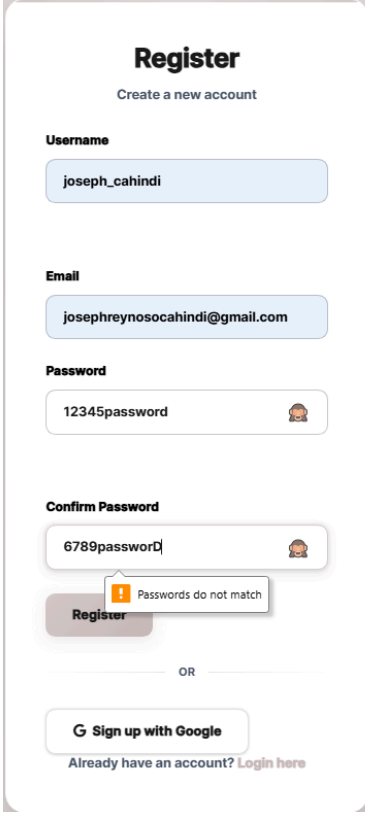
Email: josephreynosocahindi@gmail.com

Password: Aaaa

Please lengthen this text to 8 characters or more (you are currently using 4 characters).

Confirm Password: Aaaa

REGISTRATION TESTING CONFIRM PASSWORDS



Register

Create a new account

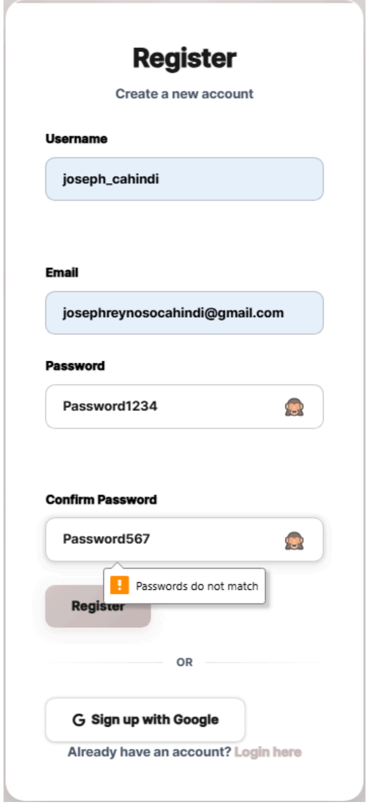
Username: joseph_cahindi

Email: josephreynosocahindi@gmail.com

Password: 12345password

Confirm Password: 6789passworD

Passwords do not match



Register

Create a new account

Username: joseph_cahindi

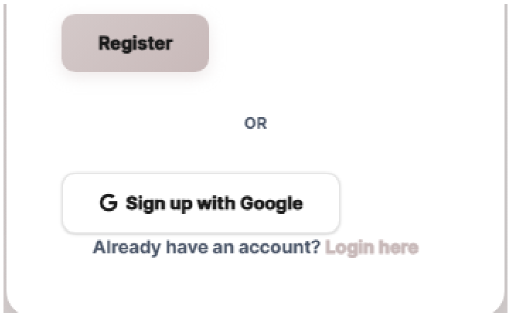
Email: josephreynosocahindi@gmail.com

Password: Password1234

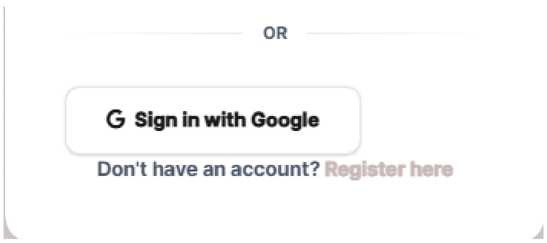
Confirm Password: Password567

Passwords do not match

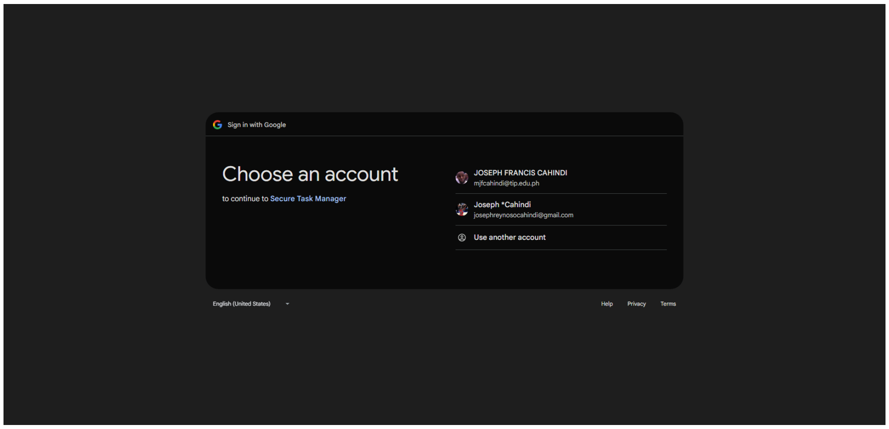
GOOGLE OAUTH REGISTRATION



Already have an account? Login here



Don't have an account? Register here



Choose an account

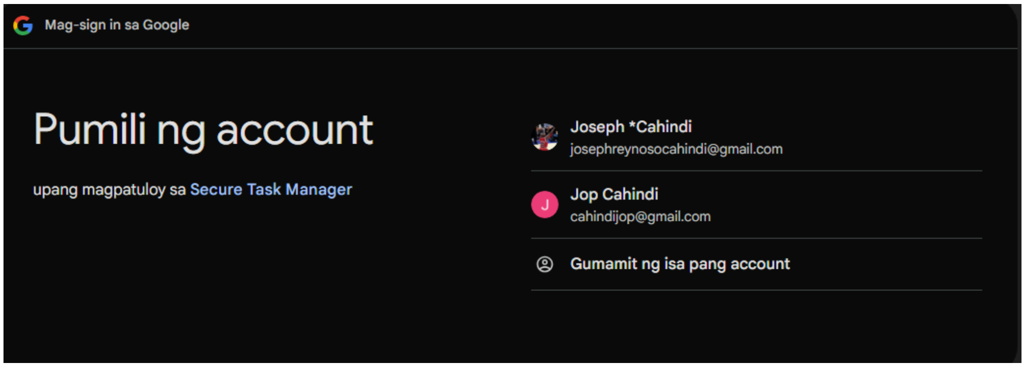
to continue to Secure Task Manager

JOSEPH FRANCIS CAHINDI
mjfcahindi@tip.edu.ph

Joseph *Cahindi
josephreynosocahindi@gmail.com

Use another account

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



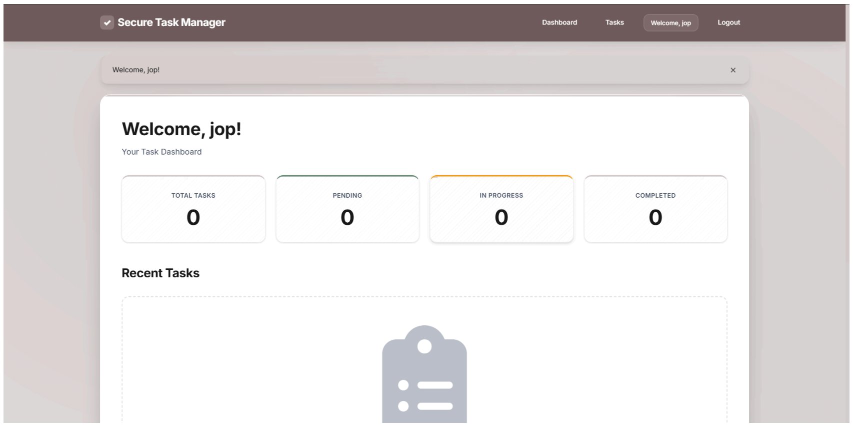
Pumili ng account

upang magpatuloy sa Secure Task Manager

Joseph *Cahindi
josephreynosocahindi@gmail.com

Jop Cahindi
cahindijop@gmail.com

Gumamit ng isa pang account



Welcome, jop!

Welcome, jop!

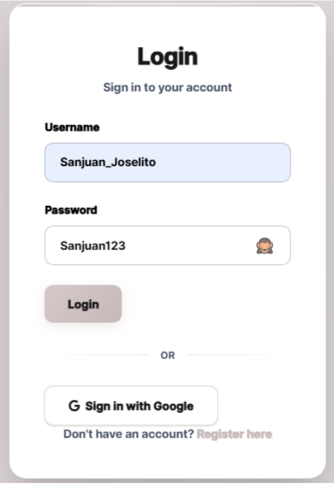
Your Task Dashboard

TOTAL TASKS	PENDING	IN PROGRESS	COMPLETED
0	0	0	0

Recent Tasks

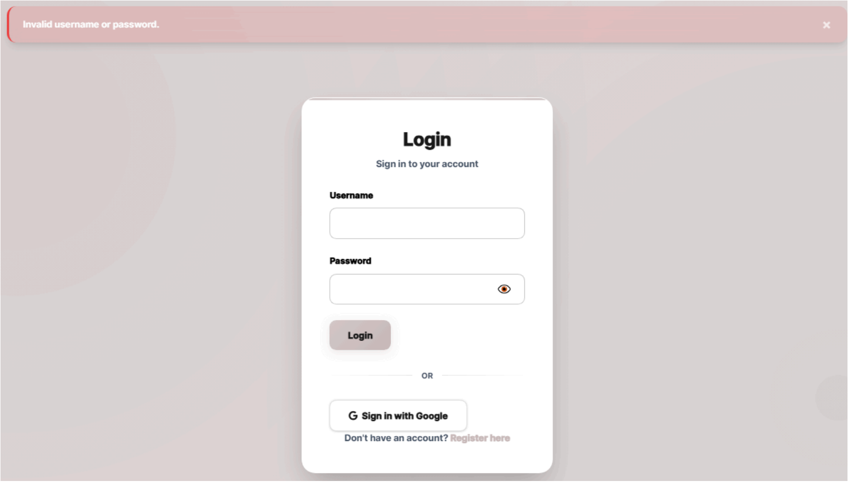
TESTING INVALID CREDENTIALS

(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)

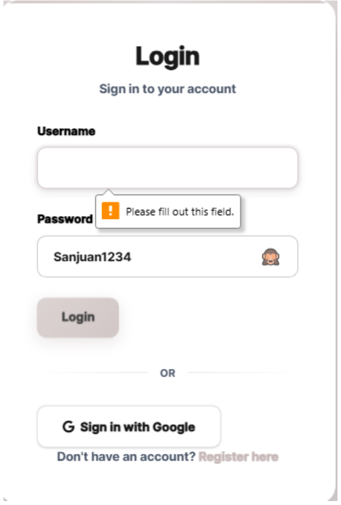


Username: Sanjuan_Joselito

Password: Sanjuan123

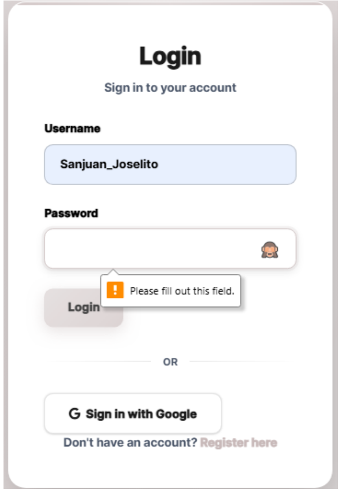


Invalid username or password.



Please fill out this field.

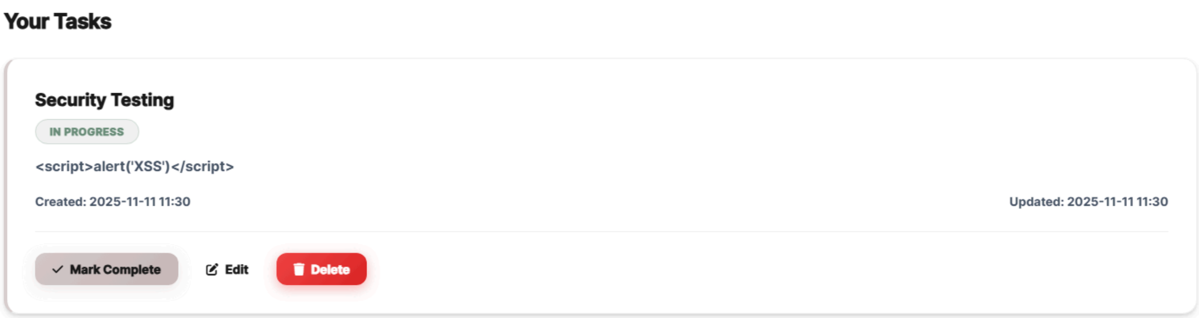
Password: Sanjuan1234



Username: Sanjuan_Joselito

Please fill out this field.

SECURITY TESTING <script>alert<’XSS’></script>



Your Tasks

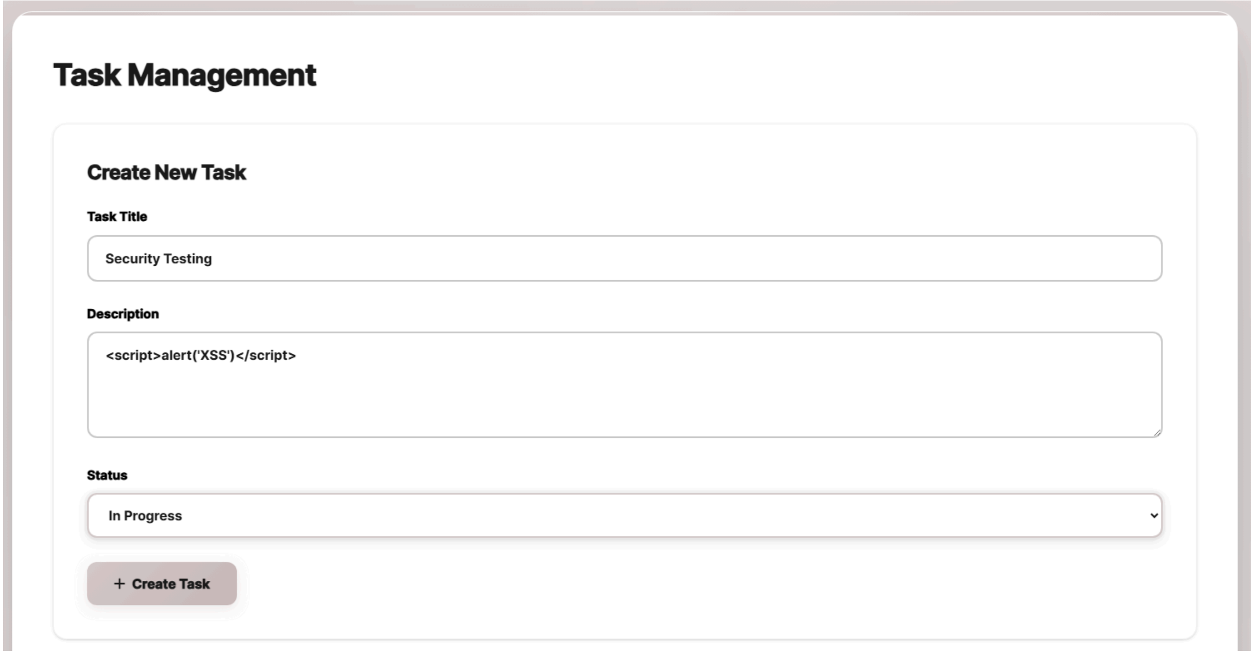
Security Testing

IN PROGRESS

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

Created: 2025-11-11 11:30

Updated: 2025-11-11 11:30



Task Management

Create New Task

Task Title

Security Testing

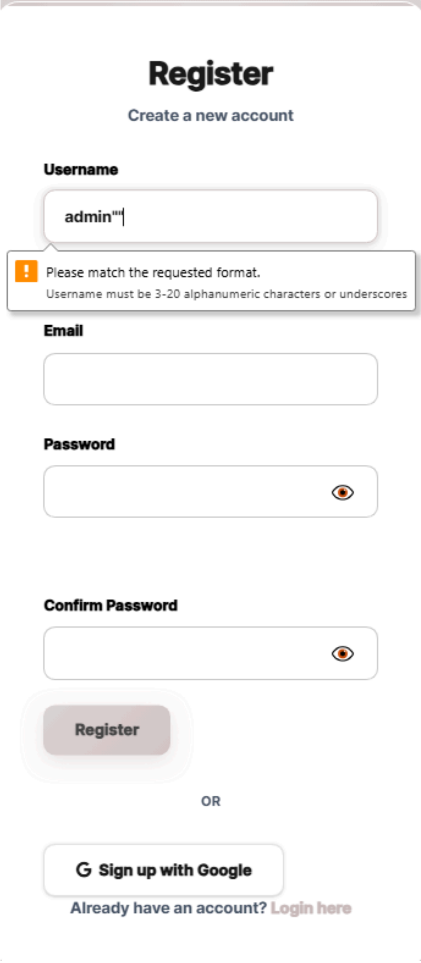
Description

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

Status

In Progress

SQL INJECTION PROTECTION



Register

Create a new account

Username

admin"'

Please match the requested format.

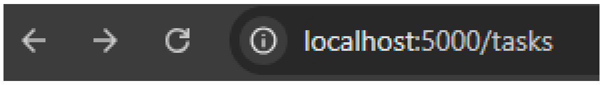
Username must be 3-20 alphanumeric characters or underscores

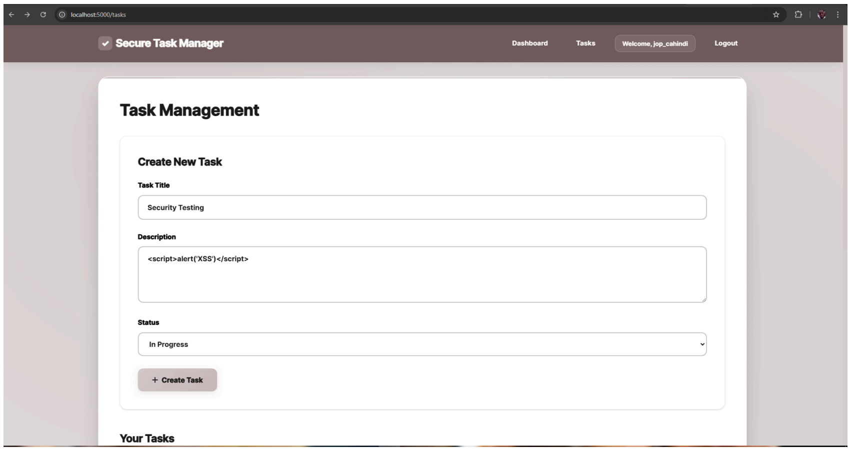
Email

Password

Confirm Password

ERROR HANDLING





Task Management

Create New Task

Task Title

Security Testing

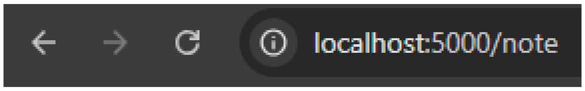
Description

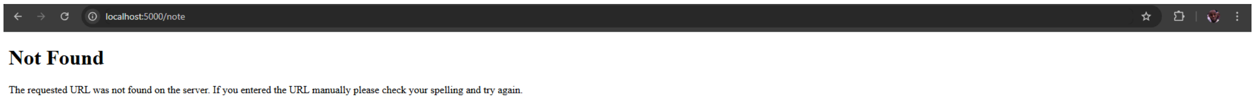
<script>alert('XSS')</script>

Status

In Progress

Your Tasks

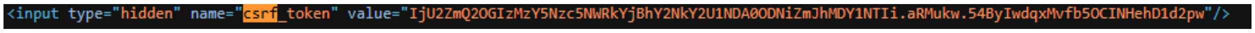




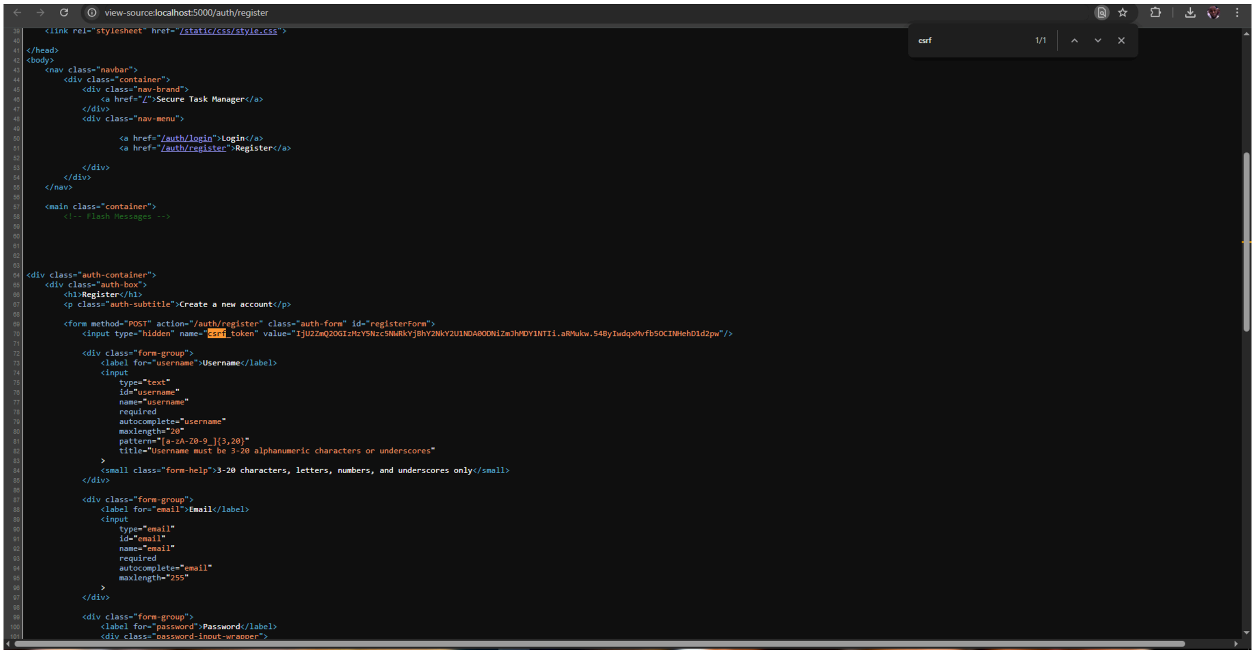
Not Found

The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

CSRRF PROTECTION

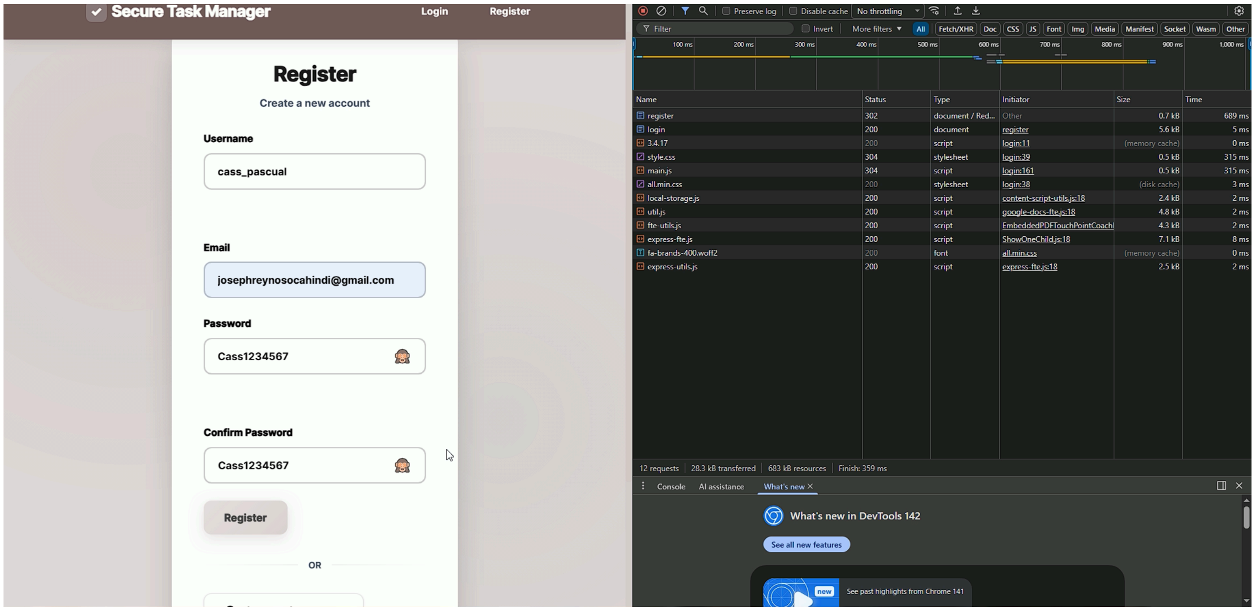


```
<input type="hidden" name="csrf_token" value="IjU2ZmQ2OGIzMzY5Nzc5NWRkYjBhY2NkY2U1NDA0ODNiZmJhMDY1NTIi.aRMukw.54ByIwdqxMvfb5OCINHehD1d2pw"/>
```



```
    <link rel="stylesheet" href="/static/css/style.css">

</head>
<body>
    <nav class="navbar">
        <div class="container">
            <div class="nav-brand">
                <a href="/">Secure Task Manager</a>
            </div>
            <div class="nav-menu">

                    <a href="/auth/login">Login</a>
                    <a href="/auth/register">Register</a>

            </div>
        </div>
    </nav>

    <main class="container">
        <!-- Flash Messages -->





<div class="auth-container">
    <div class="auth-box">
        <h1>Register</h1>
        <p class="auth-subtitle">Create a new account</p>

        <form method="POST" action="/auth/register" class="auth-form" id="registerForm">
            <input type="hidden" name="csrf_token" value="IjU2ZmQ2OGIzMzY5Nzc5NWRkYjBhY2NkY2U1NDA0ODNiZmJhMDY1NTIi.aRMukw.54ByIwdqxMvfb5OCINHehD1d2pw"/>

            <div class="form-group">
                <label for="username">Username</label>
                <input
                    type="text"
                    id="username"
                    name="username"
                    required
                    autocomplete="username"
                    maxlength="20"
                    pattern="[a-zA-Z0-9_]{3,20}"
                    title="Username must be 3-20 alphanumeric characters or underscores"
                >
                <small class="form-help">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
                    autocomplete="email"
                    maxlength="255"
                >
            </div>

            <div class="form-group">
                <label for="password">Password</label>
                <div class="password-input-wrapper">
```

CSRF TOKEN WORKING



Register

Create a new account

Username: cass_pascual

Email: josephreynosocahindi@gmail.com

Password: Cass1234567

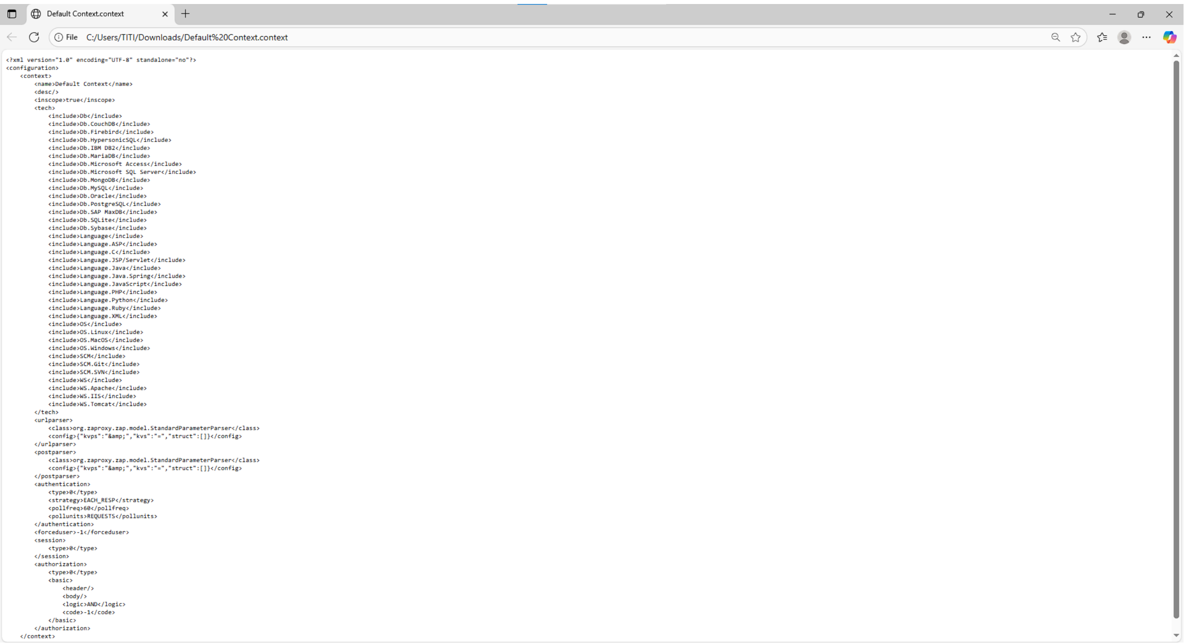
Confirm Password: Cass1234567

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.js:18	2.4 kB	2 ms
util.js	200	script	google-docs-fte.js:18	4.8 kB	2 ms
fte-utils.js	200	script	EmbeddedPDFTouchPointCoachl	4.3 kB	2 ms
express-fte.js	200	script	ShowOneChild.js:18	7.1 kB	8 ms
fa-brands-400.woff2	200	font	all.min.css	(memory cache)	0 ms
express-utils.js	200	script	express-fte.js:18	2.5 kB	2 ms

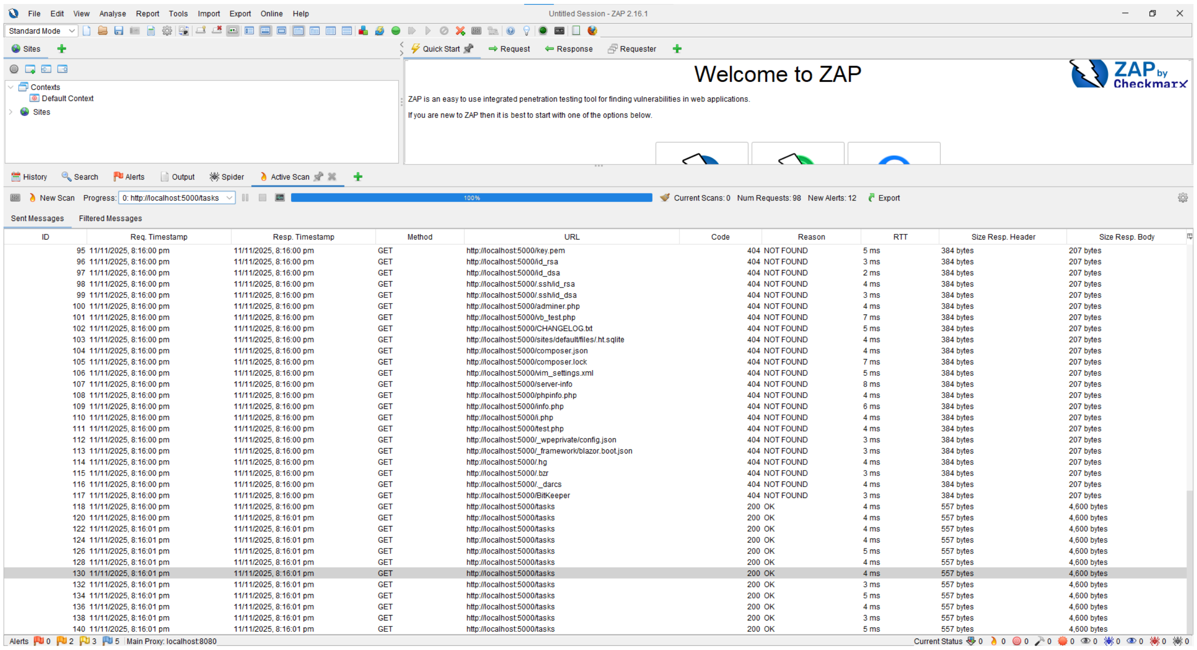
12 requests | 28.3 kB transferred | 683 kB resources | Finish: 359 ms

Console
AI assistance
What's new
What's new in DevTools 142
See all new features
new
See past highlights from Chrome 141

SECURITY AUDIT REPORT (ZAP)



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<configuration>
    <context>
        <name>Default Context</name>
        <desc/>
        <inscope>true</inscope>
        <tech>
            <include>Db</include>
            <include>Db.CouchDB</include>
            <include>Db.Firebird</include>
            <include>Db.HypersonicSQL</include>
            <include>Db.IBM DB2</include>
            <include>Db.MariaDB</include>
            <include>Db.Microsoft Access</include>
            <include>Db.Microsoft SQL Server</include>
            <include>Db.MongoDB</include>
            <include>Db.MySQL</include>
            <include>Db.Oracle</include>
            <include>Db.PostgreSQL</include>
            <include>Db.SAP MaxDB</include>
            <include>Db.SQLite</include>
            <include>Db.Sybase</include>
            <include>Language</include>
            <include>Language.ASP</include>
            <include>Language.C</include>
            <include>Language.JSP/Servlet</include>
            <include>Language.Java</include>
            <include>Language.Java.Spring</include>
            <include>Language.JavaScript</include>
            <include>Language.PHP</include>
            <include>Language.Python</include>
            <include>Language.Ruby</include>
            <include>Language.XML</include>
            <include>OS</include>
            <include>OS.Linux</include>
            <include>OS.MacOS</include>
            <include>OS.Windows</include>
            <include>SCM</include>
            <include>SCM.Git</include>
            <include>SCM.SVN</include>
            <include>WS</include>
            <include>WS.Apache</include>
            <include>WS.IIS</include>
            <include>WS.Tomcat</include>
        </tech>
        <urlparser>
            <class>org.zaproxy.zap.model.StandardParameterParser</class>
            <config>{"kvps":"&amp;","kvs":"=","struct":[]}</config>
        </urlparser>
        <postparser>
            <class>org.zaproxy.zap.model.StandardParameterParser</class>
            <config>{"kvps":"&amp;","kvs":"=","struct":[]}</config>
        </postparser>
        <authentication>
            <type>0</type>
            <strategy>EACH_RESP</strategy>
            <pollfreq>60</pollfreq>
            <pollunits>REQUESTS</pollunits>
        </authentication>
        <forceduser>-1</forceduser>
        <session>
            <type>0</type>
        </session>
        <authorization>
            <type>0</type>
            <basic>
                <header/>
                <body/>
                <logic>AND</logic>
                <code>-1</code>
            </basic>
        </authorization>
    </context>
```



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.

Progress: 0: http://localhost:5000/tasks 100% Current Scans: 0 Num Requests: 98 New Alerts: 12

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
95	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/id_rsa	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/id_dsa	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/.ssh/id_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/.ssh/id_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/adminer.php	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/vb_test.php	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.txt	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/sites/default/files/.ht.sqlite	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/composer.lock	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/vim_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/info.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/i.php	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/test.php	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/_wpeprivate/config.json	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/_framework/blazor.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/.bzr	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/._darcs	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/BitKeeper	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, 8:16:00 pm	11/11/2025, 8:16:01 pm	GET	http://localhost:5000/tasks	200	OK	4 ms	557 bytes	4,600 bytes
122	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

Alerts 0 2 3 5 Main Proxy: localhost:8080

Current Status 0 0 0 0 0 0 0 0 0 0