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 browser

- Internet connection
- No additional software required for basic usage

2.2 Installing the WebSecBot Chrome Extension

1. **Download the Extension**:
   - Visit the WebSecBot GitHub repository at https://github.com/sschritt/WebSecBot
   - Download the latest release ZIP file
   - Extract the ZIP file to a location on your computer
2. **Install in Chrome**:
   - Open Google Chrome
   - Navigate to `chrome://extensions/`
   - Enable "Developer mode" by toggling the switch in the top-right corner
   - Click "Load unpacked"
   - Select the folder where you extracted the WebSecBot files
   - The WebSecBot icon should now appear in your browser toolbar

2.3 Configuring Your LLM Backend

WebSecBot requires connection to a Large Language Model (LLM) backend to provide AI-powered analysis. The recommended setup uses AnythingLLM, which allows you to either use external API providers or run models locally.

2.3.1 Setting Up AnythingLLM

We recommend setting up AnythingLLM as your backend:

1. Install AnythingLLM on your server or local machine
   - Follow installation instructions at https://github.com/Mintplex-Labs/anything-llm
   - You can use the desktop application version for Windows, Mac, or Linux
2. Configure AnythingLLM:
   - Launch AnythingLLM (it typically runs on port 3001)
   - Go to Settings → LLM Preferences
   - Set up your preferred LLM provider:
     - For external API: Select Groq, OpenAI, or another provider
     - For local models: Select Ollama or another local option
3. Create a dedicated workspace for WebSecBot:
   - In AnythingLLM, go to "Workspaces" and click "Create New Workspace"
   - Name your workspace (e.g., "WebSecBot")
   - This workspace name will be needed when configuring the extension

Model Recommendation: Our testing shows that Llama 3.3 70B versatile (through 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.

2.3.2 Enhancing Analysis with RAG

For better security analysis capabilities, enable Retrieval Augmented Generation (RAG) by importing the WebSecBot security document collection:

1. Download the OWASP security document collection:
   - Get the files from the `OWASP-Resources` folder in the WebSecBot GitHub repository
   - These documents contain structured security knowledge that helps the LLM make better assessments
2. Import the documents into AnythingLLM:
   - In your WebSecBot workspace, click "Add Documents"
   - Upload the OWASP security document files you downloaded
   - Wait for processing to complete (the documents will be vectorized)
3. Verify RAG is enabled:
   - In workspace settings, ensure "Include documents in chat context" is enabled
   - This ensures the security knowledge is used during analysis

2.3.3 Connecting WebSecBot to AnythingLLM

Important: The extension comes with default values for the API endpoint and model name. You must change these in the util file to match your specific AnythingLLM setup for the extension to work properly.

After setting up AnythingLLM, connect your WebSecBot extension:

1. In the WebSecBot extension, click the settings icon
2. Configure the following fields:
   - **API Key**: Enter "sk-1234" (the default key) or your custom API key if you've changed it in AnythingLLM
   - **API Endpoint URL**: Enter the full path to your AnythingLLM instance followed by the OpenAI-compatible endpoint (e.g., `http://localhost:3001/api/v1/openai/chat/completions`)
   - **Model Name**: Enter the exact name of your workspace as created in AnythingLLM (e.g., `WebSecBot`)
3. Click "Save Settings"

Using Groq with AnythingLLM: If you prefer using Groq's API through AnythingLLM for faster inference:

1. In AnythingLLM, go to Settings → LLM Preferences
2. Select "Groq" as your provider

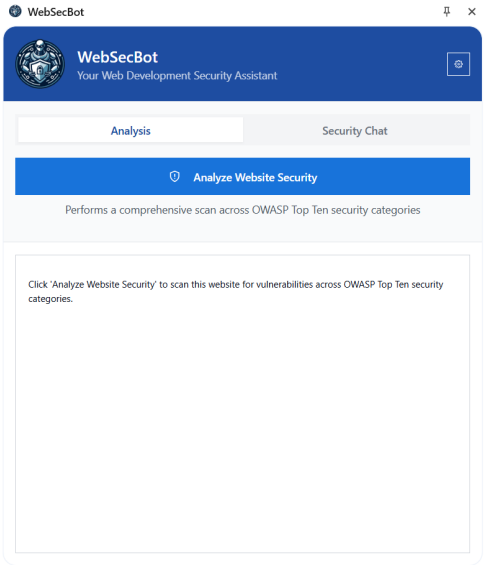
3. Enter your Groq API key (obtain from https://console.groq.com/keys)
4. Choose your preferred model
5. Save your settings

Then connect WebSecBot to your AnythingLLM instance as described above.

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

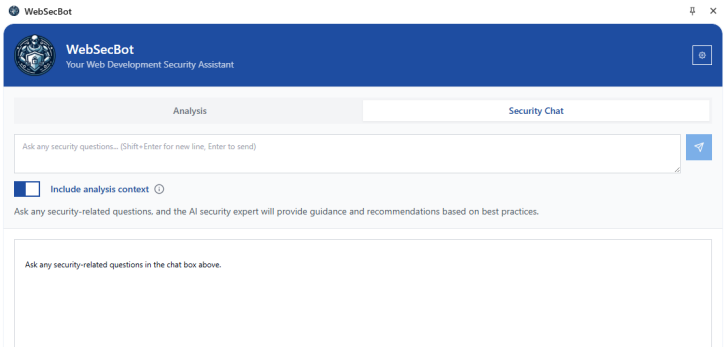
3.4 Using the Security Chat Feature

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.

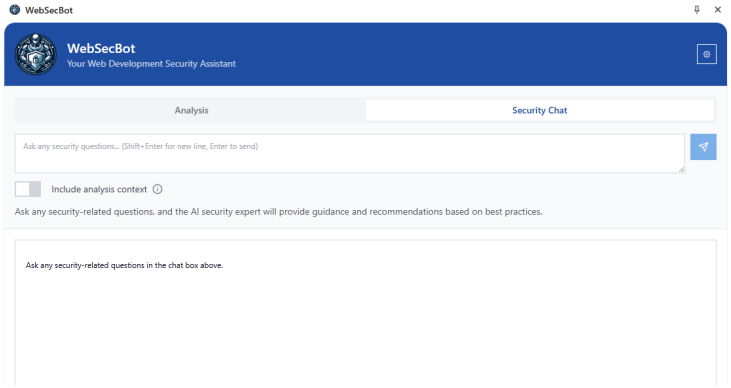
In this mode, the AI assistant can:

- 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