

# HydroDeepNet web application

## Purpose

The web application provides hydrological modeling tools, environmental data integration, and computational resources to support researchers and research institutions in conducting hydrological and environmental analyses. The platform enables:

- Hydrological model setup, calibration, and execution.
- Deep learning model development, training, and inference.
- Access to high-resolution hydrological modeling datasets.
- Visualization and analysis of hydrological simulations and data.
- Collaboration between researchers and institutions working on water resources, environmental science, and climate impact studies.

## Audience

The platform is designed for individual researchers, academic institutions, and government agencies conducting hydrological and environmental research. The primary users include:

- University researchers and students working on hydrology, hydrogeology, and environmental modeling.
- Government agencies and research institutions involved in water resource management, climate studies, and environmental assessments.
- Non-profit and private organizations engaged in watershed analysis, groundwater research, and climate adaptation planning.
- Geographical Scope: The platform primarily serves researchers and institutions within the United States, with datasets and models tailored to U.S. hydrological and environmental conditions.
- Ethical & Responsible Use: Users are expected to use the platform for scientific and research purposes only and comply with data sharing, citation, and institutional policies.

## Privacy and Policy

This web application is designed to support research and collaboration by providing access to hydrological modeling tools and datasets. We respect user privacy and are committed to protecting any information collected during platform use.

We collect user interactions with the application solely for improving system functionality, security, and performance. This includes authentication logs and feature usage analytics but

excludes personally identifiable data beyond what is necessary for secure access. All passwords are stored securely using encryption standards.

User data will not be shared with third parties unless mandated by Michigan State University's IT security policies or legal requirements. Any data provided for research purposes remains under the contributing institution's or researcher's ownership, and its use follows applicable agreements.

The platform operates entirely on open-source software and integrates national datasets, including the National Solar Radiation Database, National Hydrographical Dataset, USGS 3D Elevation Data, Gridded Soil Survey Geographic, and National Land Cover Database. We do not collect or process sensitive personal information.

By using this application, you acknowledge that minimal system interaction data is collected to improve platform reliability. You may contact the administrators for questions regarding data policies or security measures.

## **Terms of Use**

This web application is provided as a research collaboration tool for hydrological and environmental modeling. By accessing and using this platform, you agree to the following terms.

### **1. Research & Open-Source Integration**

This application is built on open-source technologies and integrates datasets from public sources, including but not limited to:

- National Solar Radiation Database (NSRDB)
- NHDPlus High Resolution
- LANDFIRE
- STATSGO2
- SNODAS

The platform also utilizes software such as QSWAT+, SWATPlusEditor, SWAT+, MODFLOW, Pytorch, and FloPy to model workflows.

### **2. User Responsibilities & Compliance**

- Users are responsible for ensuring that their activities comply with Michigan State University's IT policies and relevant research agreements.
- Unauthorized access, data scraping, or any form of misuse, including attempts to bypass authentication or disrupt system functionality, is strictly prohibited.
- Access to specific datasets may be subject to licensing agreements or institutional policies. Users contributing data must ensure they have the appropriate permissions to share it on this platform.

### **3. Citation & Attribution Requirements**

- Users must cite this web application in any publication, report, or research output that relies on the models or modeling results generated from this platform.
- Users are responsible for citing the datasets utilized within their models, following the citation requirements of each data provider.

- Citation details, including proper attribution formats, will be provided within the application and associated documentation.
- 4. Data Sharing & Ethics
  - Users contributing data or models must ensure they have the rights to share such content and that it complies with ethical and legal standards.
  - The platform is designed to foster collaboration but does not assume responsibility for the accuracy or validation of user-provided data.

---

## System Security Check

---

### 1. Apache Configuration

- ✓ **apachectl configtest** → Syntax OK
  - ✓ **Apache is running without issues** → `systemctl status apache2`
  - ✓ **No critical errors in logs** → Checked `/var/log/apache2/error.log`
- 

### 2. SSL/TLS Configuration

- ✓ **SSL Certificate Valid**
  - ✓ **SSL Key File Exists** (`/etc/ssl/private/ciwre-bae.campusad.msu.edu.key`)
  - ✓ **Correct Key Permissions** (`chmod 640` and `chown root:www-data`)
  - ✓ **Valid Certificate Chain** (Confirmed via OpenSSL `s_client`)
  - ✓ **HTTPS Redirection Works** (`curl -I http://` correctly redirects to HTTPS)
- 

### 3. Apache Modules

- ✓ **rewrite\_module** → Enabled
  - ✓ **ssl\_module** → Enabled
  - ✓ **wsgi\_module** → Enabled
  - ✓ **headers\_module** → Enabled
  - ✓ **No unnecessary modules** (e.g., `dav`, `cgi`) enabled
- 

### 4. Web Application Behavior

- ✓ **Login Redirects Work** (curl -I <https://ciwre-bae.campusad.msu.edu> → 302 FOUND)
  - ✓ **404 Handling Works** (curl -I <https://ciwre-bae.campusad.msu.edu/some-random-directory/> → 404 NOT FOUND)
  - ✓ **Admin Route Behavior** (/admin returns 404, expected since the admin page isn't configured yet)
  - ✓ **NFS Data Drive Not Exposed** (/data/ returns 404, preventing unintended exposure)
- 

## 5. **DNS & Network**

- ✓ **Correct DNS Resolution** (ping ciwre-bae.campusad.msu.edu → IP 35.9.219.73)
  - ✓ **No Network Issues** (0% packet loss on ping test)
- 











## 6. **Security Headers**

- ✓ **Strict-Transport-Security (HSTS) Enabled**
  - ✓ **X-Frame-Options** → SAMEORIGIN
  - ✓ **X-Content-Type-Options** → nosniff
  - ✓ **Permissions-Policy** → browsing-topics=()
  - ✓ **Referrer-Policy** → strict-origin-when-cross-origin
- 

## 7. **Flask-Specific Checks**






- ✓ **Flask app initializes without errors** (Flask(\_\_name\_\_) is correctly set)
  - ✓ **Flask is running under WSGI** (mod\_wsgi)
  - ✓ **Static files served correctly** (curl -I <https://ciwre-bae.campusad.msu.edu/static/>)
  - ✓ **Environment variables correctly set** (Config class in config.py)
  - ✓ **Database URI is correctly set** (SQLALCHEMY\_DATABASE\_URI)
  - ✓ **Database Connection Works** (flask db upgrade or direct connection test)
  - ✓ **Login & Signup Work Properly** (/login, /signup)
  - ✓ **Session cookies are secure** (SESSION\_COOKIE\_SECURE = True)
  - ✓ **CSRF Protection Enabled** (Flask-WTF CSRFProtect(app))
  - ✓ **Flask-Talisman Enforced Security Policies** (HSTS, force HTTPS)
-

## 8. Flask Application Routes

Route	Status
/ (Redirects to /home)	
/login (User authentication)	
/signup (User registration)	
/logout (Session clear)	
/dashboard (Restricted to authenticated users)	
/model-settings (Model configuration page)	
/hydro_geo_dataset (Data retrieval endpoint)	
/get_options (Dynamic option retrieval)	
/visualizations (Fetching visual data)	
/privacy, /terms, /about (Static pages)	

---

## 9. API & Data Access

Endpoint	Status
/get_station_characteristics	
/get_subvariables	
/search_site	
/deeplearning_models	
/vision_system	

---

## 10. Password & Authentication Security

- ✓ **Passwords Are Hashed** (Implemented in User model with proper hashing)
  - ✓ **No Plaintext Passwords Stored** (User.check\_password() properly validates hash)
  - ✓ **Strong Password Enforcement** (Checked using regex for length, case, digits, special chars)
  - ✓ **Account Verification Implemented** (Email verification via send\_verification\_email)
  - ✓ **Login Protection Against Brute Force** (Flask-Login handling session invalidation)
  - ✓ **Secure Session Storage** (Cookies are SECURE, HTTPONLY, and SAME SITE=Lax)
- 

## 11. Database Configuration & Security

- ✓ **SQLAlchemy ORM Used** (Prevents SQL Injection)
- ✓ **Database Credentials Are Secure** (Loaded from environment variables)
- ✓ **Automatic Database Migrations Enabled** (flask db upgrade)

- ✓ **Session-Based Authentication** (Using Flask-Login)
  - ✓ **User Sessions Cleared on Logout** (session.clear())
  - ✓ **Database Integrity Checks Passed** (db.create\_all() executed successfully)
- 

## 12. ✓ File & Directory Permissions

Path	Expected Owner	Expected Permissions	Status
/data/SWATGenXApp/codes/	www-data:www-data	755	✓
/data/SWATGenXApp/codes/web_application/logs/	www-data:www-data	750	✓
/etc/ssl/private/ciwre-bae.campusad.msu.edu.key	root:www-data	640	✓
/etc/ssl/certs/ciwre-bae_campusad_msu_edu_cert.cer	root:root	644	✓

---

## 13. ✓ SFTP: Security, Access, File & Directory Permissions

	Status
User directory permissions ensure restricted access (chmod 2775)	✓
Apache (www-data) has full control over user directories	✓
SFTP users (sftp_users group) cannot escape their home directory (ChrootDirectory enabled)	✓
Password authentication is enabled for SFTP, using only SSH keys	✓
SFTP users cannot execute commands or access /bin/bash (shell is /usr/sbin/nologin)	✓
Access Control Lists (ACLs) ensure Apache and SFTP users have appropriate access	✓
Users cannot see or modify each other's files	✓
SFTP users' upload directories are properly owned (user:www-data) and secured (chmod 2770)	✓
Firewall rules restrict SFTP access to specific IPs or networks (if applicable)	✓
SFTP logs are enabled and stored in /var/log/auth.log for auditing access attempts	✓
No unnecessary users have access to SFTP directories (getfacl shows only intended users)	✓
Root cannot log in via SFTP (PermitRootLogin no in /etc/ssh/sshd_config)	✓
SSH configuration (/etc/ssh/sshd_config) explicitly allows only sftp_users for SFTP (Match Group sftp_users)	✓
No weak or empty passwords (awk -F: '(\$2 == "") {print \$1}' /etc/shadow confirms no empty password fields)	✓

14. ● FINAL STATUS:

- ✓ All components, including Flask, Apache, SSL/TLS, password handling, and database security, are functioning correctly.
- ✓ Security best practices, authentication, and session handling are enforced.
- ✓ No plaintext passwords or weak security vulnerabilities detected.