Instantly share code, notes, and snippets.

virendratiwari03 / **Microwber File upload vulnerability**

Last active 2 years ago

☆ Star

<> Code   ⚬ Revisions   4

Microweber-File upload Vulnerability

<> **Microwber File upload vulnerability**

```
 1  Product: Microweber
 2
 3  Product Version: 1.1.18
 4
 5  Vulnerability: Unrestricted File Upload
 6
 7
 8  Description:
 9  The Microweber 1.1.18 application is vulnerable to unrestricted file uploads. Effective controls have not been implemented to restrict user
10
11  Attack Type: Local
12
13  Impact:
14  Unrestricted file upload is a serious vulnerability with significant impact on the application and its infrastructure. An attacker with the
15
16  Client-side attacks: Uploading malicious files can make the website vulnerable to client-side attacks such as XSS or Cross-site.
17
18  An attacker might be able to put a phishing page into the website or deface the website.
19
20  Steps:
21
22  1. Login into your Microweber account
23  2. Go to admin page
24  3. Go to Users -> My Profile -> Edit User
25  4. Try to Upload any image extension. It will successfully update.
26  5. Now, download any web shell from google and modify the extension.
27  6. capture the request of upload profile in burp and modify image extension (Eg- test.php.png)
28  7. It will succesfully upload the web shell.
29
30
31  Reference:
32  https://null-byte.wonderhowto.com/how-to/upload-shell-web-server-and-get-root-rfi-part-1-0162818/
33  http://pentestmonkey.net/tools/web-shells/php-reverse-shell
```

◀   ▶