This is a public forum to discuss functional and technical questions about Axelor.

All **technical questions** should be posted on the technical English forum.

For **proven anomalies on the software**, please report it on our GitHub page : **Axelor GitHub for Axelor Open Suite**

For **proven anomalies on the Axelor Open Platform**, please report it on our GitHub page : **Axelor GitHub for Axelor Open Platform**

Please review the :

- **FAQ/Guidelines**

/!\ Vuln sur axelor (je suis gentil)

ArianeBlow Ariane **8 févr.**

Coucou,

J'ai des vulns sur axelor à vous transmettre OU à fair enregistrer par MITRE (c'est au choix lol).

Ou je peux vous envoyer ça ? (La partie sécu de Github est just VIDE !)

Parce que bon, je voulais tester la solution sur mon tomcat pour gérer un peu mes petites affaires et j'ai donc naturellement voulu tester un peu les inputs (on ne se refais pas !). Et j'ai trouver de la XSS stocké de partout lol.

Merci

@+

Ariane.

---

admin Administrator **10 févr.**

Nous vous remercions pour votre aide nous allons prendre contact avec vous afin d'étudier les éventuelles failles trouvées.
Bien cordialement,
L'équipe Axelor

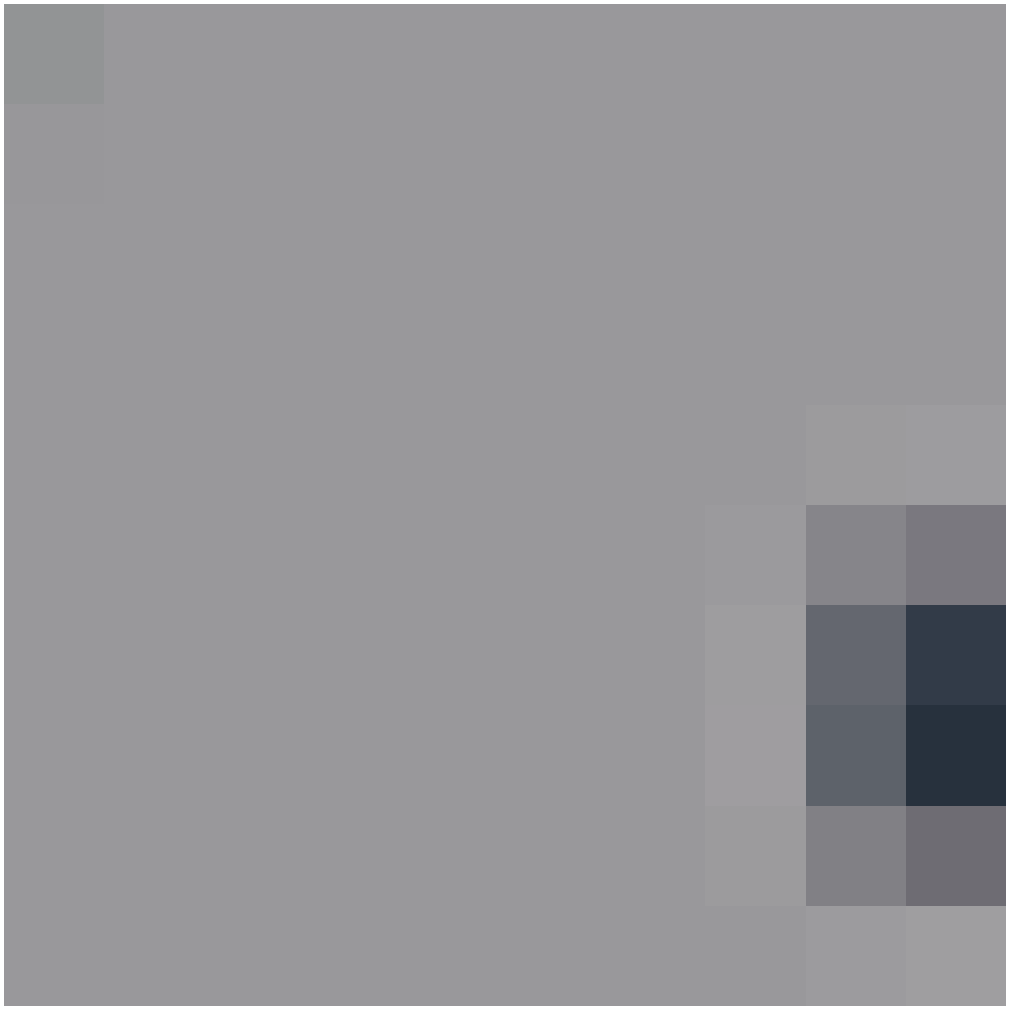
ArianeBlow Ariane **13 févr.**

Une demande d'enregistrement de CVE à été faite auprès de CVE-Mitre pour de multiple XSS stockées, l'erreur vient d'un mauvais contrôle des inputs en particuliers les iput ayant une valeure reflechies dans l'application. L'ensemble des inputs sont vulnérables avec la payload suivante :

```
<img/src/onerror=prompt(1)>
```

Ce qui provoque une execution de code JavaScript sur l'ensemble des naviguateurs des personnes visitants les pages infectés. Dans la gestion des users, des groups, des messages, des équipes, des notes …etc…etc nous retrouvons des inputs qui se refléchissent dans la page dans lesquelles il est possible d'y injecter du JavaScript.

Dans un autre genre, la méthode d'upload d'image dans les image de profile par exemple, permet une upload de fichier type SVG, ce format permet également de stockler une payload XSS ou une redirection direct via l'execution du XML qui est présent dans ce format. La méthode qui consiste à faire une de l'image une donnée encodée en base64 permet de fair « ouvrir dans une nouvelle page » une SVG contenant une XSS et ainsi piéger les visiteurs créant la aussi une XSS stockée.



(Mais je continue d’utiliser votre app, elle est super pratique quand même et assez bien fichu, il faut quand même le dire !!!)

---

p.belloy **Axelor Core team** **15 mars**

Le cas cité de l’input est fixé en **5.4.11** .

Pour les SVG, les propriétés `file.upload.whitelist.pattern`/`file.upload.blacklist.pattern` ainsi que `file.upload.whitelist.types`/`file.upload.blacklist.types` permettent de filtrer sur les filename ou les content types.

Cdlt