Laporan Bug Bounty Cilsy Fiolution

https://vuln.cilsy.id

Session Fixation (No Session Logout after changing password)

24 Juli 2022

Oleh Samuel Dasmianus

Issue Description

Session Fixation is an attack that permits an attacker to hijack a valid user session. The attack explores a limitation in the way the web application manages the session ID, more specifically the vulnerable web application. When authenticating a user, it doesn't assign a new session ID, making it possible to use an existent session ID.

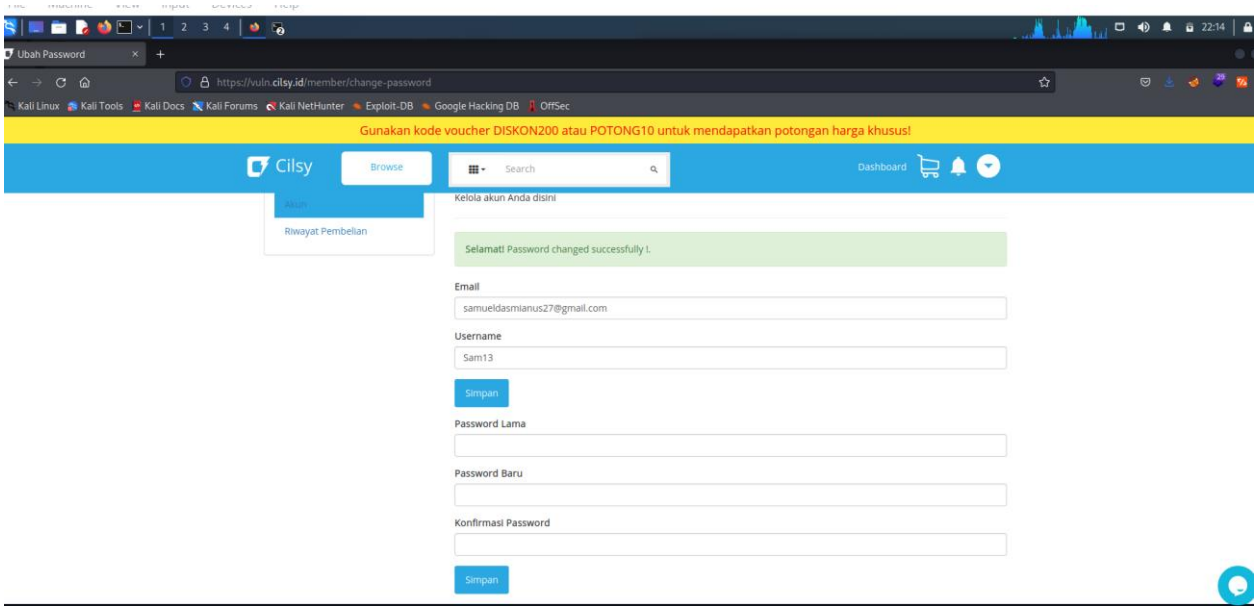
Issue Identified

User realizes his account has been logged in by someone and he changes the password, but attacker has been hijack a valid user session and still logged in.

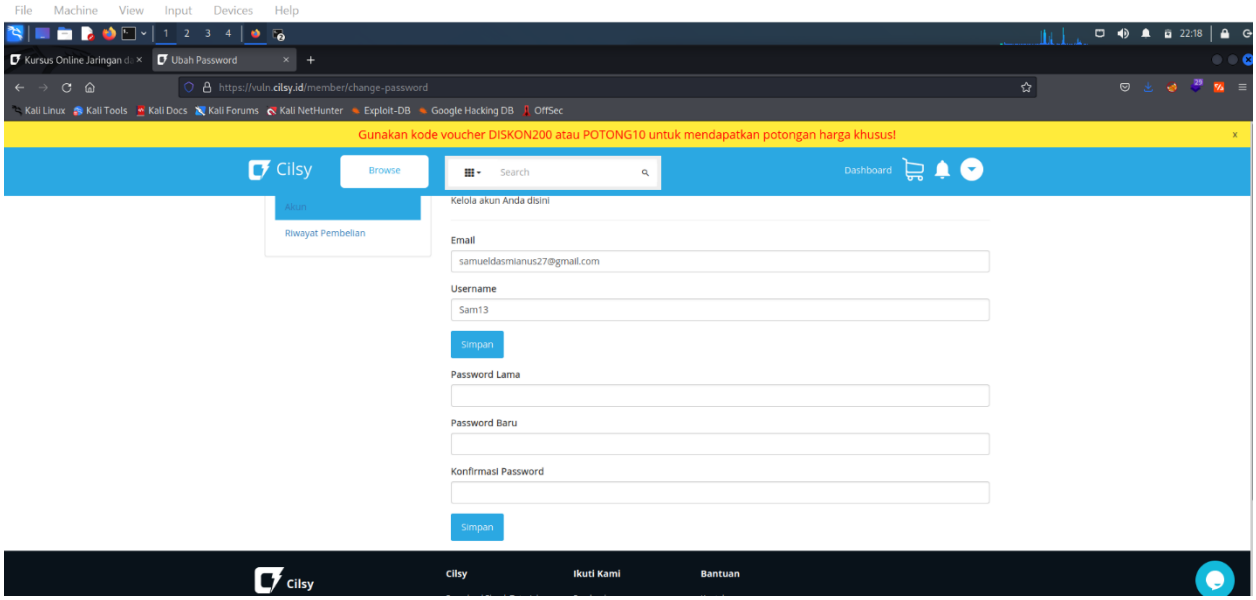
Risk Breakdown

- Risk: **Low**
- CVSS v3 Score:**2.6** (AV:A/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N)

Affected URLs & POC



Victim changed password



Attacker stiil logged in victim account

Steps to Reproduce

Step 1: Open the same accounts in 2 different browser/tab browser

Step 2: Change the password from one browser which has been logged in and copy the url to another browser/tab browser (try to refresh) and you will see the account keep logged in.

Affected Demographic

Attacker can be loggin into victim account even has been changed password before if the attacker owned the credentials before.

Recommendation

Make auto logout session after changed password / reset password.

References

For more information on remediation steps check out reference [1].

- [1] https://www.cvedetails.com/cve/CVE-2017-11398/