Improper Session management can cause account takeover[https://micropurchase.18f.gov]

Share:

State	○ Resolved (Closed)
Disclosed	**July 30, 2019 8:48pm +0530**
Reported To	TTS Bug Bounty
Asset	https://micropurchase.18f.gov (Domain)
Weakness	Insufficient Session Expiration
Severity	Medium (4 ~ 6.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE

tikoo_sahil submitted a report to **TTS Bug Bounty**. Aug 28th (2 years ago)

Hello,

I would like to report a vulnerability on https://micropurchase.18f.gov where I am able to reuse session cookie of a test user account i accessed through Github.
The problem is that the cookies stored on the browser are not getting expired after logging out from the platform and from Github as well.

Steps to Reproduce:

1. visit https://micropurchase.18f.gov
2. click on sign in through Github
3. Once you are logged in Then Use "BurpSuite" or any other Utility to get the cookies of that session ("EditThisCookie" Chrome Extension can be used and in a Case of an Attacker he can Use Any Sort Of cookie Stealing Script or Cookies Spoofing Utility to get his hands on cookies) and grab the cookies of active User Session. 4.Then Logout of the Account from https://micropurchase.18f.gov .
4. Clear all Cookies related to https://micropurchase.18f.gov using [cookies manager+ extension]Then Inject Hijacked User Cookies so that you can get into the user session...
5. After the cookies been injected You will See That the main page showing account and logout parameters on the front end.

Attack Scenario :-- If The Attacker Got his Hands Upon Users Cookies he can Get Access To the User Account.An attacker can get the user session cookies by any means Session Spoofer, Cookie Stealer etc.As the user cookies are not expiring so an attacker can directly inject the stolen cookies of a victim in a request from browser and thus can have access to the victims account.

So expire the cookies once a user is logged out of the website.
POC:- I am providing a video poc :- https://youtu.be/uLFJUJ3CnQQ , its unlisted video.

Regards
sahil tikoo

rubikcube HackerOne staff posted a comment. Aug 28th (2 years ago)
Thanks for reporting @tikoo_sahil, we're looking into this and will get back to you shortly.

tikoo_sahil posted a comment. Aug 29th (2 years ago)
ok gr8!!

coffeecup HackerOne staff changed the status to ○ **Triaged**. Aug 31st (2 years ago)
Hey @tikoo_sahil -

Thank you for your submission. We have validated this issue and forwarded the report to the responsible team for this application. They will evaluate and let us know whether or not they will be implementing a fix.

Thanks!

tikoo_sahil posted a comment. Sep 1st (2 years ago)

okay !! thanks a lot , waiting for the response.

tikoo_sahil updated the severity to Medium. Sep 1st (2 years ago)

jkm posted a comment. Sep 6th (2 years ago)

The team is working on a fix. There are some unrelated changes that need to be completed first, so it might take a while yet, but it's in progress. Thanks for your patience!

tikoo_sahil posted a comment. Sep 7th (2 years ago)

ok !! thanks for the response!!

tikoo_sahil posted a comment. Sep 14th (2 years ago)

any updates?

jkm posted a comment. Sep 15th (2 years ago)

Hi @tikoo_sahil - no change since last week. I'll be sure to update you when we close this out, but please be patient as it might be a bit. Thanks!

TTS Bug Bounty has decided that this report is not eligible for a bounty. Sep 15th (2 years ago)

https://micropurchase.18f.gov is not eligible for a bounty, but your report is still being looked into and we will update you when we have additional information to share. Thanks again for your report!

tikoo_sahil posted a comment. Oct 27th (2 years ago)

any updates ??

coffeecup HackerOne staff posted a comment. Oct 28th (2 years ago)

Thanks again for reporting @tikoo_sahil, we're still looking into this and will respond in this ticket as soon as we have an update. Apologies for any inconvenience.

tikoo_sahil posted a comment. Nov 15th (2 years ago)

As i can see the login through github functionality has been removed , i think there is no more session management functionality available , so is it resolved ?

jkm closed the report and changed the status to ○ **Resolved**. Nov 17th (2 years ago)

Yes, conforming that this is no longer an issue. We ended up archiving the app (for unrelated reasons), and
converted it to a static site. I've heard from the developers that they'd still like to fix the issue in the codebase, in case the site's stood back up at some point, and will update this report with a link to that work if/when it's done. For now, though, marking this resolved.

Thanks for your work!

Jacob

tikoo_sahil posted a comment. Nov 18th (2 years ago)

Gr8 , waiting for the issue to be resolved in the codebase !!

tikoo_sahil requested to disclose this report. Jan 15th (7 months ago)

ryan-ahearn agreed to disclose this report. Jul 30th (13 hrs ago)

This report has been disclosed. Jul 30th (13 hrs ago)