Я выбрала библиотеку для обработки Json Argo, судя по всему, она существует еще с 2008 года, поэтому ошибок в ней видимо очень мало.

Выбраны для фаззинга были три различных джсон парсера из разных классов библиотеки, первый парсит просто, второй – с событиями, конкретный метод – для итеративного парсинга, третий – без итераций, но тоже с событиями.

Фаззеры фаззились чуть более 12 часов, и какой-то в итоге нашел и записал два репродьюсера (я не учла тот факт, что они все писали бы репродьюсеры в одно и то же место, если бы нашли, так что я не могу сказать, какой именно из них нашел ошибку). Но в целом библиотека хорошо отдебажена, разработчики молодцы.

Сиды у всех были общие, корпусы у каждого свои, соответствующие номерам.