Author

Rafal Lykowski & Piyush Patil

Description

Application is vulnerable to session fixation. It means that user or malicious actor can affect the session cookie value. In this case it is possible by setting cookie to custom-crafted one and log in to the system with this value. Application also does not set neither SameSite:strict nor lax. Moreover, security flag on session cookies such as HttpOnly is not set. It means that cookie can be manipulated/retrieved when application is vulnerable to XSS attack. In this case, application is also vulnerable to reflected XSS attack with GET method what makes it vulnerable to Full account takeover. Attacker tricking victim into visiting crafted website and loading image/ opening mail message and loading the image/ clicking in the link can takeover victim's account.

Steps to reproduce the attack:

1. Open 2 different browsers (or one with 2 windows - one of them opened in incognito mode)
2. Log in to the system,
3. Paste this payload into the address bar and load it: http://localhost:8070/app/?g=admin&n=dashboard&m=21484%27%3bdocument.cookie=%22PHPSESSID=12345;path=/;%22%2f%2f It simulates victim executing XSS.
4. In the incognito window do not log in but just modify session cookie value to 12345.
5. Navigate to any application url - you will realize that you are authorized. It means that your account was taken over.

Video POC:

https://drive.google.com/file/d/1egynTGh0XsETgfu7SJtIPv1GZCs1dJ67/view?usp=sharing

Impact

Full account takeover