WebSecBot

User Documentation

Your Web Development Security Assistant

WebSecBot Team
2025

A project funded by netidee

https://www.netidee.at/websecbot

Contents

1 Introduction

1.1 What is WebSecBot?

WebSecBot is a Chrome browser extension that helps developers identify and fix security vulnerabilities in their web applications. By combining automated analysis with an AI-powered chat assistant, WebSecBot makes web security testing accessible to developers who may not have extensive security expertise.

The extension scans websites for common security issues based on OWASP Top Ten security categories and provides detailed reports with actionable recommendations. The integrated AI assistant can explain findings in plain language and suggest specific remediation steps.

Key Insight: WebSecBot bridges the gap between professional security tools and everyday development practice by offering security guidance directly in your browser as you work.

1.2 Who is it for?

WebSecBot is designed for:

- Web developers who want to improve the security of their applications
- Open source developers looking to secure their projects
- Anyone building web applications who wants to incorporate security testing into their workflow

Disclaimer: WebSecBot provides quick and accessible security guidance for developers directly in their browser. While it helps identify common issues based on OWASP Top Ten and supports remediation via LLM-driven assistance, it is not a substitute for professional penetration testing. Results may be incomplete, inconsistent, or occasionally inaccurate due to the limitations of large language models, including hallucinations and non-deterministic behavior. Use WebSecBot as a first line of defense–always validate findings through expert review for critical applications.

1.3 Key Features and Benefits

Feature	Benefit
Automated Security Analysis	Scan web applications for OWASP Top Ten vulnerabilities directly from your browser
Interactive AI Assistant	Get explanations about security findings in plain language through natural conversation
Contextual Recommendations	Receive specific suggestions for fixing identified vulnerabilities
Code Examples	Obtain sample code snippets to implement security improvements
Integrated Workflow	Seamlessly incorporate security testing into your development process

2 Installation Guide

2.1 System Requirements

- Google Chrome

- Docker Desktop[1] or `docker` & `docker-compose` packages on Linux
- Node & npm (for building the extension from source)
- Internet connection (first-time image pull and `npm install`)

2.2 Start the LLM backend (AnythingLLM via Docker)

WebSecBot talks to an OpenAI-compatible endpoint provided by **AnythingLLM**.

1. **Clone and launch AnythingLLM**

```
git clone https://github.com/Mintplex-Labs/anything-llm
cd anything-llm

# one time setup: copy env & pull images
copy docker\.env.example docker\.env          # Windows
# cp docker/.env.example docker/.env          # macOS / Linux
docker compose -f docker/docker-compose.yml pull
docker compose -f docker/docker-compose.yml up -d
```

2. Open `http://localhost:3001` in your browser.
3. On the welcome screen, click **Get Started**.

2.2.1 Setting up an LLM provider (Groq example)

AnythingLLM requires an LLM provider to function. For optimal performance, we recommend using Llama 3.3 70B versatile with a provider like Groq.

1. Create a Groq API key at `https://console.groq.com/keys`.
2. In the AnythingLLM interface, search for "LLM provider" in the search bar.
3. Select **Groq** from the options.
4. Paste your Groq API key in the designated field.
5. Choose `llama-3.3-70b-versatile` from the model dropdown.
6. Click *Save*.

Tip – Our testing shows that Llama 3.3 70B versatile (through a service like Groq or locally) provides the best balance between security analysis results and speed. Smaller models often produce less accurate security assessments, while "reasoning" variants of models significantly increase analysis time.

[1] `https://www.docker.com/products/docker-desktop`

2.2.2 Creating your workspace and API key

After setting up your LLM provider, you need to create a workspace and generate an API key for WebSecBot to use.

1. Click on **Create Workspace** and name it **My Workspace** (exact capitalization matters for default settings).
2. Test your workspace by sending a simple message like "Hi" and checking for a response.
3. Navigate to **Settings → API Keys** via the tools/settings menu.
4. Click **Generate** to create a new Developer API key.
5. Copy the generated key - you'll need this for WebSecBot.

2.2.3 Enhancing analysis with RAG

Retrieval-Augmented Generation lets AnythingLLM pull facts from your own document collection while it reasons about a prompt. For WebSecBot we provide a ready-curated OWASP knowledge pack.

1. **Download the documents**
   Grab everything in the `OWASP-Resources/` folder of the WebSecBot repo.
2. **Import into AnythingLLM**
   - Open your `My Workspace` workspace
   - Click *Add Documents* and upload the files
   - Add them to the current workspace
3. **Enable use at chat time**
   In *Workspace Settings* make sure *"Include documents in chat context"* is toggled ON.

RAG lets WebSecBot cite OWASP chapters verbatim and produce far more actionable fixes.

2.3 Installing and configuring the WebSecBot extension

1. **Download or clone the code**
   - Grab the latest ZIP at `https://github.com/sschritt/WebSecBot` and extract it somewhere
2. **Install dependencies & build**

```
npm install          # fetch packages (~1 min)
npm run build        # outputs the 'build/' folder
```

3. **Load the unpacked extension in Chrome**
   - Open `chrome://extensions/`
   - Toggle *Developer mode* (top-right)
   - Click *Load unpacked* and select the `build` folder created in the previous step
   - The WebSecBot icon now appears in the toolbar

2.4 Point WebSecBot at AnythingLLM

Open the WebSecBot settings panel (gear icon) and fill in the connection details:

Field	Value to enter
Endpoint / Base URL	`http://localhost:3001/api/v1/workspace/my-workspace/chat`
Model name	`my-workspace`
API key	paste the Developer key you generated earlier

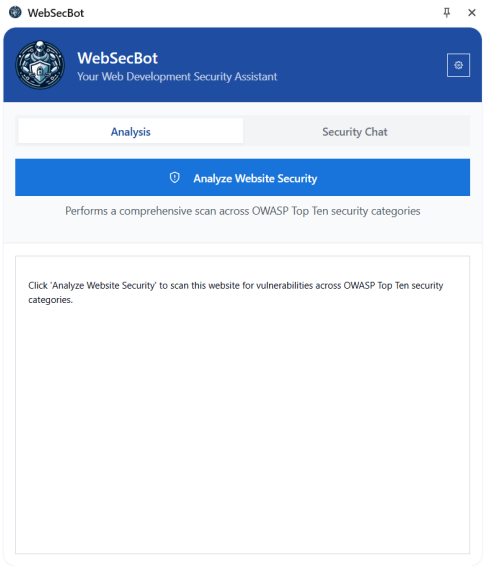
Note: The default settings now use "my-workspace" (lowercase) as the model name and endpoint includes the workspace name. Make sure your workspace name in AnythingLLM exactly matches "My Workspace" (with capitals) for the default settings to work correctly.

Click *Save*. Reload the web page you want to test and press *Analyse Website Security*–a report should appear within seconds.

3 Using WebSecBot

3.1 User Interface Overview

After installation, WebSecBot integrates into your browser with a sleek side panel interface:



The main components are:

- **WebSecBot Icon**: Located in your browser toolbar, click to open the side panel
- **Analysis Tab**: For running security scans on websites
- **Security Chat Tab**: For interacting with the AI assistant
- **Settings**: Configure the extension and backend connection

Tip: For best results, ensure you're on the main page of the website you want to analyze, or the specific page you're concerned about testing.

3.2 Running a Security Analysis

You can analyze any website by:

1. Navigating to the website in your Chrome browser
2. Opening WebSecBot by clicking its icon in the toolbar
3. Selecting the "Analysis" tab
4. Clicking "Analyze Website Security"

The extension will scan the current page and any accessible resources, checking for common security vulnerabilities based on the OWASP Top Ten security framework.

Behind the Scenes: WebSecBot examines multiple aspects of the web page including forms, inputs, headers, scripts, meta tags, and potential sensitive directories. This comprehensive data collection enables detailed security analysis.

3.3 Understanding the Analysis Results

After the analysis completes, you'll see a comprehensive report structured by security categories. The report includes:

1. **Executive Summary**: An overview of the security posture with key findings highlighted
2. **Category Sections**: Detailed findings organized by security categories such as:
   - Broken Access Control
   - Injection Vulnerabilities
   - Cryptographic Failures
   - Security Misconfigurations
   - Vulnerable & Outdated Components
3. **Prioritized Remediation Plan**: Recommendations for addressing findings in order of importance
4. **Additional Security Recommendations**: General best practices to improve security

Each finding includes:

- Description of the issue
- Evidence found on the page
- Criticality level (High/Medium/Low)
- Explanation of the security implications
- Recommendations for fixing the issue

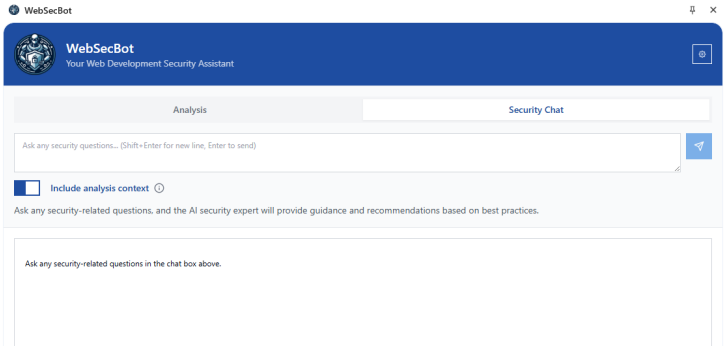
3.4 Using the Security Chat Feature

WebSecBot provides an AI-powered security chat assistant that offers two distinct modes of operation to help you understand and address security concerns.

3.4.1 Chat with Analysis Context

This mode connects your security analysis results directly to the AI assistant, allowing for highly specific guidance about your website:

1. Click the "Security Chat" tab
2. Ensure "Include analysis context" is toggled ON (the toggle will appear blue when enabled)
3. Ask security-related questions in the chat box
4. The AI will respond with insights based on the analysis results



What is Analysis Context? When this option is enabled, WebSecBot feeds your previous security analysis results to the AI assistant as context. This means the AI can "see" all the vulnerabilities detected on your website and provide answers that are specifically tailored to your situation. This feature essentially gives the AI assistant detailed knowledge about your website's security posture.

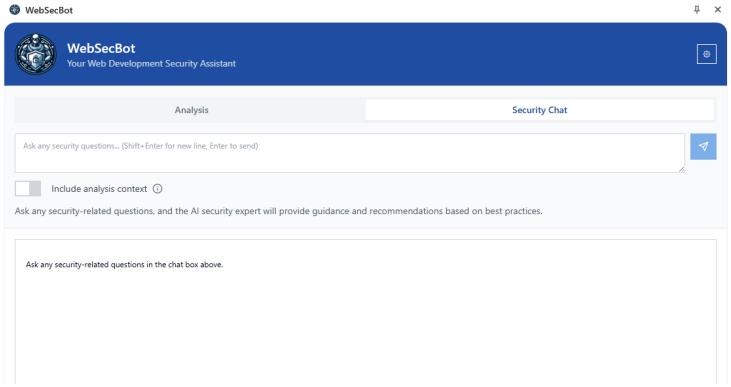
In this mode, the AI assistant can:

- Reference specific vulnerabilities found in your website
- Prioritize advice based on the severity of detected issues
- Provide code examples tailored to your website's technology stack
- Explain the technical details behind identified security problems
- Suggest precise remediation steps for your specific situation

3.4.2 General Security Chat

For broader security education or questions not directly related to your current analysis:

1. Click the "Security Chat" tab
2. Toggle "Include analysis context" to OFF (the toggle will appear gray when disabled)
3. Ask any security-related questions
4. The AI will provide general security guidance based on best practices



When to Use General Chat: Use this mode when you want to learn about security concepts that might not be directly related to your current website, or when you want to explore broader security topics. Without analysis context, the AI provides more general knowledge but can cover a wider range of topics.

In this mode, the AI assistant can:

- Explain security concepts and best practices
- Provide educational content about different types of vulnerabilities
- Offer general implementation advice for security controls
- Discuss emerging security threats and trends
- Help with understanding security terminology and standards

Note: The "Include analysis context" option will be disabled (grayed out) if you haven't performed an analysis yet. You'll need to run a security analysis first before this feature becomes available.

4 Sample Workflows

4.1 Example Scenario: Finding and Fixing Security Vulnerabilities

Here's a typical workflow for using WebSecBot to improve your web application's security:

1. **Initial Analysis**:
   - Open your web application in Chrome
   - Run a WebSecBot analysis
   - Review the Executive Summary to understand the overall security posture
2. **Exploring Findings**:
   - Examine each category of findings
   - Note the criticality levels to prioritize your efforts
   - Review the detailed explanations to understand the issues
3. **Getting Implementation Guidance**:

- Switch to the Security Chat tab
- Ensure "Include analysis context" is ON
- Ask specific questions about the findings

4. **Implementing Fixes**:
   - Follow the recommendations provided in the analysis and chat
   - Apply the suggested code changes to your application
   - Re-run the analysis to verify improvements

4.2 Effective Questions to Ask with Analysis Context

After running an analysis, try questions like these in the chat with analysis context enabled:

- "Can you explain the most serious security findings in simple terms and how they might impact my website?"
- "What's the easiest security improvement I can implement that would have the biggest impact?"
- "Can you create a detailed step-by-step action plan to address these security issues with clear examples?"
- "Can you provide sample code for implementing the security fixes you recommended?"
- "How can I test if my security fixes are working properly?"
- "What ongoing security monitoring should I set up after implementing these fixes?"
- ...

These are just examples - feel free to ask any security-related questions about your analysis results.

4.3 General Security Questions (Without Analysis Context)

When you need general guidance not related to a specific analysis, toggle off analysis context and try questions like:

- "What are the OWASP Top 10 vulnerabilities and how can I prevent them?"
- "How do I implement proper input validation for a login form?"
- "What's the difference between authentication and authorization?"
- "Can you explain Cross-Site Scripting (XSS) and how to prevent it?"
- "What security headers should I implement on my website?"
- "How should I securely store user passwords in my database?"

5 Troubleshooting

5.1 Common Issues and Solutions

5.1.1 Analysis Not Starting

- **Error Message**: "Initializing comprehensive security analysis..." appears but doesn't progress
- **Solution**:
  1. Check if you have navigated to a valid website (error: "No webPageInfo found")
  2. Ensure the page is fully loaded before starting analysis
  3. Refresh the current web page and try again
  4. If the problem persists, check your connection to the LLM backend

5.1.2 API Connection Error

- **Error Message**: "Error with API" in console logs
- **Solution**:
  1. Verify your API key is correctly entered in the settings tab
  2. Confirm the API endpoint URL is accessible and properly formatted
  3. Check the browser console for detailed error messages
  4. Verify your AnythingLLM instance is running and accessible
  5. Ensure your model name matches exactly with your workspace name

5.1.3 No Response from Security Chat

- **Error Message**: "Failed to get response from the security expert"
- **Solution**:
  1. Check your internet connection
  2. Verify the LLM backend service is running
  3. Try sending a shorter, simpler message
  4. Restart the extension by closing and reopening the side panel
  5. Check if your API credentials have expired or reached usage limits

6 Privacy and Data Handling

WebSecBot is designed with privacy in mind:

- When using external LLM providers like Groq, your website data is processed according to their privacy policies. The specific data categories sent include:
  - HTML forms and input fields from the current page
  - Security headers from the web response
  - Website URLs and paths being analyzed
  - Meta tags and script snippets (first 500 characters only)
  - Detected JavaScript patterns
  - Information about mixed content resources
  - Comments found in the HTML source

  - Results from directory/file path scans
  - Cookie strings (without values)

- The WebSecBot Chrome extension processes website data only for the duration of your analysis and does not retain this data after you close the extension
- The extension does not track your browsing activity beyond the pages you explicitly analyze

Note on Data Privacy: WebSecBot sends page content to the LLM for analysis. If you're testing sensitive applications, consider using a self-hosted LLM solution to keep all data within your control.

7 Additional Resources

- WebSecBot GitHub Repository: https://github.com/sschritt/WebSecBot
- netidee Project Page: https://www.netidee.at/websecbot
- OWASP Top Ten Project: https://owasp.org/www-project-top-ten/
- OWASP Web Security Testing Guide: https://owasp.org/www-project-web-security-testing-guid