URL is vulnerable to clickjacking https://app.passit.io/

Share:

State	○ Resolved (Closed)
Disclosed	**May 10, 2019 1:49pm +0530**
Reported To	Passit
Asset	app.passit.io (Domain)
Weakness	UI Redressing (Clickjacking)
Severity	Low (0.1 ~ 3.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE

whitehacker18 submitted a report to **Passit**. Apr 6th (about 1 month ago)

URLs do not have X-FRAME-OPTIONS set to DENY or SAMEORIGIN, and they are vulnerable to clickjacking.

Reproduce steps:

1. enter your credentials and click on stay logged into this device then login
2. Run under the browser's code and you will see that the listed links are vulnerable to clickjacking attacks

```
<frameset cols="25%,25%,25%">
<frame src="https://app.passit.io/account"/>
<frame src="https://app.passit.io/list"/>
<frame src="https://app.passit.io/groups"/>
</frameset>
```

Mitigation and fix:

implement X-FRAME-OPTIONS set to DENY or SAMEORIGIN

Supporting materials and references :

https://hackerone.com/reports/337219

it's the first time for me to submit this vulnerability , i've decided to try my luck and report it to you , kindly if you see that i'm mistaken in something or you don't accept please close the report as informative ...thanks in advance

i've attached a screenshot as a poc

Impact

E.g: Hackers can lure users into the personal settings page, change data that is useful to hackers, delete accounts...

1 attachment:
F463486: POC.PNG

whitehacker18 changed the report title from **URL is vulnerable to clickjacking** to **URL is vulnerable to clickjacking https://app.passit.io/**. Apr 6th (about 1 month ago)

whitehacker18 posted a comment. Apr 8th (about 1 month ago)

Anyone is looking into this issue?

david_x4am4 changed the status to ○ **Needs more info**. Apr 8th (about 1 month ago)

X-Frame-Options is already set to SAMEORIGIN. You can verify this at https://observatory.mozilla.org/analyze/app.passit.io

Could you add more details to this report?

whitehacker18 changed the status to ○ **New**. Apr 8th (about 1 month ago)

i've just searched for a little while and i've found the cause of the problem , it seems that csp header is implemented unsafely here https://observatory.mozilla.org/analyze/app.passit.io (i've attached a screenshot as a poc)

here is owasp link : https://www.owasp.org/index.php/Clickjacking

you can find down
`Defending against Clickjacking`
`There are two main ways to prevent clickjacking:`
`Sending the proper Content Security Policy (CSP) frame-ancestors directive response headers that instruct the browser to not allow framing from other domains. (This replaces the older X-Frame-Options HTTP headers.)`

also here is another link for more information about the fix :

https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Clickjacking_Defense_Cheat_Sheet.md

sir, i'll follow up if you need any other help tell me please

1 attachment:
F464528: Csp_issue.PNG

david_x4am4 changed the status to ○ **Triaged**. Apr 8th (about 1 month ago)

Something's a little strange for sure. I'll give this a look soon.

whitehacker18 posted a comment. Apr 8th (about 1 month ago)

alright sir , i'll be here if you need any help please tell me

david_x4am4 closed the report and changed the status to ○ **Resolved**. Apr 10th (about 1 month ago)

This is fixed on staging.passit.io.

The issue is a strange one. I think it has to do with the usage of service workers and django not setting X-FRAME-OPTIONS on static files. For example .js files in app.passit.io don't have it. While now with the proposed fix they do on staging.passit.io

One first load, X-FRAME-OPTIONS is sameorigin on app.passit.io which is why the Mozilla Observatory reports it as good. On second load it does not, presumably because the service worker is handling the assets. Enabling X-FRAME-OPTIONS on static files from Django fixes the problem. The angular index.html itself is a static file.

I don't fully understand why first load is handled differently than when served via the service worker. However it appears this change fixes the issue.

whitehacker18 posted a comment. Updated Apr 10th (about 1 month ago)

Alright , happy to see it got resolved

whitehacker18 requested to disclose this report. Apr 10th (about 1 month ago)

david_x4am4 posted a comment. Apr 10th (30 days ago)

This is now live on app.passit.io - I'll allow the 30 day window for disclosure to give self hosted users some time to update. Thanks.

whitehacker18 posted a comment. Apr 10th (30 days ago)

alright sir

This report has been disclosed. May 10th (about 1 hr ago)