# NetShield Web Application Security Scanner

NetShield is a cutting-edge web security scanner designed to identify vulnerabilities within websites and web applications. This tool is developed with the aim of providing users, from beginners to advanced security professionals, a comprehensive and user-friendly platform for conducting thorough and effective web security assessments. NetShield helps to protect websites against a wide range of security threats, ensuring the integrity, confidentiality, and availability of web-based resources.

How to Use NetShield
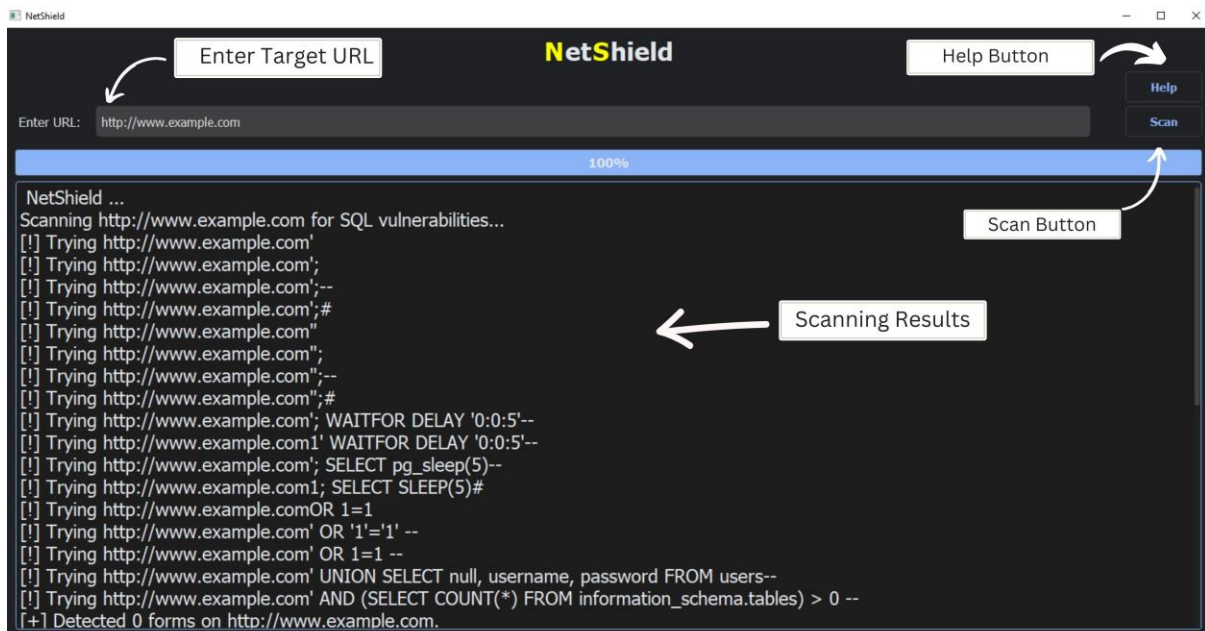
Step 1: Launch NetShield

- Start NetShield on your computer. You should see the main interface as shown in the screenshot.

Step 2: Enter Target URL

- Locate the "Enter URL" field at the top of the interface.

- Type in or paste the URL of the web application you wish to scan. Ensure the URL is correct to avoid scanning the wrong site.

Step 3: Initiate the Scan

- Once the URL is entered, find the "Scan" button located towards the right-hand side of the interface, near the top.

- Click on the "Scan" button to start the scanning process. NetShield will begin to assess the specified web application for vulnerabilities.

Step 4: Monitor Scanning Progress

- After initiating the scan, observe the progress bar at the top of the scanning results area. The progress bar will fill up, indicating the percentage of the scan that has been completed.

- Below the progress bar, NetShield will display real-time scanning results, including the tests it's performing and any vulnerabilities detected.

Step 5: Review Scanning Results

- As the scan progresses, you'll see a detailed list of actions taken and vulnerabilities found in the "Scanning Results" area. Each entry will include the type of test performed and its outcome.

- For SQL vulnerabilities, for example, you might see attempts to inject SQL commands and the responses from the web application.

- Pay special attention to any detected vulnerabilities, noted by specific alerts or messages in the results area.

Step 6: Analyze and Act on Findings

- Upon completion of the scan, review all identified vulnerabilities. NetShield may provide information on the vulnerability type, its location within the application, and potential impact.

- Consult the detailed scan report (if available) for recommendations on how to address each vulnerability. This may involve code changes, configuration updates, or applying patches.

Additional Features

- If you need help or further information on specific features or findings, use the "Help" button located at the top right corner of the interface. This provide access to Netshield webpage to help.

Step 7: Rescan if Necessary

- After addressing the vulnerabilities identified by NetShield, it's a good practice to run the scanner again to ensure all issues have been adequately resolved.

- Repeat the scanning process as needed to maintain the security of your web application.