Abusing Backup/Restore feature to achieve Remote Code Execution in microweber/microweber

0

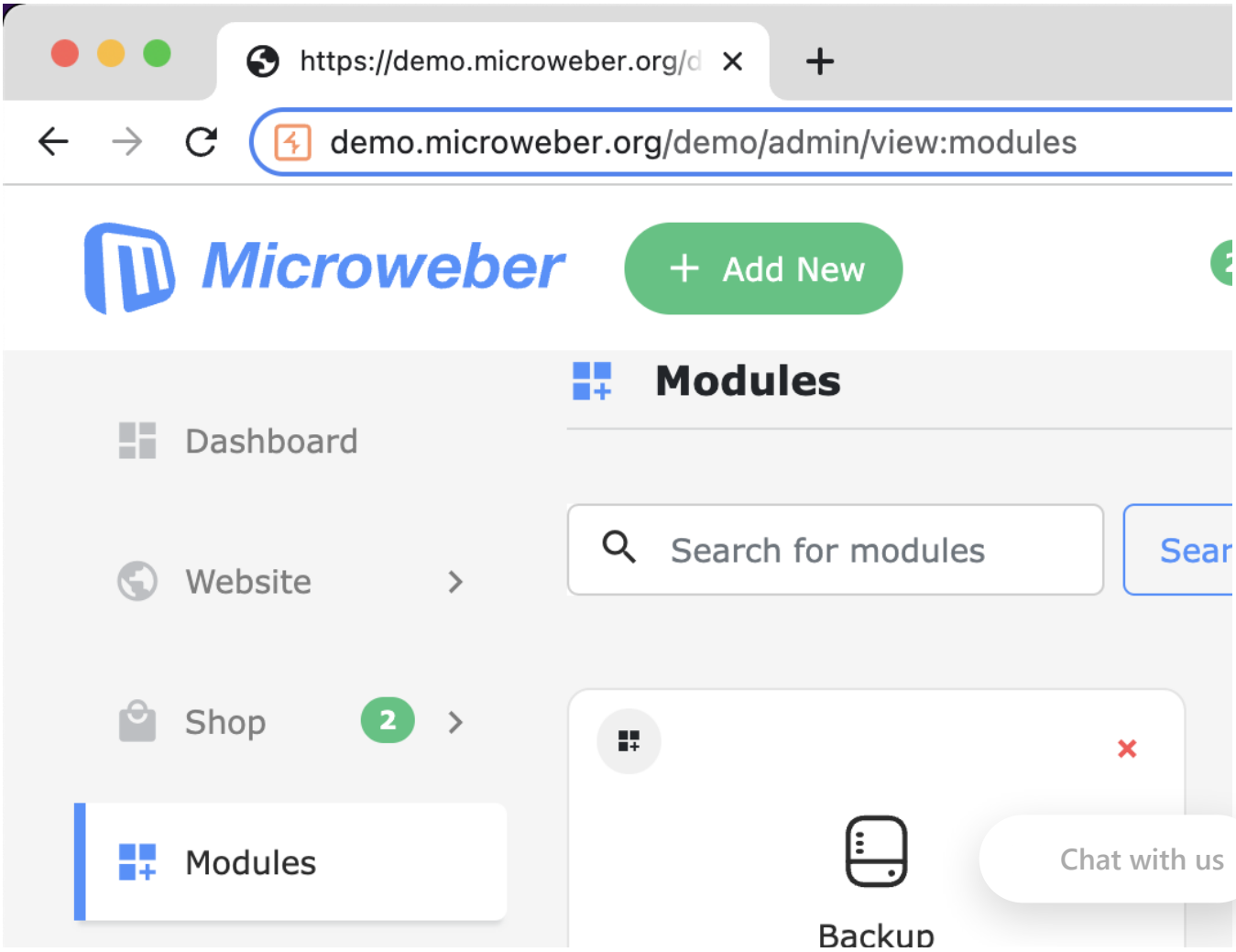
Valid Reported on Mar 9th 2022

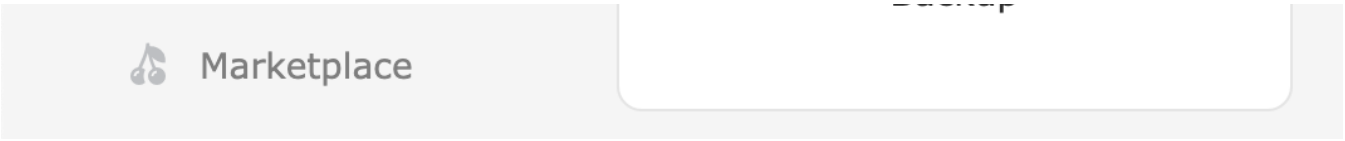
Description

Admin can use `Backup` modules to upload a malicious PHP file, which can lead to RCE.

Proof of Concept

Log in as admin, navigate to **Modules** -> **Backup**: `https://demo.microweber.org/demo/admin/view:modules/load_module:admin__backup`

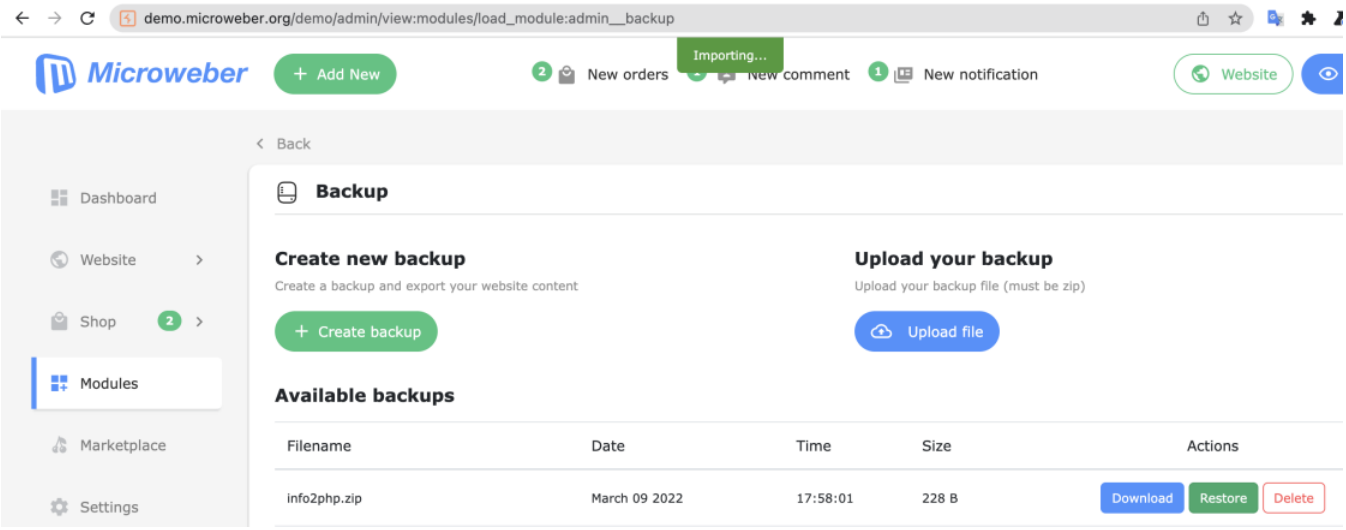




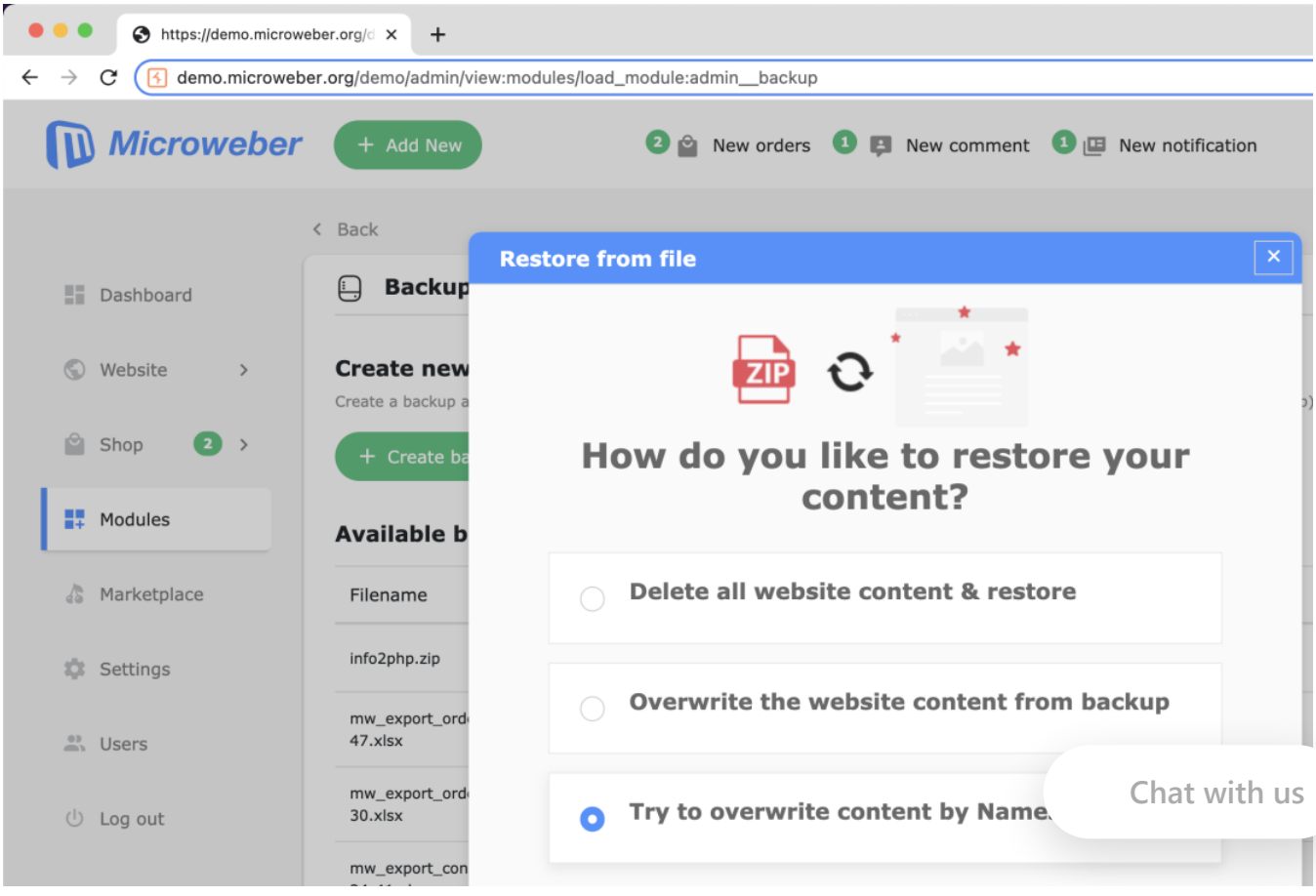
Prepare a malicious PHP file, in this case `info2.php`

```
<?php system($_GET['cm']); ?>
```

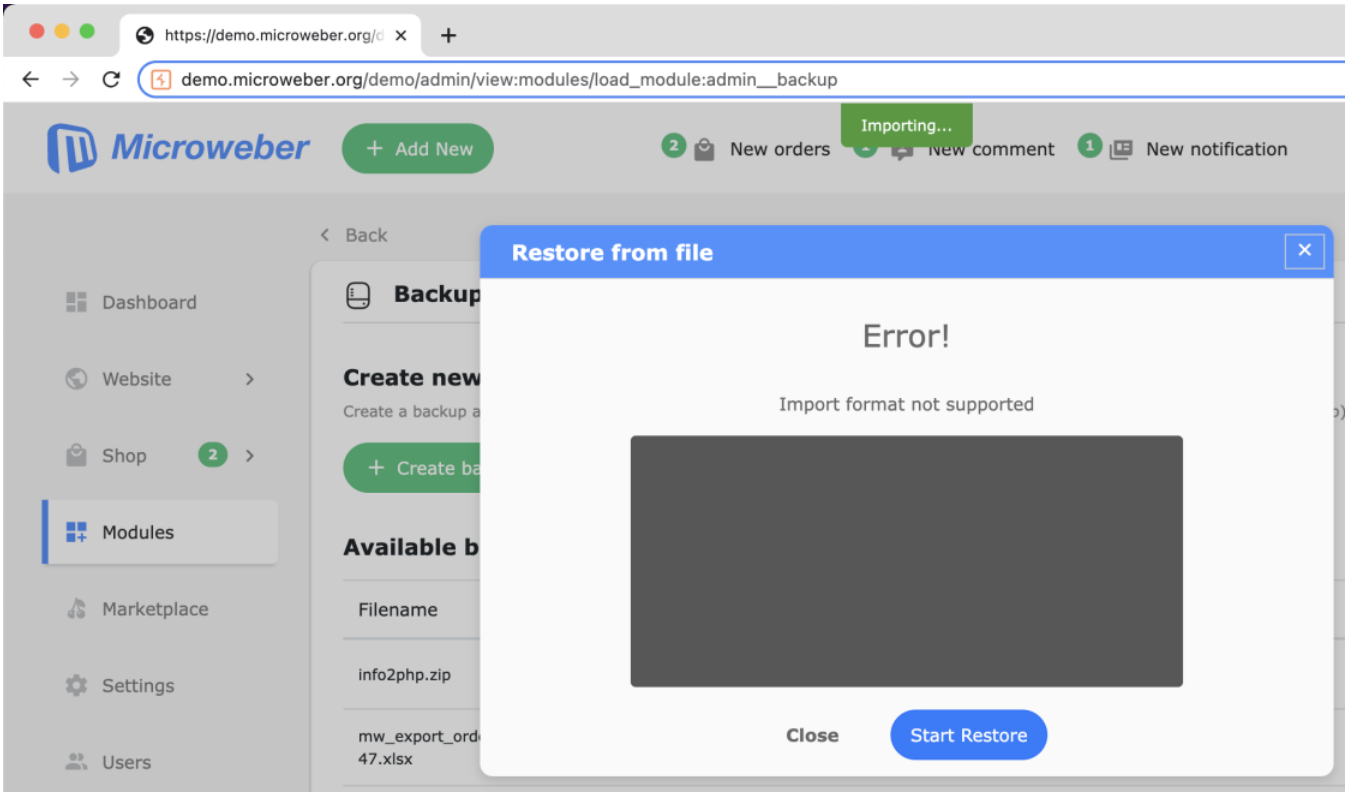
Compress this file to `info2php.zip`, then click `Upload your backup`.



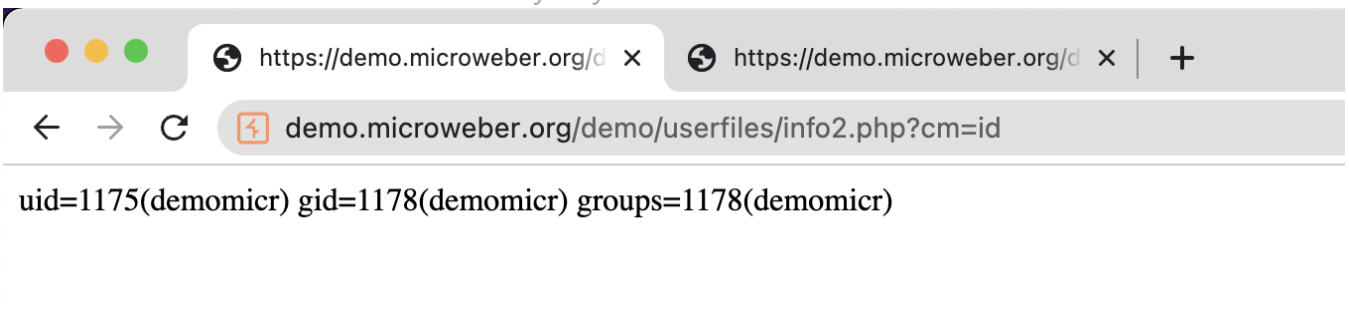
After successfully uploaded, click to **Restore**, choose **Try to overwrite content by Names & Titles**, then **Start Restore**



The system returns **Import format not supported**



However, the malicious file `info2.php` is unzipped and located in `/userfiles/`, and that malicious PHP file can be accessible by anyone:



Impact

Remote code execution (RCE) attacks allow an attacker to remotely execute malicious code on a computer. The impact of an RCE vulnerability can range from malware execution to an attacker gaining full control over a compromised machine.

CVE
CVE-2022-0921
(Published)

Vulnerability Type
CWE-94: Code Injection

Severity
High (7.2)

Visibility
Public

Status
Fixed

Found by

Quan Doan
@quandqn
unranked

Fixed by

Bozhidar Slaveykov
@bobimicroweber
maintainer

This report was seen 738 times.

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

Quan Doan modified the report 9 months ago

Quan Doan modified the report 9 months ago

Bozhidar Slaveykov validated this vulnerability 9 months ago

Quan Doan has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Quan Doan 9 months ago Researcher

Hi @bobimicroweber, since the report was validated, should I remove the ma
demo server? Or will you reset the site later?

Thank you!

Bozhidar Slaveykov marked this as fixed in **1.2.12** with commit **867bdd** 9 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation