**DAY 38**

🡪Any sub domain might have vulnerabilities.

🡪We should enumerate the newly created sub domains.

🡪We should focus more on infamous sub domains.

🡪A sub domain can set a cookie for the base domain.

🡪The code to set a cookie is done via JS.

🡪Session cookies maintain and store session id.

Scenario:

1. A user has logged into google.com

google.com will create a session id for the logged in user

2. blog.google.com can set a cookie for google.com

Note: user is not logged into blog.google.com

Cookie: gsid:phpsessionuser123123

3. An attacker sends a specially crafted XSS payload which set the cookie value for the session cookie as attackers session id

Cookie: gsid:phpsessidattacker123123

4. The attacker will have the session as the user, the session authorization of user will be given attacker’s sessionid.

5. Finally session is hijacked.

Learn basics of JS.

Hackerone