Stored Cross-Site Scripting vulnerability in Recipe Instructions allows Admin session hijacking in hay-kot/mealie

0

Valid Reported on Jun 28th 2022

Description

A low privilege user can insert malicious JavaScript code into the Recipe Instructions which will execute in another person's browser that visits the recipe.

Proof of Concept

```
<img src=x onerror=alert(document.domain)>
```

Reproduction Steps:

As a lower privileged user login to the Mealie web application.
Create a recipe and using the inline markdown editor add the Proof of Concept code to the Instructions.
An alert box will appear indicating the presence of XSS.

Impact

A lower privilege user can submit malicious JavaScript into the Recipe Instructions which will execute in the context of another person's browser when they navigate to the vulnerable page. Since this is a Stored XSS vulnerability, no user interaction is required besides browsing to the vulnerable page. An attacker can use this XSS vulnerability to do anything that JavaScript can do, including but not limited to, making arbitrary HTTP requests in the victim's browser, hook a victim's browser, and hijack an admin session.

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

Severity
High (8.1)

Registry
Pypi

Affected Version
v1.0.0beta-3

Visibility
Public

Status
Fixed

Found by

0xbruno
@0xbruno
legend

Fixed by

Hayden
@hay-kot
unranked

This report was seen 469 times.

We are processing your report and will contact the **hay-kot/mealie** team within 24 hours.
5 months ago

0xbruno 5 months ago Researcher

@admin - can you donate my bounty to the maintainer?

0xbruno 5 months ago Researcher

I did not realize at the time of submission that the session cookie `auth._token.` the `HttpOnly` flag set. This means that JavaScript has access to the session co attacker can hijack an admin's session. This would bump this vulnerability up to a high.

0xbruno modified the report 5 months ago

Jamie Slome 5 months ago Admin

We are happy to donate the bounty to the maintainer. Before we can do this, we need the maintainer to establish a fix for the report and elect themselves as the "fixer". We will then be able to do this for you ♥

We have contacted a member of the **hay-kot/mealie** team and are waiting to hear back 5 months ago

We have sent a follow up to the **hay-kot/mealie** team. We will try again in 7 days. 5 months ago

We have sent a second follow up to the **hay-kot/mealie** team. We will try again in 10 days. 5 months ago

We have sent a third and final follow up to the **hay-kot/mealie** team. This report is now considered stale. 4 months ago

Hayden validated this vulnerability 4 months ago

0xbruno has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

We have sent a fix follow up to the **hay-kot/mealie** team. We will try again in 7 days. 4 months ago

Hayden marked this as fixed in **v1.0.0beta-1** with commit **13850c** 4 months ago

Hayden has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation