Assignment 3

XSS and Fix on xxs_2.py

- Start running the python file on terminal using command: ‘python3 xss_2.py’
- Start postman to test for input validity and ensure a well formed html at each instances.
- On the browsers instead of ‘name’, I inserted **“><button onClick=”alert(‘You have a virus’);>Click me</button><a href=”** in order to achieve a button that when clicked, gives and alert.

Fix

- inserted ‘from html import escape’ and ‘format(escape(name))’ to avoid XSS attack on the page.

The screenshots for this exercise are below:

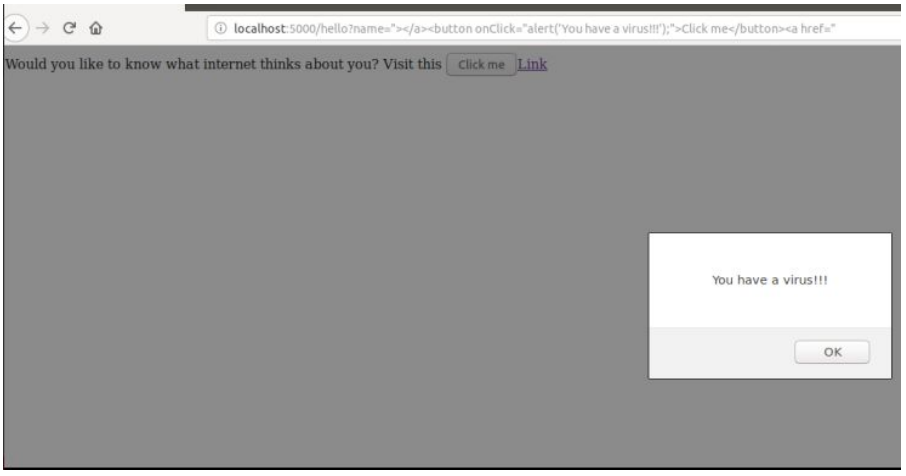

Fig1. Attacked site

```
<html>
    <head>
        <title>Internet knows</title>
    </head>
    <body>
            Would you like to know what internet thinks about you? Visit this
        <a href="https://www.bing.com/search?q="></a>
        <button onClick="alert('You have a virus');">Click me</button>
        <a href="" attribute="aaa">Link</a>
    </body>
</html>
```

Fig 2. Well formed html after inserting XSS script

```
<html>
    <head>
        <title>Internet knows</title>
    </head>
    <body>
            Would you like to know what internet thinks about you? Visit this
        <a href="https://www.bing.com/search?q=&amp;quot;&amp;gt;&amp;lt;/a&amp;gt;&amp;lt;button onClick=&amp;quot;alert(&amp;#x27;You have a virus&amp;#x27;)
            ;&amp;gt;Click me&amp;lt;/button&amp;gt;&amp;lt;a href=&amp;quot;" attribute="aaa">Link</a>
    </body>
</html>
```

Fig3. Fixed site showing characters instead of well formed html