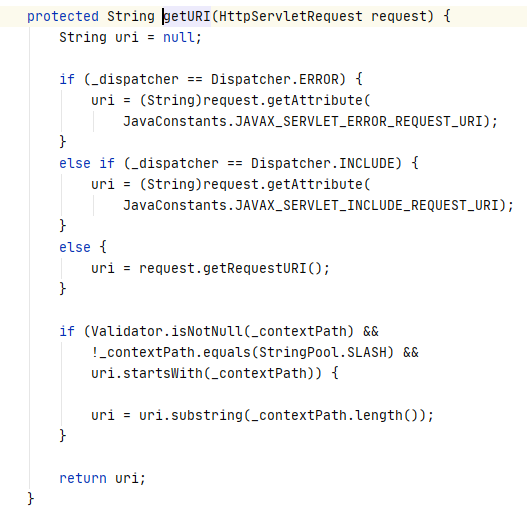
Câu f. Liferay đã fix lỗ hổng như nào?

* Lỗi hổng xảy ra do class InvokerFilter khi xử lý uri truyền vào đã không loại bỏ dấu /, khiến không tìm thấy filter custom. Trong phiên bản mới đã có thêm đoạn để lọc bỏ dấu / thừa nhằm tìm thấy filter của mình.

Ảnh dưới là hàm getURI trong class com.liferay.portal.kernel.servlet.filters.invoker. InvokerFilter nhằm lấy được uri của request ở phiên bản 6.2 ga2. Nhận thấy trong hàm uri không được xử lý mà lấy trực tiếp từ request.



Ở phiên bản 6.2 ga6 hàm getURI đã thêm phần xử lý loại bỏ dấu ‘/’ bị thừa trong uri. Nhờ đó input đầu vào là ‘/api/////liferay’ sẽ được chuyển thành ‘/api/liferay’ và từ đó sẽ sẽ nhận filter.

