Naughty or nice: security vulnerabilities

Posted on December 9, 2025

> You should probably read " Plugin development with KTD - your complete toolkit" before this if you haven't already.

The Koha community is a very nice place composed of individuals and organisations from all around the planet coming together for a common good: the open source Koha web application. Unfortunately, Koha also exists in a global technology space where there are naughty people who want to abuse online systems. The way these people perform malicious actions is by exploiting security vulnerabilities.

What is a security vulnerability?

Any time a user can perform an action that they should not otherwise be authorised to do, you have a security vulnerability.

This might mean that they can access someone else's personal information, they might be able to perform a web action in Koha that they shouldn't be able to perform, they might be able to get arbitrary code to execute on the server or in the database, they might be able to get Javascript to execute in someone else's browser, et cetera.

How do I find a security vulnerability?

Typically, security vulnerabilities are either found by accident or by someone specifically testing the security.

If you are a Koha web user or developer, you might notice that you can perform an action that you wouldn't normally be allowed to do. Rather than ignore it, you should tell someone about it.

If you are a manager or director of a library using Koha, you might hire a security consultant or request your IT department to do penetration testing. Security consultants will typically spend one or more days testing your system, and present a report at the end listing any security vulnerabilities, their severity, and steps for reproducing them.

How do I report a security vulnerability?

Regardless of how you find a security vulnerability, the process for reporting it is always the same.

You go to the Koha Community website and follow the instructions at this URL: https://koha-community.org/security/. Alternatively, review the SECURITY.md document in Koha's git repository, and follow the steps there.

Note that the only people who initially see your report are you and the Koha security team. However, eventually once the security vulnerability is fixed, your report will be made public, so be careful about what information you provide in your report. Do not include anything that you would not want the world to see later. If the security team need more information, they can request it after your initial report submission.

What happens next?

After you report the security vulnerability, the Koha security team will acknowledge it, try to reproduce it, and rate its severity.

If you are a developer, you can provide a patch yourself. Otherwise, the Koha security team will write a patch.

Once the patch is submitted, it goes through Koha's typical development process of testing and quality assurance (i.e. a team member tests the code, and then another team member provides a more in-depth review and test). Once it's been fully approved, the Release Manager and Release Maintainers work together to include the patch into the next month's Koha release.

Once the patch is pushed out to all the supported versions of Koha, the security report on Bugzilla becomes public and is treated like a normal bug report.

Finally, remember to be patient

While this process might sound easy, fast, and straightforward, sometimes there might be delays.

If delays occur, it is important to remember to be patient. Koha developers - even the Koha security team - volunteer their time to Koha. They are real people who are scattered across a range of timezones and must balance a number of responsibilities.

It is also possible that work is being done behind the scenes even if no new comments are added to Bugzilla. The security team might be discussing the bug behind the scenes, or they might be carefully coordinating the monthly release.

If you find that the process is not moving along, consider waiting a day or two. If there is no response, politely ask if there are any updates.

Written by David Cook, Prosentient Systems

← PREVIOUS POST

NEXT POST →