




Submit #562383: handrew browserpilot 0.0 Code Injection

Title handrew browserpilot 0.0 Code Injection

Description browserpilot is an intelligent web browsing agent controlled by natural language with LLM.. The `__run_compiled_instructions` function in the `GPTSeleniumAgent` class of the BrowserPilot project is affected by a code injection vulnerability (CWE - 94). This function utilizes the `exec()` method to run the `instructions` parameter sourced from the `InstructionCompiler`. However, there is no proper verification of these instructions. Attackers can manipulate the input fed into the `InstructionCompiler`, causing malicious Python code to be injected into the `instructions` variable. When `exec()` is executed, this malicious code will run within the program's context. This can lead to severe security issues like unauthorized access to system resources, data leakage, and system compromise. All versions of the project are impacted.

More details: <https://github.com/handrew/browserpilot/issues/20>

Source  <https://github.com/handrew/browserpilot/issues/20>

User  ybdesire (UID 83239)

Submission 04/19/2025 02:09 PM (14 days ago)

Moderation 05/02/2025 02:55 PM (13 days later)

Status Accepted

VulDB Entry 307195 [handrew browserpilot up to 0.2.51 gpt_selenium_agent.py GPTSeleniumAgent instructions code injection]

Points 20

Notice

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling