

## Vulnerability: Deprecated Interface (Security Misconfiguration)

Juice Shop Challenge: Deprecated Interface

Date Found: 2025-04-15

Severity/Difficulty (Juice Shop Rating): ★★☆☆☆

Location/URL:

/#/complain

Parameter/Input Field: Upload file type

Description:

Old B2B XML interface still accessible despite UI limitations.

Steps to Reproduce (STR):

1. Go to Complaint page
2. Only PDF/ZIP visible
3. Discover XML via inspecting main.js
4. Upload XML and send to backend

Proof of Concept (PoC):

Payload Used:

XML format upload via custom request

Impact:

Enables attackers to interact with deprecated logic.

Root Cause (Conceptual):

Interface not properly deprecated or disabled on backend.

Remediation / How to Fix:

Remove or block deprecated functionality server-side.

Relevant OWASP Resource: OWASP Misconfiguration Cheat Sheet

Tools Used:

Burp Suite, Dev Tools

Personal Notes/Learnings:

Learned that frontend restrictions are not enough.

# Complaint

Customer

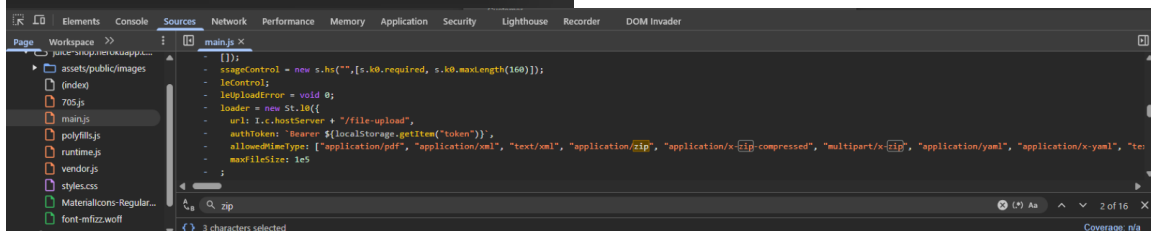
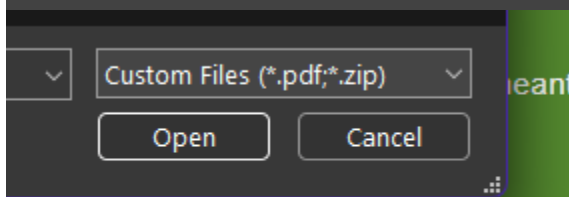
aziz@sec

Message\*

Max. 160 characters

0/160

Invoice:  No file chosen




# Complaint

Customer

aziz@sec


Message\*

aziz

 Max. 160 characters

4/160

Invoice:  aziz.xml

 Submit