**Discovery:  
  
screenshot of vulnerable code**

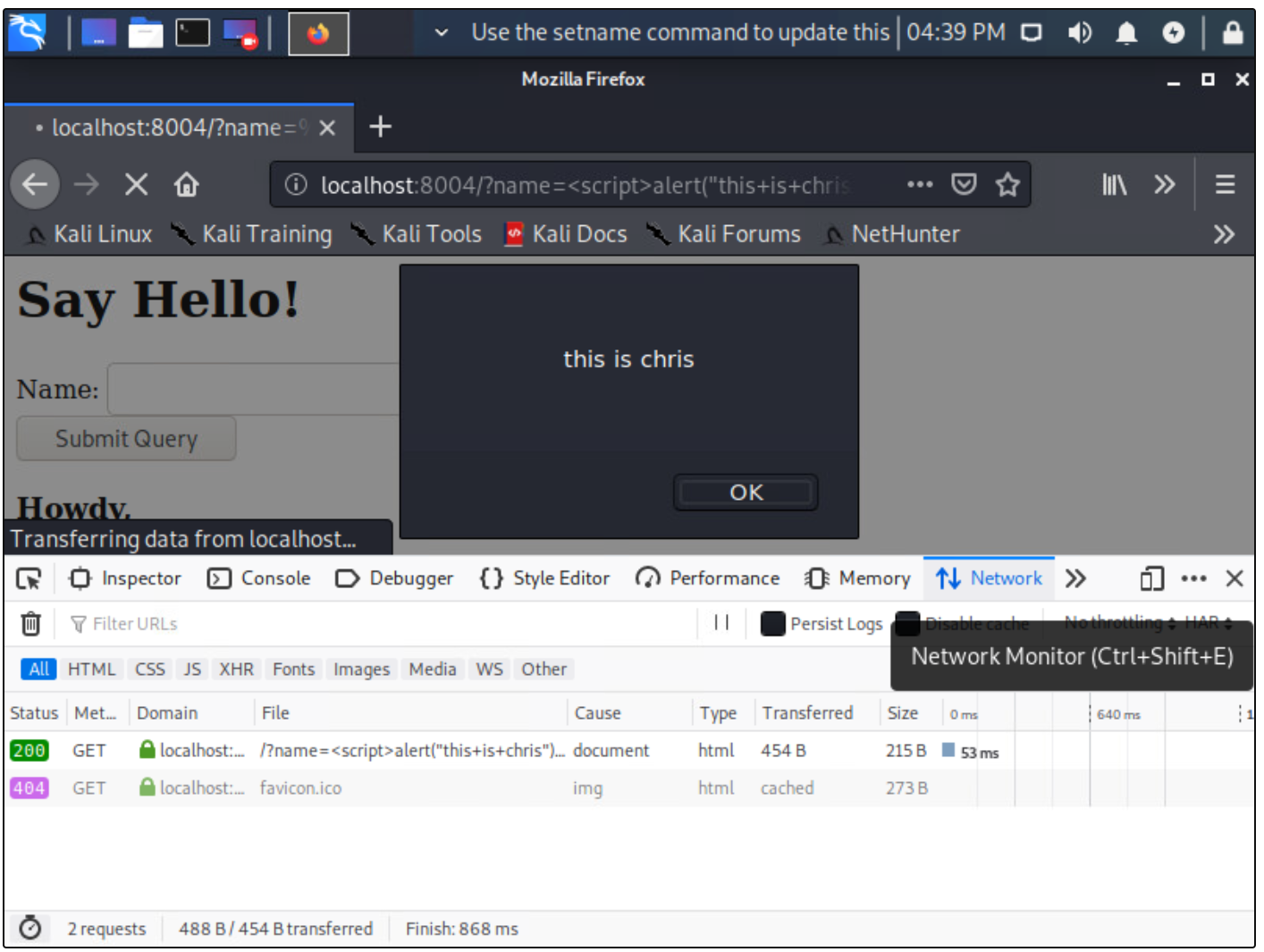
****

****

**Issue explanation**

We insert the user provided input directly into the webpage without escaping characters that the browser could interpret in unintended ways, i.e. script tags and their contained code.

**Exploitation screenshots:**



**Remediation:**

**Screenshot of adapted code**



**Explanation of why this defense prevent issues.**this prevents the contents of the script tags from being interpreted as executable code.

**Testing – why: malicious input successful/unsuccessful**

Was unsuccessful due

**Testing – screenshot of safe output + get request passed along with name**

