- DISCLOSED VULNERABILITY REPORT -

By Prv | mail | github | bugcrowd |

Name: (CHAIN) Session Tokens Storage Insufficiently & Re-Use After Logout

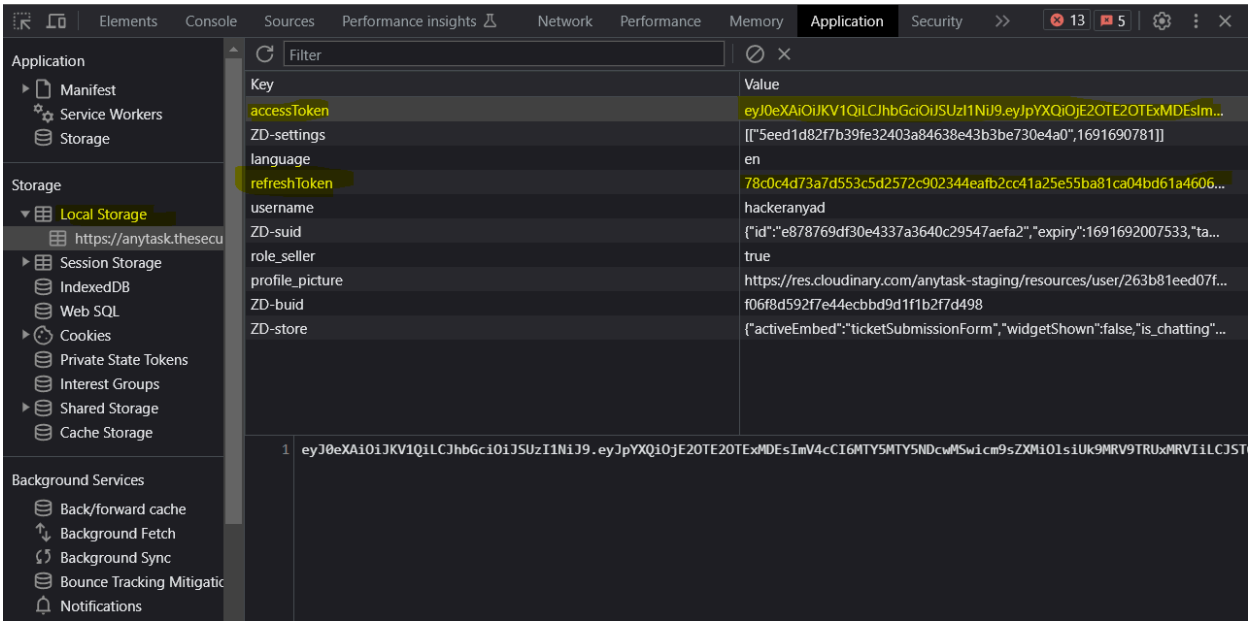
Vulnerability type: Insecure Session Management (easily obtainable session tokens)

Severity: Medium

Vulnerability Description:

During analysis of the client web application, I noticed that upon login session tokens were not visible via the 'cookies' tab- leading me to suspect the tokens were stored elsewhere on the application.

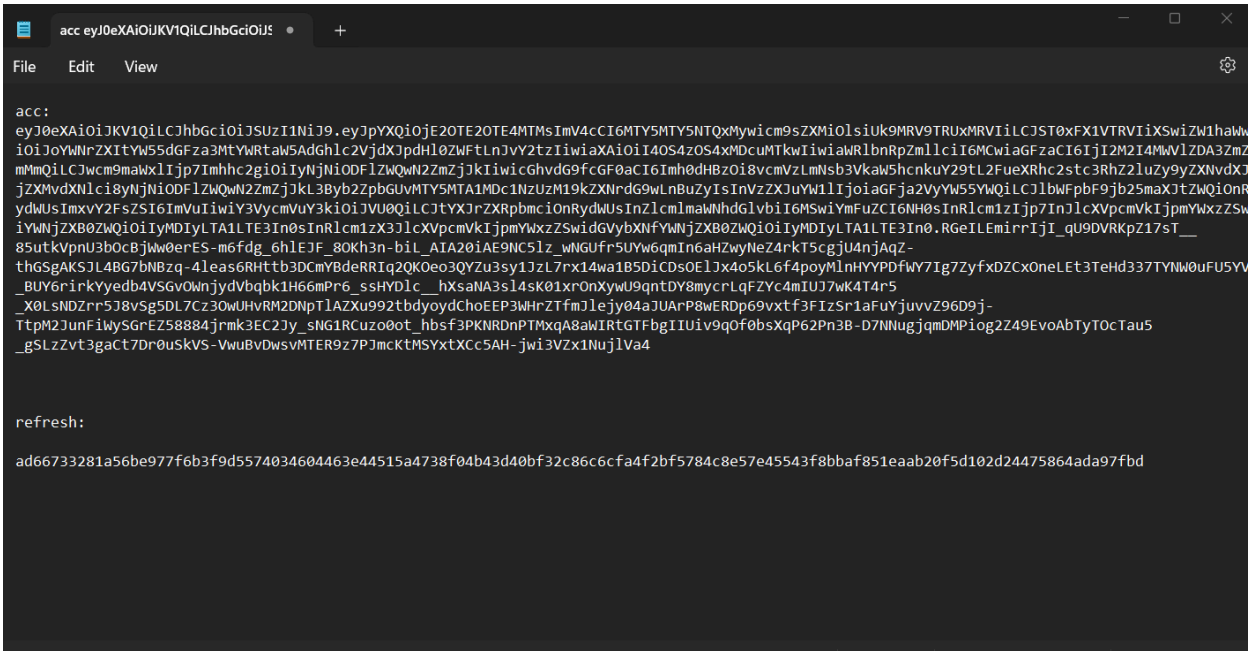
This was then confirmed when checking the 'Local storage' tab, found that these tokens were stored insecurely:



Further to this, when doing further testing of these session tokens realised that upon logout, you could also re-establish these same tokens into the application to log back into the previous session you were in, meaning they did not correctly invalidate after use either.

Chaining these two vulnerabilities together, realised it was then possible for an attacker to easily obtain these tokens through a range of methods due to their incorrect storage location- and once

obtained use them as a persistent access vector into a users account due to the nature of the further invalidation vulnerability:



This can allow an attacker to use a stored XSS Vector to obtain the easily accessible session tokens and further that attack to obtain persistent access to their account through improper invalidation.

Resolution:

The two vulnerabilities were made aware to the client and changes were quickly implemented to mitigate this issue- reputational rewards also given as a result of these findings.
