Clickjacking Vulnerability Report - Planka v2.0.0-rc.4

Discovered by

Sunhawat Sremeesub

VULNERABILITY SUMMARY:

- Type: Clickjacking (UI Redressing Attack)
- Severity: Medium
- Affected Version: Planka v2.0.0-rc.4
- Root Cause: Missing X-Frame-Options and CSP frame-ancestors headers

IMPACT:

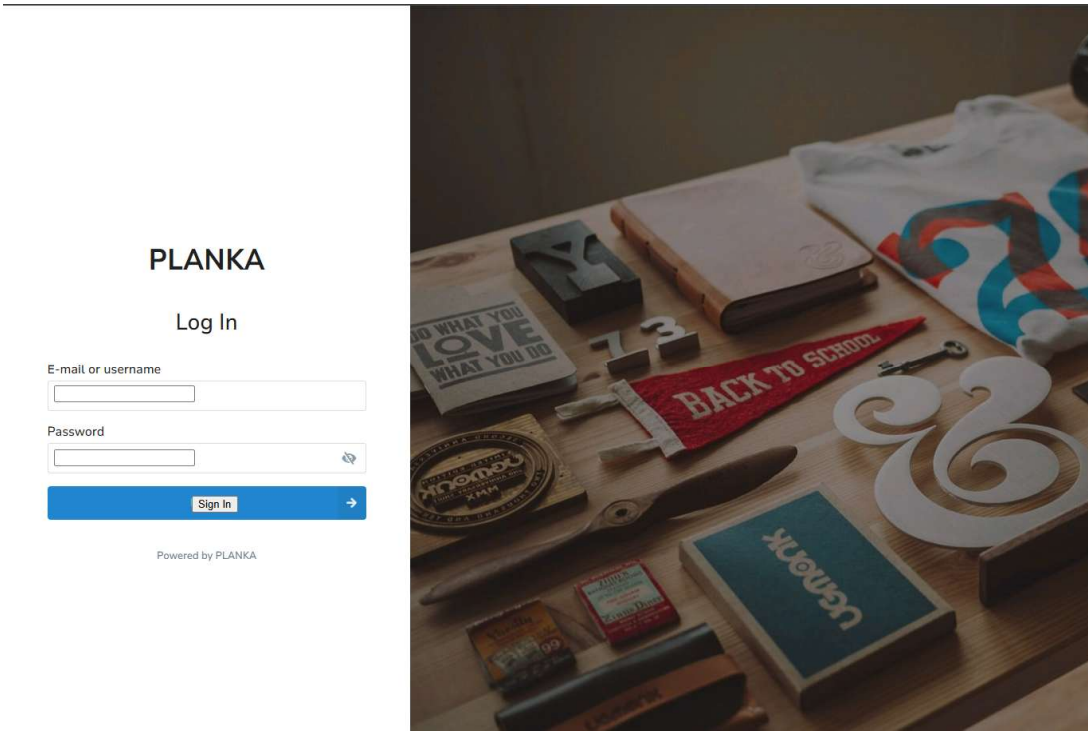
PLANKA 2.0.0 lacks `X-Frame-Options` and CSP `frame-ancestors` headers, allowing the application to be embedded within malicious iframes. **While this does not lead to unintended modification of projects or tasks, it exposes users to Phishing attacks.** Attackers can frame the legitimate Planka application on a malicious site to establish false trust (UI Redressing), potentially tricking users into entering sensitive information or credentials into overlaid fake forms.

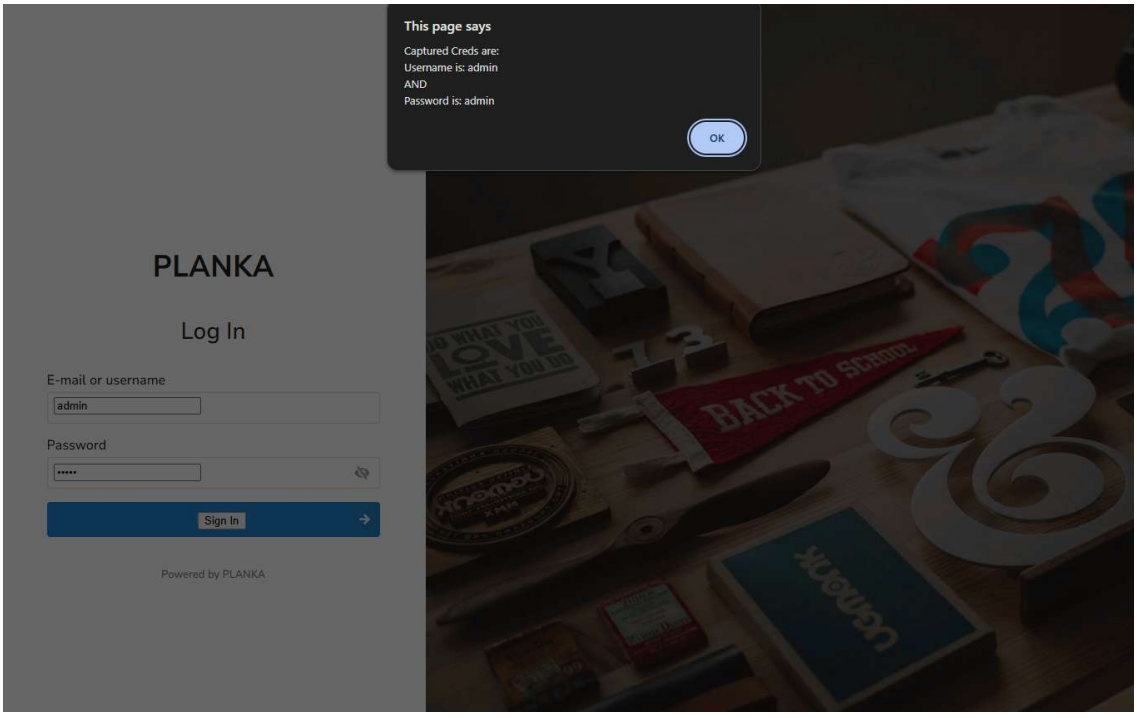
RECOMMENDED FIX:

Implement the following security headers:

- X-Frame-Options: DENY (or SAMEORIGIN)
- Content-Security-Policy: frame-ancestors 'self' (or 'none')

Proof of concept





Tools

https://github.com/sensepost/jack.git

https://github.com/plankanban/planka.git