

## [Security] Stored XSS #38



edoardottt commented on Sep 19 • edited ▼

Tested version: 8c2c8909 (latest)

Steps to reproduce the vulnerability:

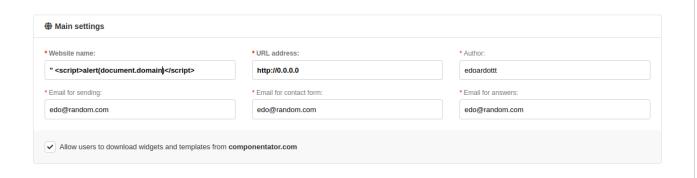
• Login in the application.

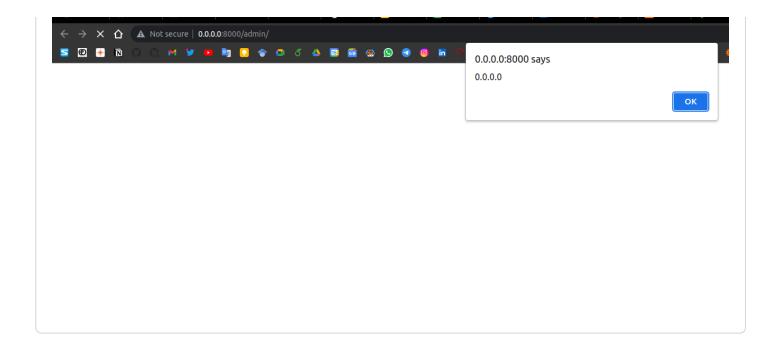
• Set " <script>alert(document.domain)</script> as website name.

- Fill other required fields with random values and save.
- Then just visit the admin dashboard and the alert will fire.

Each time a target will visit the dashboard the payload will fire, even if the target is not logged in! Since the wesbite redirects to /admin/ presenting the login form, but the payload is reflected also there.

In order to test this, just click logout and reload the page.





edoardottt closed this as completed on Sep 22

Assignees	
No one assigned	
Labels	
None yet	
Projects	
None yet	
Milestone	
No milestone	
Development	
No branches or pull requests	



