Project Proposal

Team Spark

Karthik Venkatesh
Mohan Ambati
Sai Guru Karthik Damuluri

Ghost (https://github.com/TryGhost/Ghost)

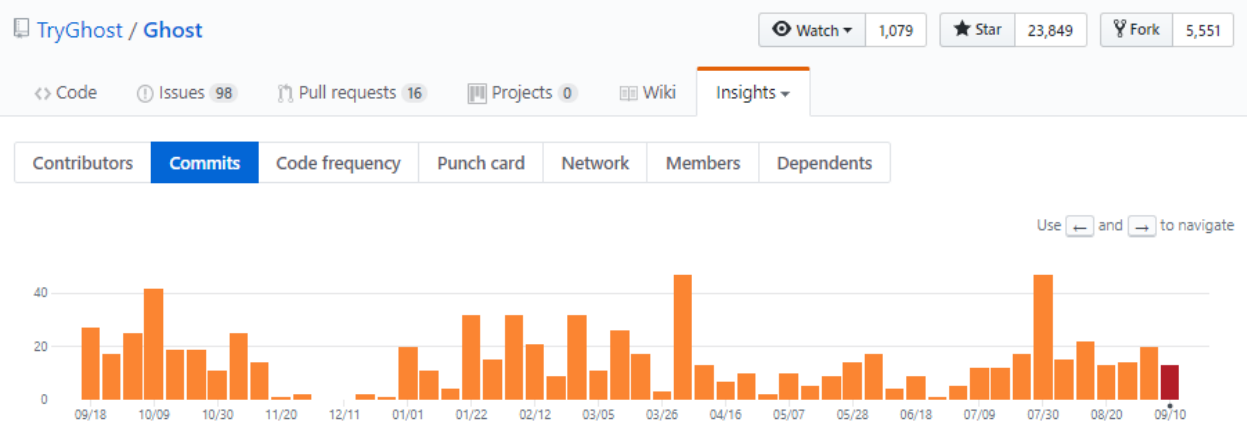
Ghost is a modern, open source publishing platform built on Node.js with an Ember.js admin client, a JSON API, and a theme API powered by Handlebars.js. Its default database is MySQL, connected via Bookshelf as an ORM layer - so other databases can also be used.

Ghost simplifies the process of online publishing for individual bloggers as well as online publications, it is a best open source tools for independent journalists and writers across the world, and have a real impact on the future of online media.

It is currently in production and used by popular companies like bitcoin, NASA, mozilla, coinbase, AngelList, Square, Zappos, brave, BIGCOMMERCE.

Contributors: 273 contributors

Activity: Highly Active



Languages Used: JavaScript, Html

Documentation Sources:

https://docs.ghost.org/docs
https://github.com/TryGhost/Ghost/wiki

Motivation

The Ghost is a famous content management system, used by major publishing companies to publish their daily articles. We were interested to take Ghost as we wanted to learn the vulnerabilities that are associated with a content management system. We were curious how sensitive data could be exploited by any attacker or in this case a rival publisher.

License

Procedure for making Contributions

GitHub issue tracker and submitting pull requests are the channels used for Reporting bugs and change requests.
Please find more information about the contribution in the link below.
https://docs.ghost.org/v1/docs/contributing

Contributor Agreement

By contributing your code to Ghost you grant the Ghost Foundation a non-exclusive, irrevocable, worldwide, royalty-free, sub licensable, transferable license under all of Your relevant intellectual property rights (including copyright, patent, and any other rights), to use, copy, prepare derivative works of, distribute and publicly perform and display the Contributions on any licensing terms, including without limitation: (a) open source licenses like the MIT license; and (b) binary, proprietary, or commercial licenses. Except for the licenses granted herein, You reserve all right, title, and interest in and to the Contribution

Security Related History

- Ghost blog fails RSS validation and cannot be parsed by some utilities and syndications
- When RSS is accessed over SSL the title feed should appropriately link to HTTPS, but the links to the posts and images are pointing to HTTP
- Ghost using Public API, where the Public API injects inline scripts into page which results to XSS
- Sign-in fails after redirection from an authenticated route - Login authentication failure

Functional Security Requirements

Login Authentication

Necessary Login authentication has to be given to a user, so that he can login to his publication dashboard only.

Session Management

The browser session has to be managed between the client and the ghost server to avoid any session hijacking.

Role Permissions

The Appropriate permissions must be assigned to the users, to avoid leaking of sensitive data and unnecessary modifications to the publication. Different roles included here are Author, editor, administrator and owner.

Ensure API Authentication

The system must ensure API authentication to avoid security attacks and vulnerabilities from third party API integration.
API Authentication must follow the token bearer authentication process.

Application should handle critical risks

The system should handle script injection in input fields and avoid XSS scripting and code injection.

Error Handling

The system should handle all types of error by throwing appropriate errors.

GitHub Repository, Project Plans and Collaboration

Since we are new to GitHub, we wanted to make our project code repository separate from our working repositories to reduce merge conflicts and collaboration errors.

Please find the workflow of our team explained more detailed in below link.
https://github.com/teamsparkuno/Ghost/blob/master/teamspark_collabration