Escalating your privileges via open signups in popular services

BY BLACKBIRD-EU · JULY 4, 2024 · LAST UPDATED ON MARCH 6, 2025

Most software companies resort to using third-party solutions for completing certain tasks within their company. A common example is a ticketing platform that helps teams and companies stay organized with issues that internal employees or customers may experience.

Unfortunately, due to lack of time and strict deadlines, there's sometimes little to no room left for assessing the security impact of these services. And this can sometimes open up new attack surfaces for your business.

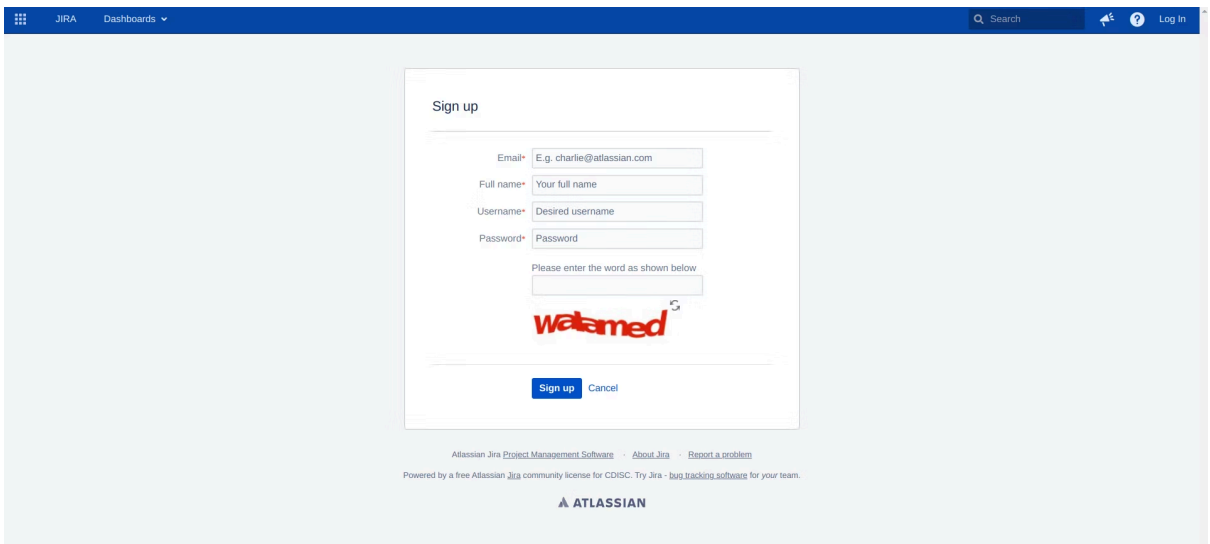
In this post, we'll go over three popular third-party software services that most (internal) software teams make use of. We'll explain thoroughly how they can lead to data theft, service disruption, or even financial damage when access to them is left incorrectly configured.

1) Atlassian Jira

Atlassian Jira is a popular ticketing software often used by developers and IT teams to keep track of internal issues.

However, if left configured incorrectly, it can be possible for anyone to sign up and create an account on your Atlassian Jira instance. Ultimately, allowing unauthorized users to get access to your internal data (depending on the privileges provided for new accounts).

To quickly check if your instance is currently configured incorrectly, navigate to `/secure/Signup!default.jspa` and check if signups are enabled.



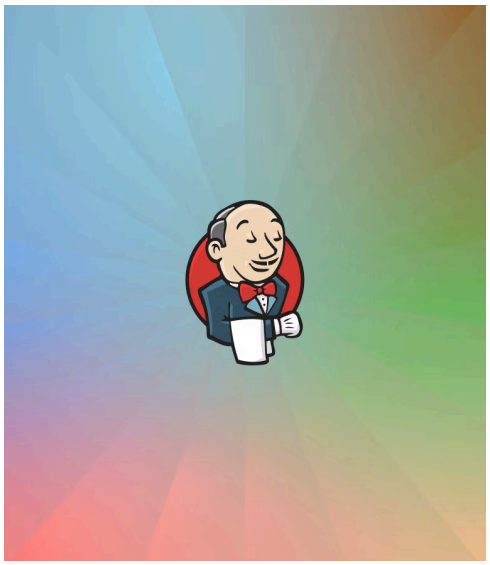
Follow the following remediation steps to disable public registrations in Atlassian Jira.

2) Jenkins

Jenkins is a popular continuous integration and continuous delivery (CI/CD) tool used by developers to help them build and deploy production-ready applications and web services at scale. It can save developers a lot of time. However, Jenkins also supports signups and if this setting is left incorrectly configured. It could open up another attack surface, allowing bad actors to gain access to your CI/CD pipeline(s).

You can easily check if your Jenkins instance has public signups enabled. Simply navigate to `/signup` or `/jenkins/signup` and verify if you can create an account.

If signups are open and you'd like to revert to this setting, simply follow [these remediation steps in Jenkins] to disable public signups. This would make sure that public signups are disabled by default.



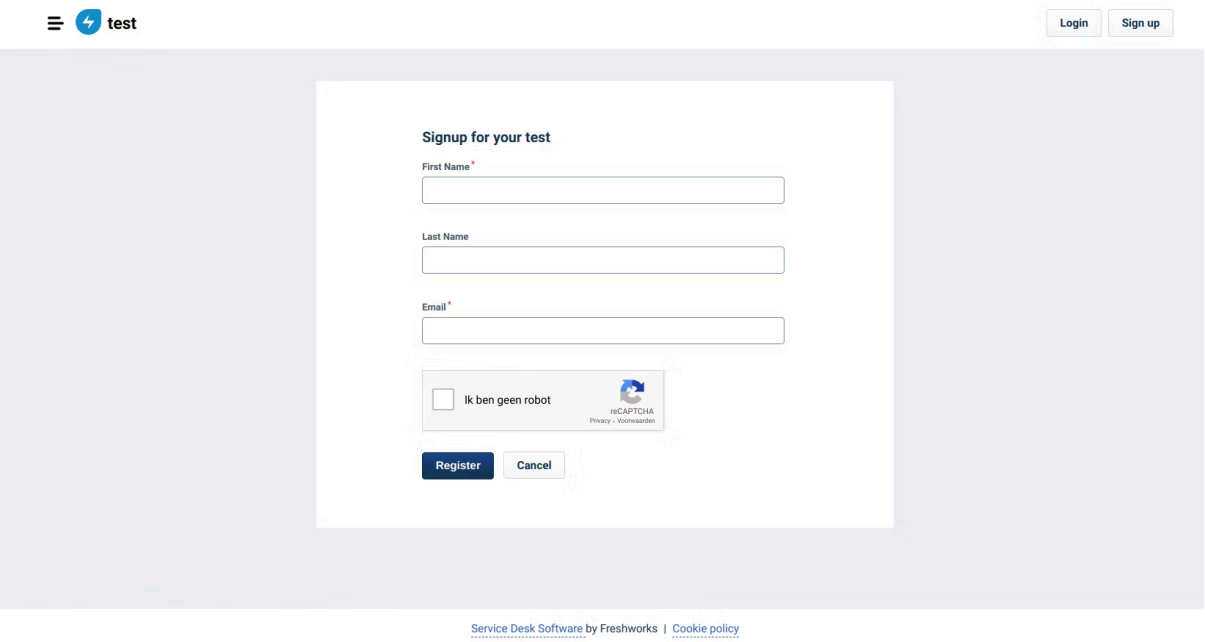
Jenkins Signup

3) Freshworks Freshservice

Freshworks Freshservice is a service management platform that helps businesses with ticketing, KB, and other services for its employees. By default, Freshservice allows anyone to create an account on your instance.

If you make use of Freshservice only for internal purposes, the best approach would be to disable public account creations. This, if not considered, may disclose sensitive data to unauthorized users.

A simple way of checking if signups are enabled is by visiting the following app route on your Freshservice instance: `/support/signup`



If registrations are left open to your Freshservice instance, it could mean that new users gain access to internal-only resources. Examples include internal support tickets, company business metrics, or even personal identifiable information (PII) of customers.

To disable signups on your instance, we recommend going through the following remediation steps for Freshservice.

Automated tooling

A while ago we released Misconfig Mapper, an automated tool dedicated to help find these types of security misconfigurations in popular third-party services such as the ones mentioned above.

Furthermore, we've also documented the potential impact it can bring and clear step-by-step guides on how to resolve these security misconfigurations.

Conclusion

Third-party solutions and cloud services can provide a lot of benefits to your team. However, can also be a means of opening new attack surfaces to your company or organization if incorrectly configured.

You've just learned how to find security misconfigurations in popular third-party services like Atlassian and Jenkins... Right now, it's time to put your skills to the test! Browse through our 70+ public bug bounty programs on Intigriti, and who knows, maybe your next bounty will be earned with us!

START HACKING ON INTIGRITI TODAY

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com