COMMUNITY CONTENT

Submit #784052: Fosowl agenticSeek 0.1.0 Remote Code Execution

Title	Fosowl agenticSeek 0.1.0 Remote Code Execution
Description	AgenticSeek (versions 0.1.0) allows unauthenticated Remote Code Execution (RCE) via the /query endpoint. The application fails to sandbox LLM-generated code across multiple interpreters.The optional safe_mode is disabled by default and relies on a flawed keyword blocklist that is easily bypassed due to implementation errors and a lack of path-based filtering.
Source	https://github.com/August829/CVEP/issues/29
User	Yu Bao (UID 88956)
Submission	03/20/2026 10:24 AM (16 days ago)
Moderation	04/04/2026 11:31 PM (16 days later)
Status	Accepted
VulDB entry	[Fosowl agenticSeek 0.1.0 query Endpoint PyInterpreter.py PyInterpreter.execute code injection]
Points	19

Community Content

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