Stored XSS when uploading files to an invoice

124

Share:

State	Resolved (Closed)
Disclosed	**March 26, 2020 3:18pm +0530**
Reported To	**Visma Public**
Asset	app.workbox.dk (Domain)
Weakness	Cross-site Scripting (XSS) - Stored
Bounty	$250
Severity	Medium (4 ~ 6.9)
Participants	
Visibility	Disclosed (Limited)

Collapse

SUMMARY BY VISMA PUBLIC

I've found a stored XSS from the fileupload. The parameter fileID is vulnerable and will be stored to the page.

Steps To Reproduce

- Login
- Navigate to one of your invoices
- Upload some file and intercept the traffic
- Once you see the JSON payload like this {"id":"abcabccabcabc","name":"file-name"} modify it for this {"id":"abcabc\"><svg/onload=confirm(1)>abcabc","name":"file-name"}
- Refresh the page and see that javascript will be executed

TIMELINE · EXPORT

muon4 submitted a report to **Visma Public**.	Mar 2nd (3 months ago)
christoffer-visma posted a comment.	Mar 2nd (3 months ago)
christoffer-visma changed the status to **Triaged**.	Mar 2nd (3 months ago)
Visma Public rewarded muon4 with a **$250** bounty.	Mar 2nd (3 months ago)
muon4 posted a comment.	Mar 2nd (3 months ago)
christoffer-visma closed the report and changed the status to **Resolved**.	Mar 5th (3 months ago)
martin-visma changed the report title.	Mar 6th (3 months ago)
martin-visma requested to disclose this report.	Mar 6th (3 months ago)
muon4 agreed to disclose this report.	Mar 26th (2 months ago)
This report has been disclosed.	Mar 26th (2 months ago)