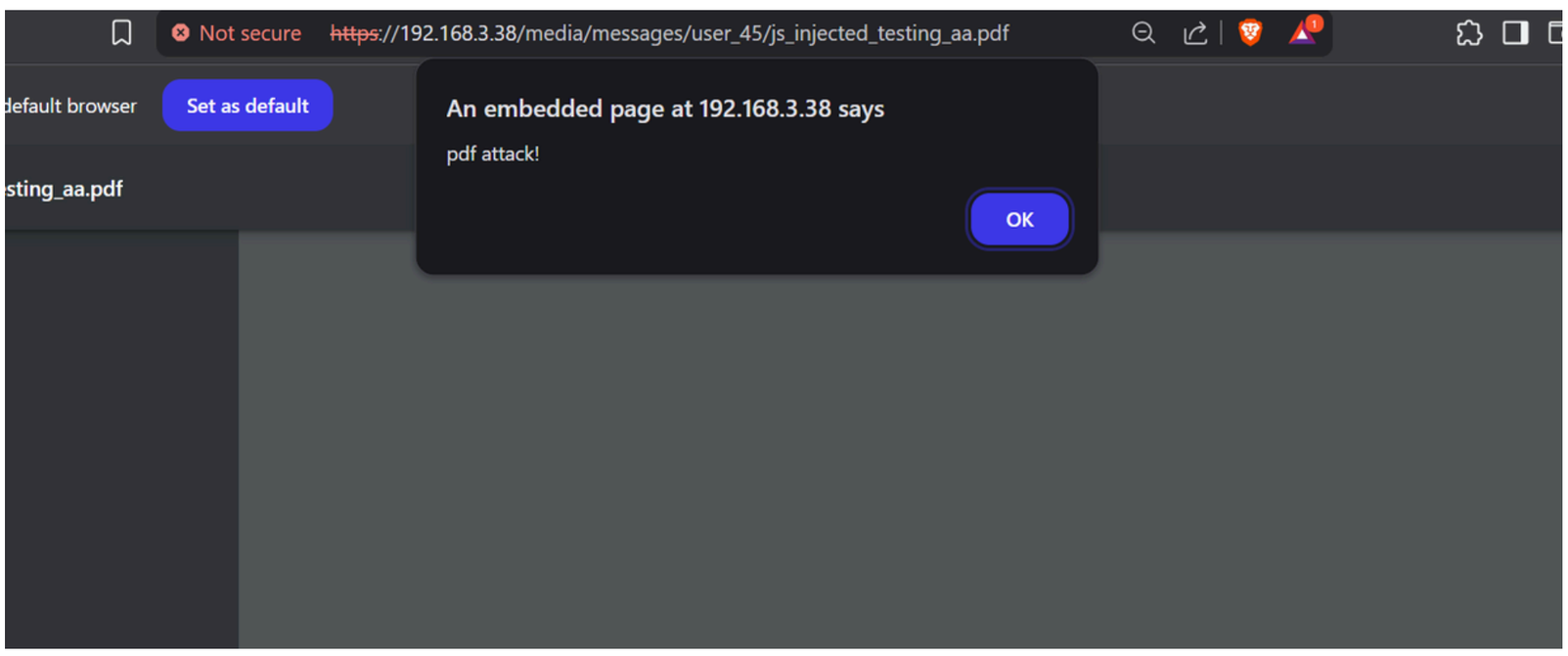
Group number attacked	group 24
type	security
bug type	stored XSS via file upload
endpoint	https://192.168.3.38/media/messages/user_45/js_injected_testing_aa.pdf (Accessible from: backlink (vulnerable file path))

short description of the bug

a user can upload a .pdf file through the messages feature that is rendered inline &d executes javascript when opened, this will lead t0 st0red XSS

exact steps to reproduce

1. log in to the site
2. then g0 to https://192.168.3.38/messages/
3. now c0mpose a message (used https://github.com/cornerpirate/JS2PDFInjector) and upload a .pdf file with the following payload - <script>alert('XSS triggered via PDF')</script>
4. send the message
5. when the recipient 0pens the pdf (served inline), the javascript code executes
6. we can observe an alert box, confirming execution



impact

- attacker can run arbitrary javascript in victim’s br0wser.
- can lead to coakie theft, session hijack or/ phishing