Gmail **Krishnamurthy Ganesh B <ganeshsurfs@gmail.com>**

Agenda for Privacy CG call on 2023-01-12

4 messages

Martin Thomson <mt@mozilla.com> Wed, Jan 11, 2023 at 5:15 AM
To: public-privacycg@w3.org

Hey all,

We have a Privacy CG call scheduled for January 12 in the APAC-friendly time slot (7pm US Eastern). An agenda is posted at https://github.com/privacycg/meetings/blob/main/2023/telcons/01-13-agenda.md

We currently have just one item on our agenda. If you have something you wish to discuss, let me know.

Cheers,
Martin

Krishnamurthy Ganesh B <ganeshsurfs@gmail.com> Thu, Jan 19, 2023 at 2:22 PM
To: Martin Thomson <mt@mozilla.com>
Cc: public-privacycg@w3.org

Hello,

Are there minutes of the meeting or recording for this meet?

Regards,
Ganesh B
+919986052445
[Quoted text hidden]
--
Regards,
K. Ganesh Bhat, Masters (Life Sciences)
ganeshsurfs@gmail.com,

Martin Thomson <mt@mozilla.com> Fri, Jan 20, 2023 at 5:36 AM
To: Krishnamurthy Ganesh B <ganeshsurfs@gmail.com>
Cc: public-privacycg@w3.org

I just merged https://github.com/privacycg/meetings/pull/26, so: https://github.com/privacycg/meetings/blob/main/2023/telcons/01-13-minutes.md
[Quoted text hidden]

Krishnamurthy Ganesh B <ganeshsurfs@gmail.com> Fri, Jan 20, 2023 at 6:07 PM
To: Martin Thomson <mt@mozilla.com>, wilander@apple.com
Cc: public-privacycg@w3.org

Hello,

Looking at the minutes of the meeting I see a similar use case of iFrame facing a "similar best practice translation" problem of the core issue of sandboxing and access of data, cookies. I wish you could help me loop in the W3C WebApp security Group for the benefit in large.

I had a small feature request:
Sandboxing access and CSRF, XSS, Script Inject attacks/ based Background data send blocking.

"I wanted to propose sharing of work on features and IP Process of Security Sandboxing (Feature/Domains) for the browsers. The focus is to create hard sandboxing of browsers to target XSS, CSRF, Cross Domain Shared/non-shared Cookie Access Blocking from third party domains. Possibly, ScriptInjection (urls, plus ...) as well.". The knowledge database for blocking CSP, XSS, CSRF, CS-Cookies, Script Injection in URLS, Images, etc are already available and sandboxing along with sanity checks using a strict mode option in these sections may be a great fit for browser feature and W3C standard both? Domain hard sandboxing is one of the many target points I may

also wish to explore considering so many cross domain cookie thefts and forgeries; apart from the fact that MIM attacks are yet one breach point that may need to be addressed separately.

I wish the team shared their views. I wish I could share some/ many I have faced.

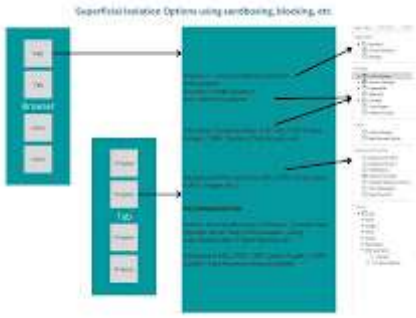
Regards,
Ganesh B

[Quoted text hidden]

3 attachments

Sandboxing__Web capture_22-6-2022_211742_twitter.com.jpeg
419K

Web capture_20-1-2023_174453_mail.google.com.jpeg
107K



Superficial Layman Non-Detailed View.jpg
79K