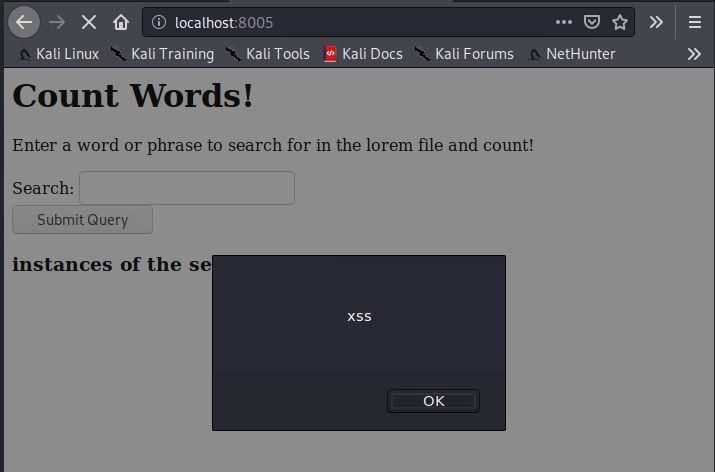
**Discovery:**

 Xss: we don’t sanitize or escape the user input, and concatenate it directly with the output.

Command Injection: the exec() function doesn’t clean input either, allowing us to collect information about the system. I am having some trouble getting multiple lines of output to appear in the result, I’m assuming there’s an issue converting newline characters to their html line-break equivalents. That being said, there is most certainly a way to remove / substitute the newline characters and dump the entire output. – might just need to pipe output to a file and run some other operations on it before ‘cat’ing it.



**Remediation:**

For the xss, we sanitized the output string containing user input before printing it:



For the command injection, we used the described php functions to scan the file for the user search string, and count matches.

