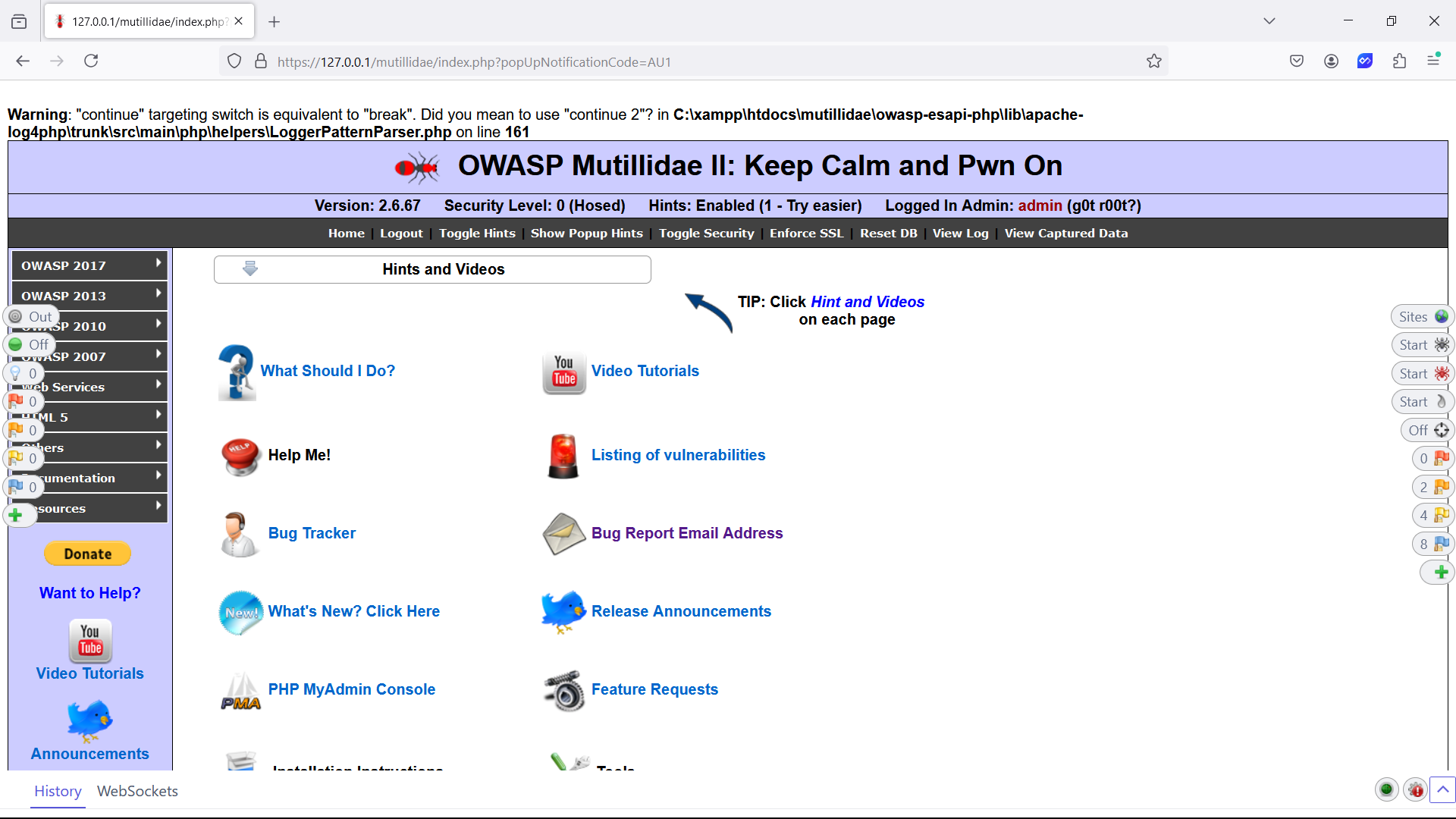
**Report 2**

**Buffer over flow**

**Definition:**

Buffer overflow happens when a program writes more data to a temporary storage area (called a buffer) than it can hold. Think of a buffer like a container; if you pour too much liquid into it, the excess spills out. In computing, this "spill" can overwrite other important data in memory, which can cause the program to crash or be exploited by hackers to run malicious code

Website used :

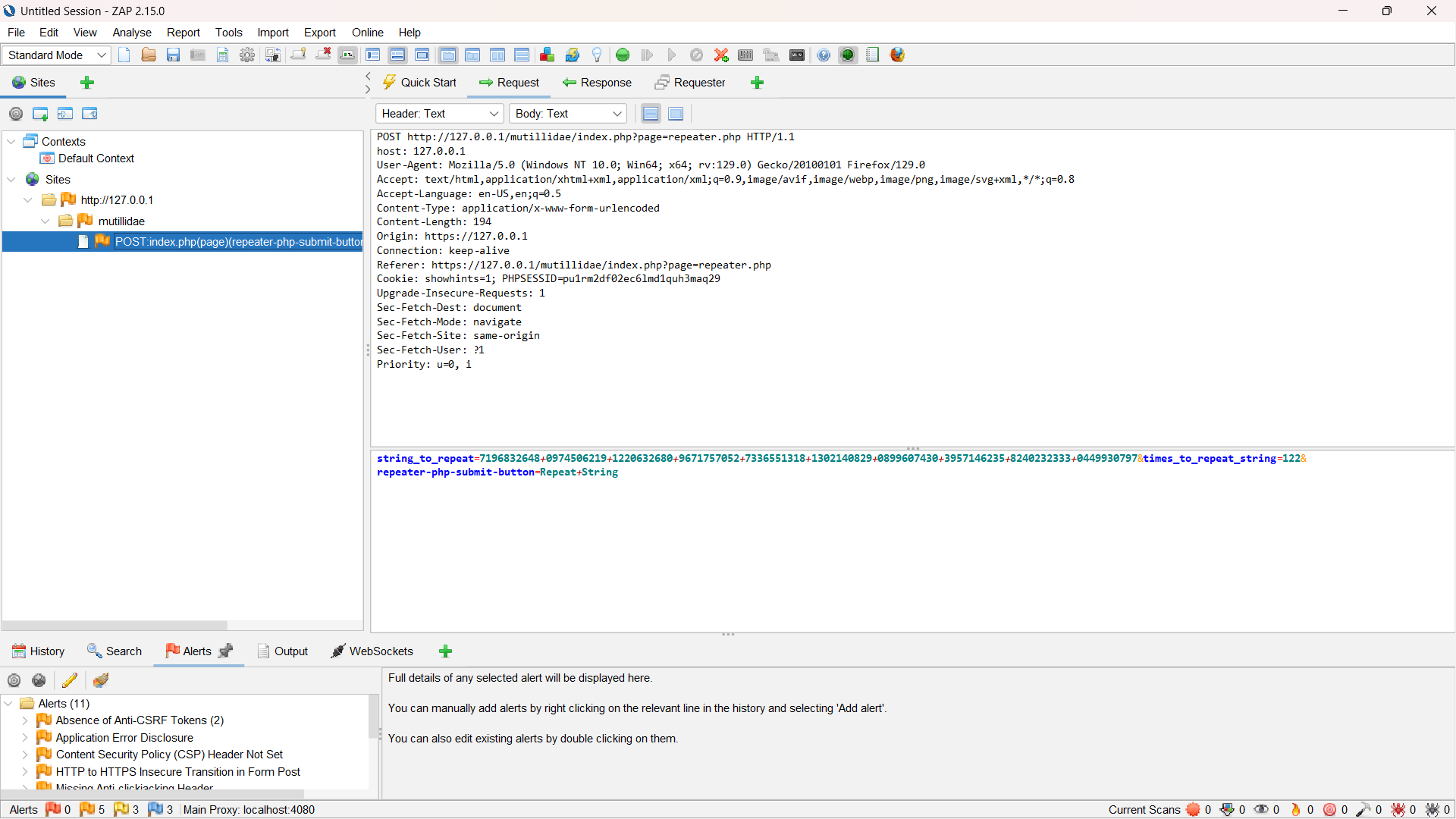
 Mutillidea 2 ,it is a vulnerable web site specifically created for pen testers

**Proof of concept:**

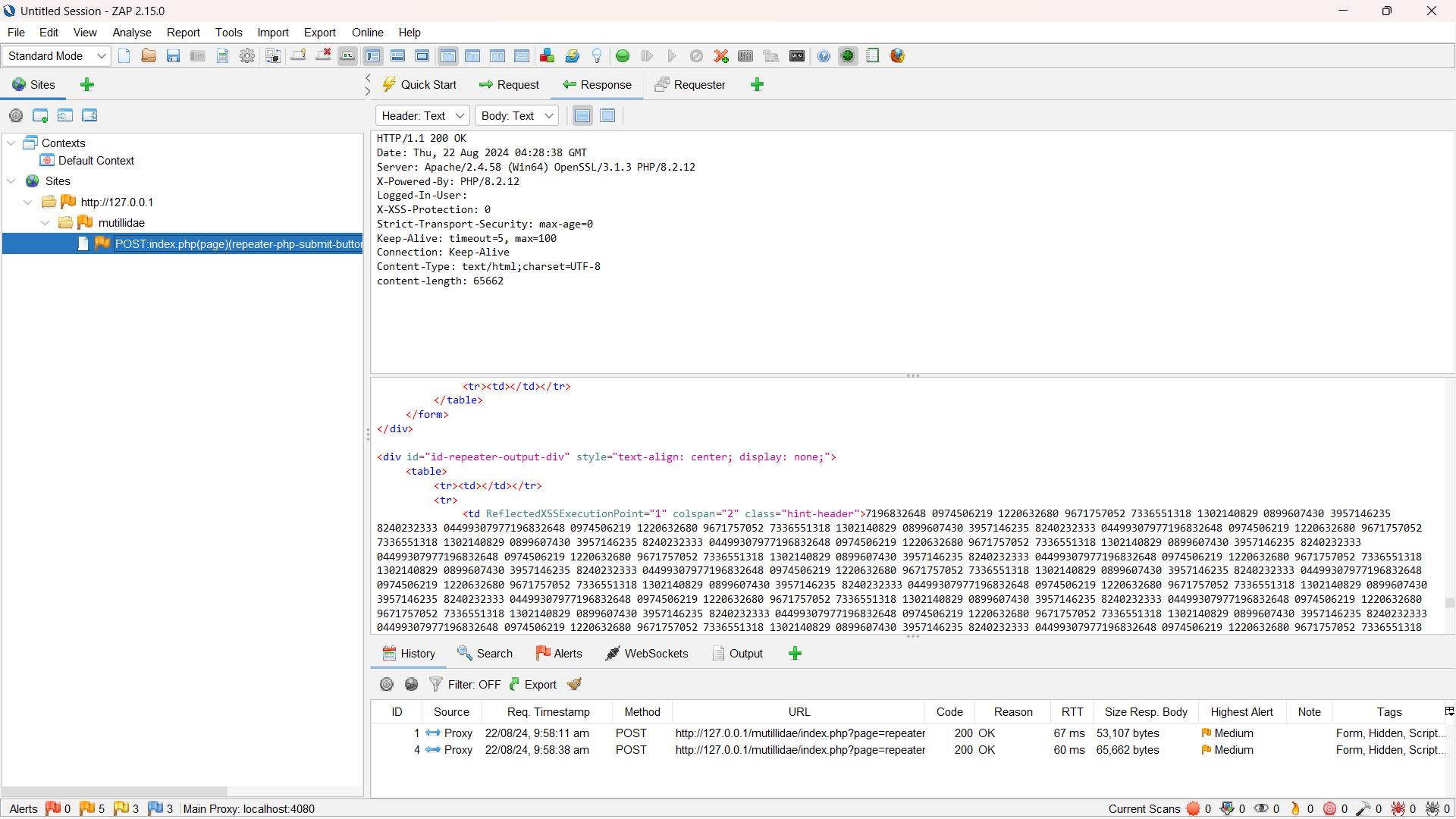
Step1

Sending more characters than usual in input box

Request

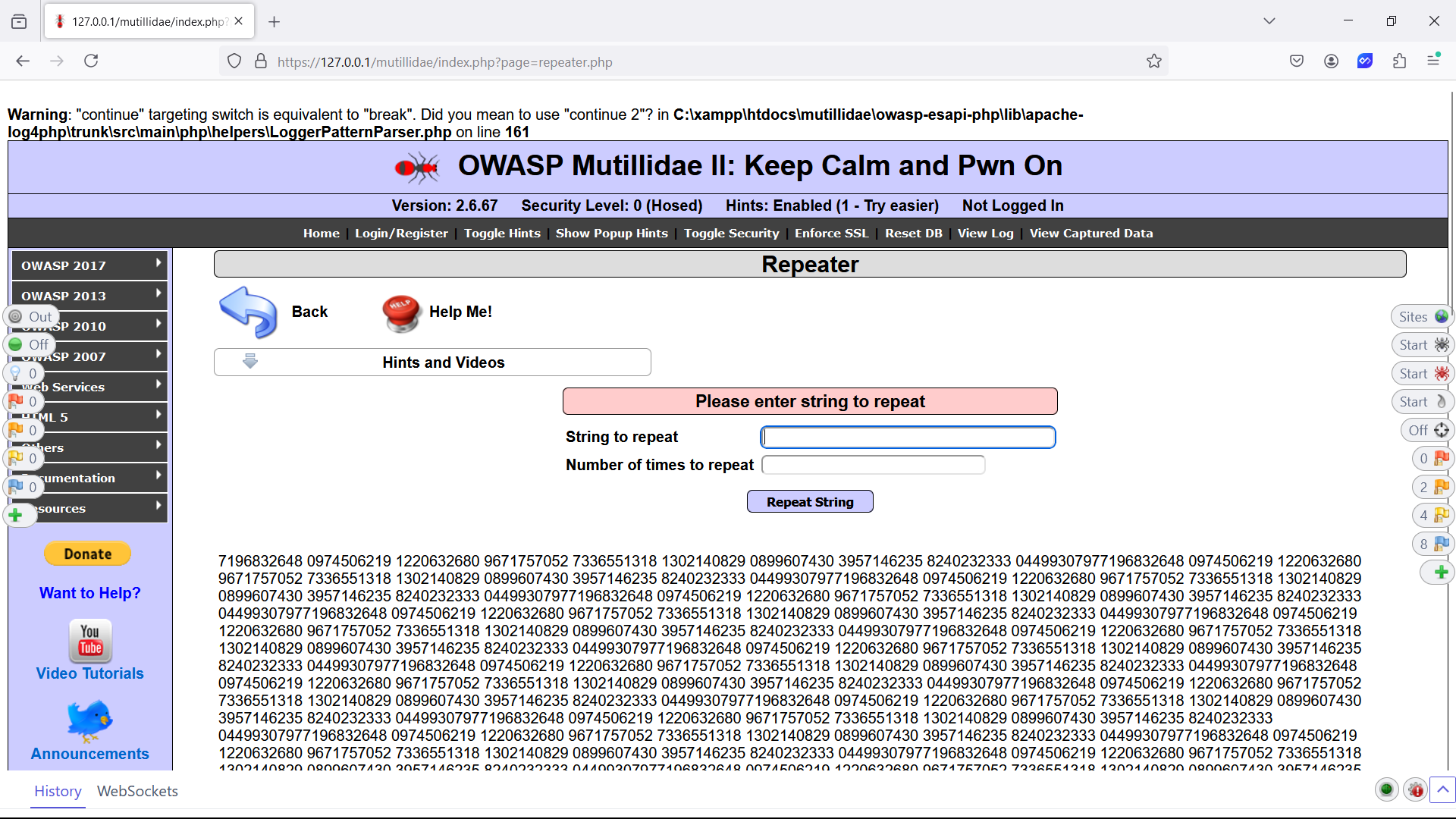


Response



**Result:**

Giving too many stings in the text box can leads to buffer over flow and it can cause Denial of service

**Vulnerability report:**

here is the reference for the Zap. The report is been generated

**https://github.com/TARIKAPRABHAKARAN/Cybersecurity**