MervinPraison / **PraisonAI** Public

Code | Issues 56 | Pull requests 3 | Discussions | Actions | Projects

Commit `0accebb`

MervinPraison committed 5 days ago · ✕ 6 / 13

```
refactor: harden sqlite identifier validation
```

main · v4.6.2 ••• v4.5.133

1 parent 757559f commit 0accebb

3 files changed +10 -3 lines changed

Top

Filter files…

- .github
  - praisonai-issue-triage.yaml
- src/praisonai/praisonai
  - gateway
    - server.py
  - persistence/conversation
    - sqlite.py

3 files changed +10 -3 lines changed

Search within code

.github/praisonai-issue-triage.yaml

```
@@ -40,7 +40,7 @@ steps:
40 40        action: |
41 41          Implement the changes required to solve the issue:
42 42          1. Review the analyst's plan.
43    -        2. Check out a dedicated fix branch by calling `execute_command` with `command` set to `git checkout -b praisonai/issue-$ISSUE_NUMBER`. Do NOT provide a `cwd` argument.
```

```
      43 +       2. Check out a dedicated fix branch by calling `execute_command` with `command` set to `git checkout -b praisonai/issue-{{ISSUE_NUMBER}}`. Do NOT provide a `cwd` argument.
44    44         3. Carefully modify the necessary files in the repository using bash commands (e.g. `cat`, `sed`, `echo`, or small inline scripts).
45    45         4. Double-check your edits by inspecting the file outputs or running `git diff` to ensure you changed what was required.
46    46       expected_output: "Confirmation that the git branch was successfully created and the files were reliably modified without syntax errors."
          @@ -52,7 +52,7 @@ steps:
52    52         1. Stage the files with `execute_command` where `command` is `git add .`. Do NOT provide a `cwd` argument.
53    53         2. Commit the changes: `git commit -m "PraisonAI Automated Fix"`
54    54         3. Push the branch to GitHub: `git push -u origin HEAD`
55        -       4. Create the Pull Request back to main: `gh pr create --title "Fix Issue $ISSUE_NUMBER" --body "Automated triage by PraisonAI Native Issue Triage." --head "praisonai/issue-$ISSUE_NUMBER" --base main`
56        -       5. Post a comment on the original issue letting the user know: `gh issue comment $ISSUE_NUMBER -b "I have autonomously analyzed the codebase and written a fix for this issue! I've opened a Pull Request for your review."`
      55 +       4. Create the Pull Request back to main: `gh pr create --title "Fix Issue {{ISSUE_NUMBER}}" --body "Automated triage by PraisonAI Native Issue Triage." --head "praisonai/issue-{{ISSUE_NUMBER}}" --base main`
      56 +       5. Post a comment on the original issue letting the user know: `gh issue comment {{ISSUE_NUMBER}} -b "I have autonomously analyzed the codebase and written a fix for this issue! I've opened a Pull Request for your review."`
57    57       expected_output: "The URL of the successfully created Pull Request."
58    58       dependencies: [analyze_issue, implement_fix]
```

src/praisonai/praisonai/gateway/server.py

```
          @@ -203,6 +203,7 @@ def __init__(
203   203           """
204   204           self.config = config or GatewayConfig(host=host, port=port)
205   205           if hasattr(self.config, 'auth_token') and not self.config.auth_token:
      206 +             import secrets
206   207               self.config.auth_token = secrets.token_hex(16)
207   208               logger.warning(
208   209                   f"No auth_token provided for Gateway server. Generated temporary token: {self.config.auth_token}. "
```

...raisonai/persistence/conversation/sqlite.py

```
@@ -46,6 +46,12 @@ def __init__(
46 46              check_same_thread: SQLite check_same_thread parameter
47 47          """
48 48          self.path = path
   49 +
   50 +         # Prevent SQL injection in table identifiers
   51 +         import re
   52 +         if not re.match(r'^[a-zA-Z0-9_]*$', table_prefix):
   53 +             raise ValueError("table_prefix must contain only alphanumeric characters and underscores")
   54 +
49 55          self.table_prefix = table_prefix
50 56          self.sessions_table = f"{table_prefix}sessions"
51 57          self.messages_table = f"{table_prefix}messages"
```

Comments 0

Please sign in to comment.