

# - DISCLOSED VULNERABILITY REPORT -

By Prv | [mail](#) | [github](#) | [bugcrowd](#) |

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

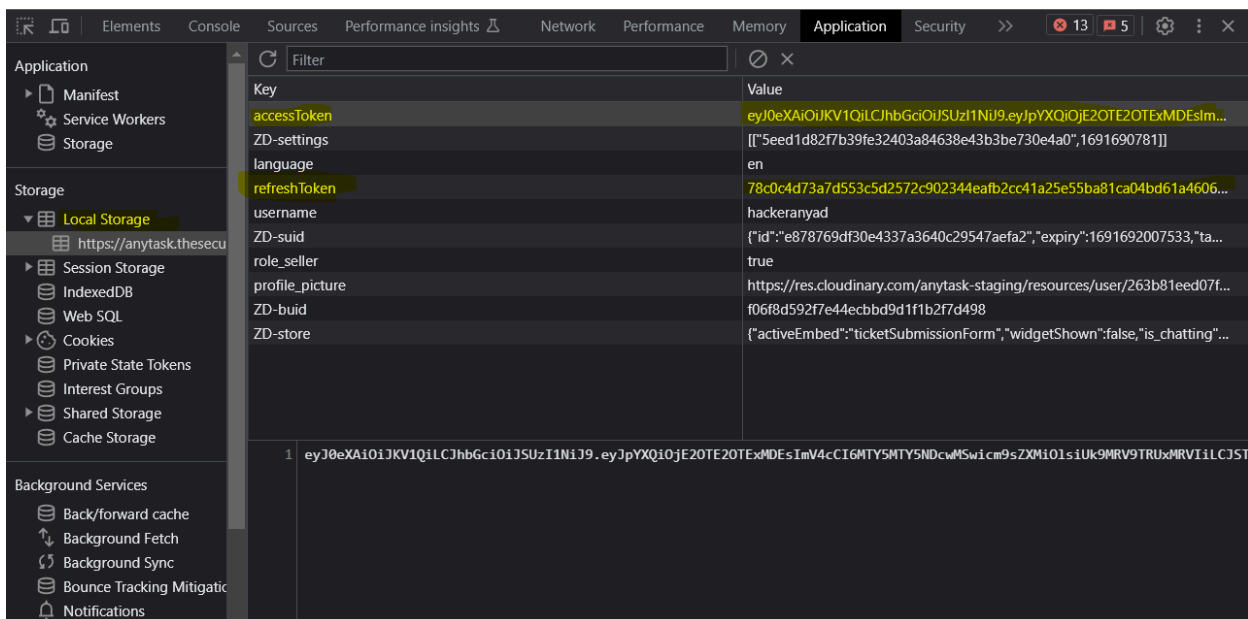
**Vulnerability type:** Insecure Session Management (easily obtainable session tokens)

**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.

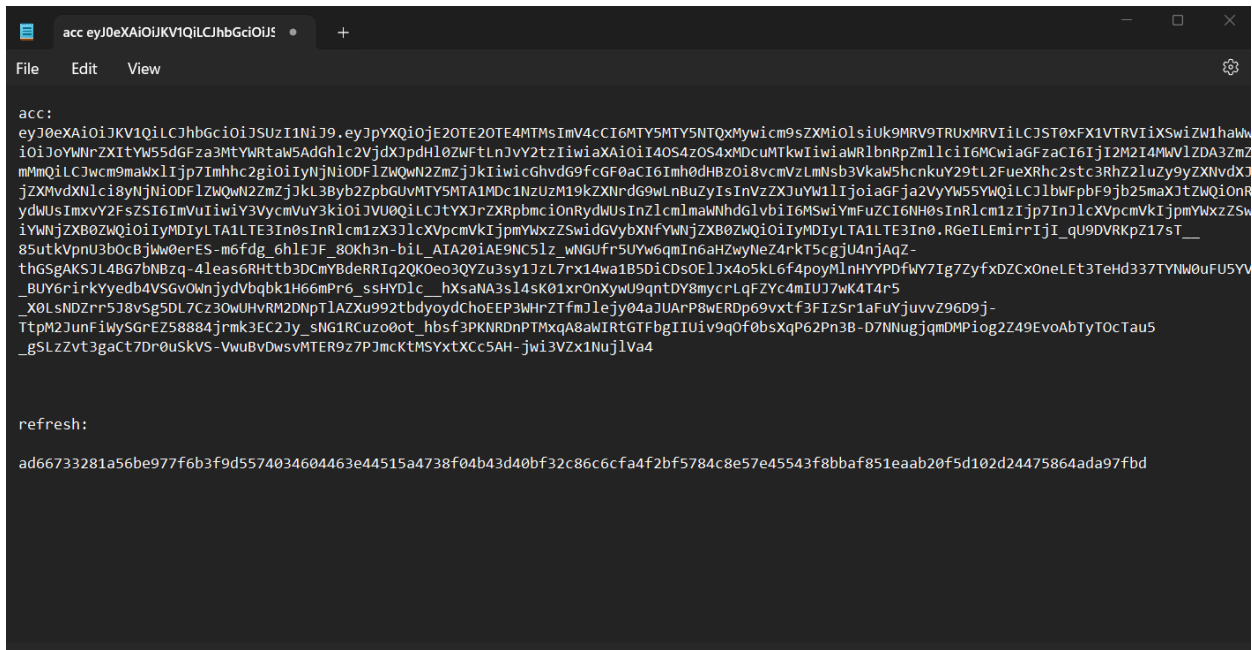
This was then confirmed when checking the 'Local storage' tab, found that these tokens were stored insecurely:



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:



```
acc:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2OTE2OTE2MTMsImV4cCI6MTY5MTY5NTQxMywic9sZXMwI0siUk9MRV9TRUxMRVIlLCJST0x0FXI1VTRVIlXSwiZW1haWw
iOiJoYWNRZlZlYm55dGFza3M0YWRtaW5AdGhlcnZvdXJpdHl0ZWFTLnJvY2tziIiwiaXAiOiI4OS4zOS4xM0cuMTkwIiwiaWRlbnRpdzmlciI6MCwiaGFzaCI6IjI2M2I4MmVlZDA3ZmZ
mMmQilCjwcm9maWx1IjP7Imhhc2giOiIyNjNiODFlZWQwN2ZmZjJkL3Byb2ZpbGUvMTY5MTA1MDc1NzUzM19KZXNrdG9wLnBuZyIsInVzZXJ0YVw1IjoiaGFja2V5YVY5YmQilCjlbWp9b25maXJtZWQlbnR
ydkU0SImxvY2FsZSI6ImVvIiwiaWV3VycmVudY3kiOiJlVU0QilCjYXJrZXRpbmciOiNRYdWUsInZlcm1maW5hdG1vbiI6MSwiYmFuZC6NH0SInRlcm1zIjP7InJlcXVpcmVkiJpmYXxzZSw
iYWVjZXB0ZWQlOiIyMDIyLTA1LTE3In0SInRlcm1zX3JlcXVpcmVkiJpmYXxzZSwidG9yYmVjZXB0ZWQlOiIyMDIyLTA1LTE3In0. RgeILEmirrIjI_qU9DVRKpZ17sT__
85utkVpnU3b0c8jw0erES-m6fdg_6h1EJF_80Kh3n-bil_AIA20IAE9NC5Lz_wNGUfr5UYw6qmIn6aHZwyNeZ4rkT5cgjU4njAqZ-
thGsgAKSJL4BG7bNBzq-4leas6RHTtb3DCmYBdeRRiQ2QK0eo3QYzu3y1JzL7rx14wa1B5DiCDsOE1Jx4o5kL6f4poyMlnHYYPdfWY7Ig7ZyfxDCXOneLet3TeHd337TYNW0uFUYV
BUY6rirkYyedb4VSGV0WnjydvbqbK1H66mPr6_ssHYDlc_hXsANA3s14sK01xrOnXywu9qntDY8mycrLqFZYc4mIUJ7wK4T4r5
_X0LSNDZrr5J8vSg5DL7Cz30wUHVrm2DNpTLAZXu992tbdyoydChoEEP3WHRZTfmJleJy04aJUARP8wERDp69vxtf3FIzSr1aFuYjuvzv96D9j-
TtpM2JUnFiWysGrEZ58884jrmk3EC2Jy_sNG1RCuzo0ot_hbsf3PKNRDnPTMxqA8aWIRtGTfBgIIUiv9q0f0bsXqP62Pn3B-D7NNugjqmDMPiog2Z49EvoAbTyTocTauS
_gSLZvt3gaCt7Dr0uSkVS-VvuBvDwsVMTER9z7PJmCkTMSYxtXcc5AH-jwi3Vzx1NuJlVa4

refresh:

ad66733281a56be977f6b3f9d5574034604463e44515a4738f04b43d40bf32c86c6cfa4f2bf5784c8e57e45543f8bbaf851eaab20f5d102d24475864ada97fbd
```

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.

---

This document is a disclosed vulnerability report by a practised security researcher, all vulnerabilities and issues mentioned in this report have been released under the permission of the owner and/or have been mitigated against and fixed before this report was written, if by any chance the contents of this report can be replicated this is due to another vulnerability or mere coincidence, please report any issues or regards: [prv@anche.no](mailto:prv@anche.no)

---