

fix security issue with url parsing #1561

New issue

🔗 Merged

pirate merged 2 commits into `main` from `security-fix` 📄 yesterday


💬 Conversation 1

🔗 Commits 2

📄 Checks 39

📄 Files changed 2

+26 -6 🟢🟢🟢🟢🟢

 **pirate** commented yesterday • edited ▾ Member

Fixes <https://github.com/browser-use/browser-use/security/advisories/GHSA-x39x-9qw5-ghrf>

Read + run the test to verify it: `uv run pytest tests/test_url_allowlist_security.py`

Specifically verifies that URLs with authentication credential-based bypass attempts are properly detected and disallowed, including:

1. <https://example.com:password@malicious.com> - Using the colon in the example.com domain to trick the URL parser
2. <https://example.com@malicious.com> - Using example.com as a username
3. <https://example.com%20@malicious.com> - Using URL-encoded space character to bypass checks
4. <https://example.com%3A@malicious.com> - Using URL-encoded colon character to bypass checks



All these malicious URLs are now properly detected as non-allowed URLs, while legitimate credentials like <https://user:password@example.com> still work correctly.

Summary by mrge

Fixed a security issue where URLs with embedded credentials or encoded characters could bypass domain checks. Now, only the actual hostname is used for validation, blocking malicious URL formats.

- **Bug Fixes**

Reviewers

 **mrge-io[bot]** 

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone



Development

Successfully merging this pull request may close these issues.

None yet

1 participant

- Blocks URLs like <https://example.com:password@malicious.com> and similar tricks.
- Legitimate credentials (e.g., <https://user:password@example.com>) still work.

  fix security issue with url parsing Unverified ✓ ebdeb61

  **pirate** enabled auto-merge yesterday

  **pirate** disabled auto-merge yesterday




 **mrge-io** bot reviewed yesterday [View reviewed changes](#)


mrge-io bot left a comment


mrge reviewed 1 file and found no issues. Review this PR in mrge.io.

  add test Unverified ✓ 3a1fa0f

 **pirate** merged commit **cd2fc91** into main [View details](#)
yesterday
39 checks passed

  **pirate** deleted the security-fix branch yesterday

 **dharam1291** pushed a commit to dharam1291/browser-use that referenced this pull request yesterday

 fix security issue with url parsing 425ed86
([browser-use#1561](#))