Cybersecurity Threat Detection System - Setup Guide

Prerequisites

Before starting, ensure you have the following installed:

1. **XAMPP** (recommended) or **WAMP/LAMP** stack
   - Apache Web Server
   - MySQL Database
   - PHP (version 7.4 or higher)
2. **Web browser** (Chrome, Firefox, Safari, etc.)
3. **Text editor** (VS Code, Sublime Text, etc.) - optional for modifications

Step 1: Install XAMPP

Windows:

1. Download XAMPP from https://www.apachefriends.org/
2. Run the installer and follow the setup wizard
3. Install Apache, MySQL, and PHP components
4. Start XAMPP Control Panel

macOS:

1. Download XAMPP for macOS
2. Mount the DMG file and drag XAMPP to Applications
3. Launch XAMPP from Applications folder

Linux:

```bash
# Download and install XAMPP
wget https://www.apachefriends.org/xampp-files/8.2.12/xampp-linux-x64-8.2.12-0-installer.run
chmod +x xampp-linux-x64-8.2.12-0-installer.run
sudo ./xampp-linux-x64-8.2.12-0-installer.run
```

Step 2: Start Services

1. Open XAMPP Control Panel

2. Start **Apache** service (click "Start" button)
3. Start **MySQL** service (click "Start" button)
4. Verify both services are running (green status)

Step 3: Set Up Project Files

1. **Navigate to htdocs folder:**
   - Windows: `C:\xampp\htdocs\`
   - macOS: `/Applications/XAMPP/htdocs/`
   - Linux: `/opt/lampp/htdocs/`
2. **Create project folder:**

```
mkdir cyber-security-dashboard
cd cyber-security-dashboard
```

3. **Copy your project files:**
   - `index.html` - Main dashboard interface
   - `threat_detector.php` - Backend API
   - `setup.sql` - Database setup script

Step 4: Database Setup

Method 1: Using phpMyAdmin (Recommended)

1. Open web browser and go to: `http://localhost/phpmyadmin`
2. Click "Import" tab
3. Choose your `setup.sql` file
4. Click "Go" to execute the script

Method 2: Using MySQL Command Line

```
bash

# Access MySQL
mysql -u root -p

# Run the setup script
source /path/to/your/setup.sql
```

Method 3: Manual Setup

1. Go to `http://localhost/phpmyadmin`
2. Click "New" to create database
3. Name it `cyber_security`
4. Copy and paste the SQL commands from `setup.sql` in the SQL tab

Step 5: Configure Database Connection

Open `threat_detector.php` and verify the database configuration:

```php
class Database {
    private $host = 'localhost';
    private $db_name = 'cyber_security';
    private $username = 'root';
    private $password = '';  // Default XAMPP password is empty
    // ... rest of the code
}
```

Note: If you set a MySQL password, update the `$password` field.

Step 6: Test the Setup

1. **Access the dashboard:**
   - Open browser and go to: `http://localhost/cyber-security-dashboard/`
   - You should see the cybersecurity dashboard
2. **Test API endpoints:**
   - `http://localhost/cyber-security-dashboard/threat_detector.php`
   - `http://localhost/cyber-security-dashboard/threat_detector.php?action=getStats`
   - `http://localhost/cyber-security-dashboard/threat_detector.php?action=healthCheck`

Step 7: Verify Everything Works

Dashboard Features to Test:

- ✅ **Start Full Scan** - Should simulate scanning process
- ✅ **Update Threat Database** - Shows update confirmation
- ✅ **Generate Report** - Displays security report
- ✅ **Clear Logs** - Clears threat log entries

- ✅ **Real-time Metrics** - Numbers should update automatically
- ✅ **Threat Log** - Should populate with simulated threats

Database Verification:

1. Go to phpMyAdmin: `http://localhost/phpmyadmin`
2. Select `cyber_security` database
3. Check that these tables exist:
   - `threats`
   - `threat_logs`
   - `security_metrics`
   - `network_monitoring`
   - `firewall_rules`
   - `system_alerts`

Common Issues and Solutions

Issue 1: "Access Denied" Database Error

Solution:

```php
// In threat_detector.php, try this configuration:
private $host = 'localhost';
private $db_name = 'cyber_security';
private $username = 'root';
private $password = '';  // Keep empty for default XAMPP
```

Issue 2: Apache/MySQL Won't Start

Solutions:

- Check if ports 80 (Apache) and 3306 (MySQL) are available
- Try different ports in XAMPP config
- Run XAMPP as administrator/sudo

Issue 3: 404 Error When Accessing Dashboard

Solution:

- Ensure files are in correct htdocs subfolder
- Check file permissions
- Verify Apache is running

Issue 4: Database Connection Failed

Solutions:

1. Verify MySQL is running in XAMPP
2. Check database credentials in `threat_detector.php`
3. Ensure `cyber_security` database exists

Issue 5: PHP Errors

Solution:

- Enable error reporting by adding to `threat_detector.php`:

```php
error_reporting(E_ALL);
ini_set('display_errors', 1);
```

Advanced Configuration

Enable SSL (Optional)

1. In XAMPP, edit `httpd-ssl.conf`
2. Access via `https://localhost/cyber-security-dashboard/`

Custom Domain (Optional)

1. Edit hosts file:
   - Windows: `C:\Windows\System32\drivers\etc\hosts`
   - macOS/Linux: `/etc/hosts`
2. Add: `127.0.0.1 cybersecurity.local`
3. Access via `http://cybersecurity.local/cyber-security-dashboard/`

Performance Optimization

1. **Enable PHP OPcache** in `php.ini`
2. **Optimize MySQL** settings

3. **Use CDN** for external resources

Project Structure

```
cyber-security-dashboard/
├── index.html              # Main dashboard
├── threat_detector.php     # Backend API
├── setup.sql               # Database schema
├── README.md               # This guide
└── screenshots/            # Optional: screenshots folder
```

API Endpoints Reference

Endpoint	Method	Description
`?action=getThreats`	GET	Fetch recent threats
`?action=getStats`	GET	Get threat statistics
`?action=simulateThreats`	GET	Generate sample threats
`?action=getNetworkStats`	GET	Network monitoring data
`?action=healthCheck`	GET	System health status
`?action=logThreat`	POST	Log new threat
`?action=cleanOld`	GET	Clean old records

Security Considerations

⚠️ **Important Notes:**

- This is a **demonstration project** - not for production use
- Change default database passwords
- Implement proper authentication
- Add input validation and sanitization
- Use HTTPS in production
- Implement rate limiting
- Add proper error handling

Next Steps

1. **Customize the dashboard** - Modify colors, layout, or add features
2. **Add real threat detection** - Integrate with actual security tools

3. **Implement user authentication** - Add login system
4. **Create mobile app** - Develop companion mobile interface
5. **Add email alerts** - Implement notification system

Support

If you encounter issues:

1. Check XAMPP error logs
2. Verify database connection
3. Test API endpoints individually
4. Check browser console for JavaScript errors

Success Indicators

- ✅ Dashboard loads without errors
- ✅ Buttons respond and show animations
- ✅ Threat log populates with sample data
- ✅ Real-time metrics update
- ✅ API endpoints return JSON data
- ✅ Database contains sample threat data

Congratulations! Your cybersecurity threat detection system is now running successfully.