CVE-2024-50659 – Reflected XSS/HTML Injection

Description: The parameter **shippingAsBilling** does not properly validate the user input. As a result, an error is returned with the input reflected in the error message without output sanitization.

Remediation:

- Properly validate all input
- Handle error messages gracefully without returning a stack trace
- If reflecting input, properly sanitize before reflection.

Figure 1-Request with XSS

Figure 2-Response with Input Reflected and Unsanitized

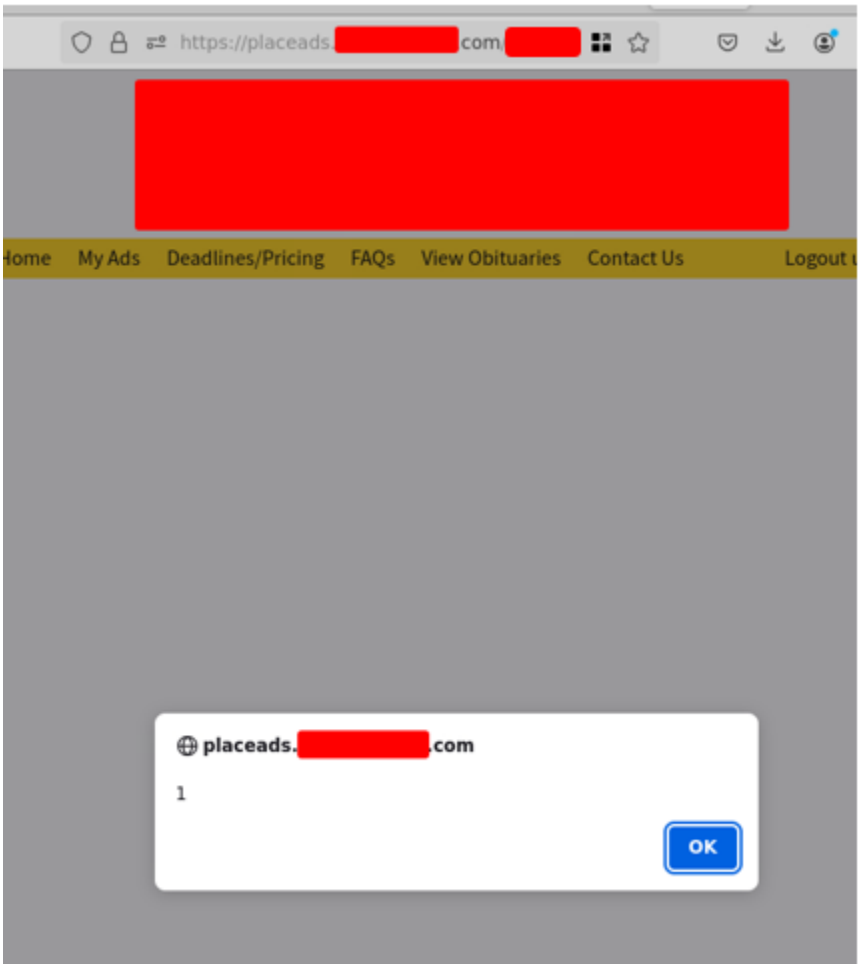

Figure 3-XSS Response in Browser

HTML Injection

Figure 4-HTML Injection Request

Figure 5-HTML Injection Response

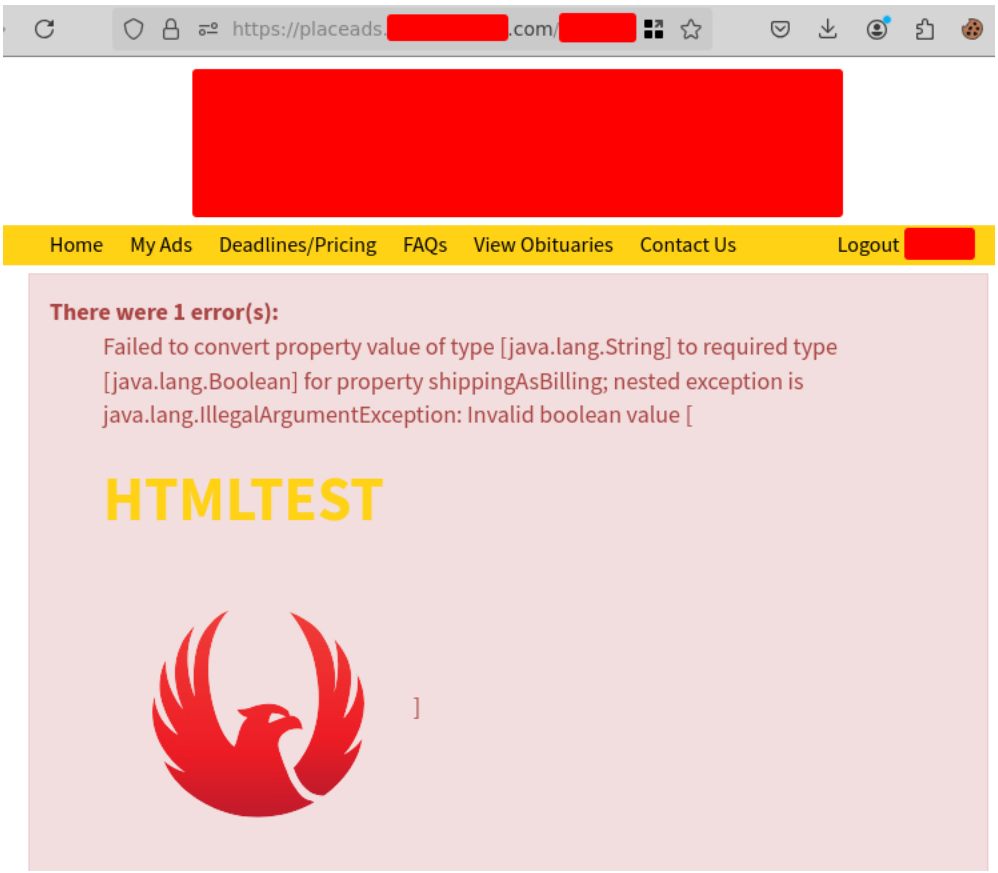

Figure 6-HTML Rendered in Browser

CVE-2024-50658 – SSTI (Server-Side Template Injection)

Description: The parameters **shippingAsBilling** and **firstname** do not properly validate the user input. As a result, the **shippingAsBilling** causes an error with the server evaluating the injected template and the **firstname** parameter reflects the server output of the injected template.

Remediation:

- Properly validate all input
- Handle error messages gracefully without returning a stack trace
- Do not allow users to modify or submit new templates
- Use a logic-less template engine such as Mustache

Figure 7-HTTP Request with SSTI Command

*Figure 8-Server Evaluating 7*7*

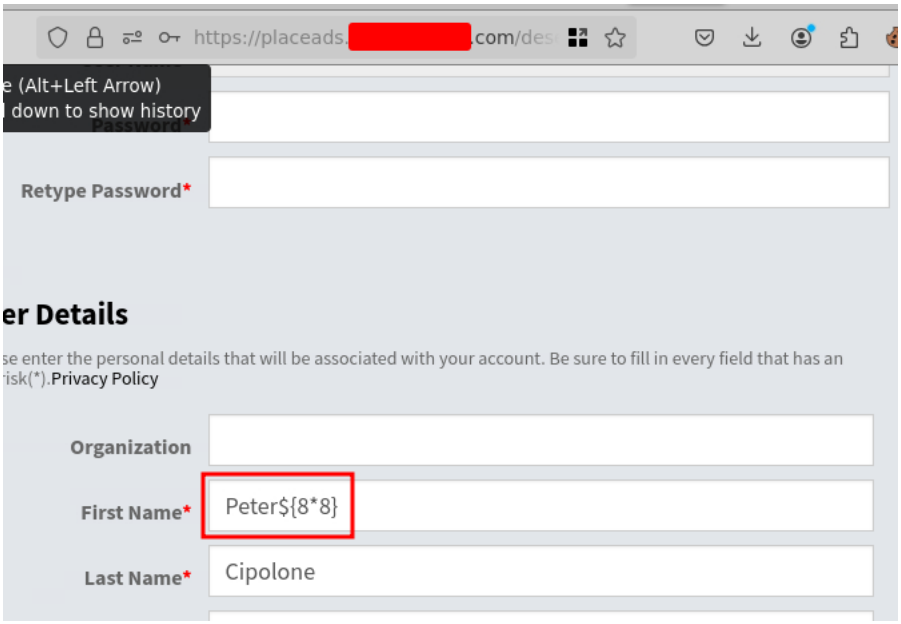

Figure 9-SSTI Request in First Name

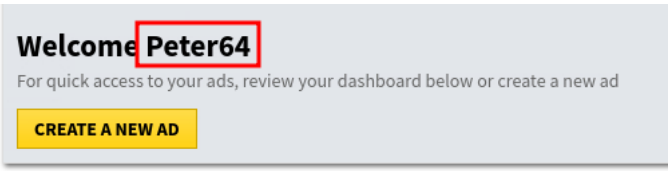

*Figure 10-Server Evaluating 8*8*

CVE-2024-50660 – Unrestricted File Upload

Description: During the obituary creating process, the file upload requirements are only enforced on the client-side and not the server-side. This allows for the upload of any file type which can be viewed in the browser.

Remediation:

- Ensure file upload checks are performed on both client-side and server-side
- Ensure file extension, Content-Type, and File Magic Bytes are all properly verified

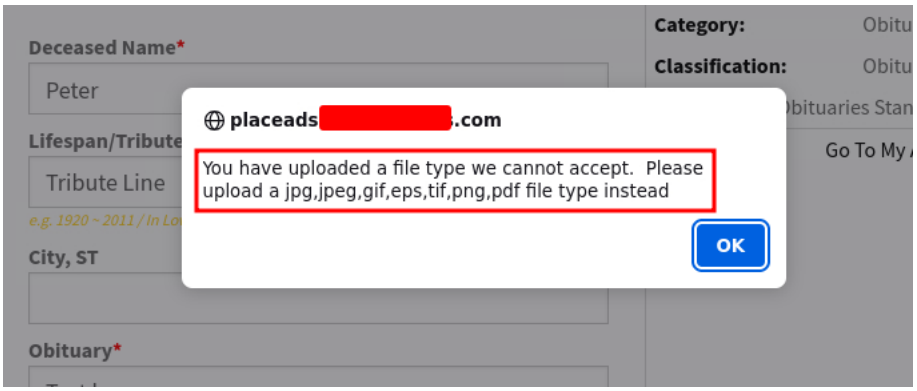

Figure 11-Warning About Acceptable File Types

```
5
6  _eventId_create
7  ----------------------------376033127218666375191152344147
8  Content-Disposition: form-data; name="file"; filename="test.txt"
9  Content-Type: text/plain
0
1  This is a test by Peter Cipolone!
2
3  ----------------------------376033127218666375191152344147--
4
```

Figure 12-Changing File Extension and Content-Type

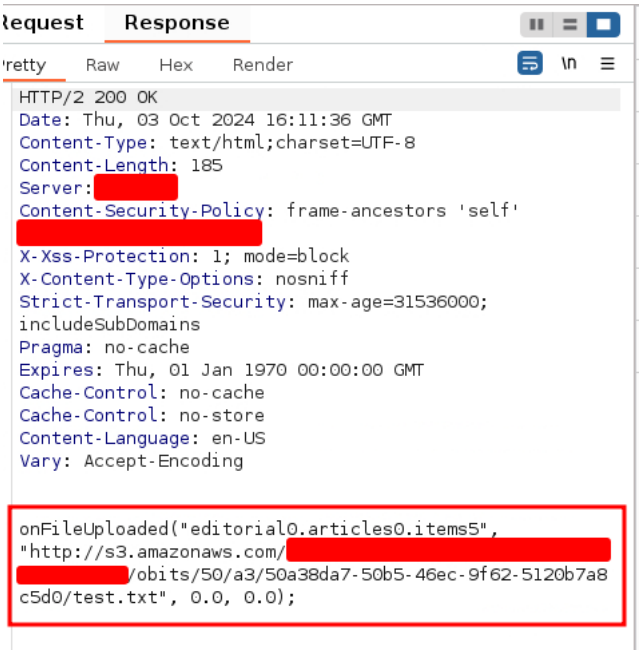

Figure 13-Server Response with Image File Location

Figure 14-Text File Upload Successful - Confirmation