Author

Rafal Lykowski & Piyush Patil

Description

Cubecart 6.4.2 allows someone to fixate (aka find or set) another user's session ID which permits an attacker to hijack a valid user session.

Steps to Reproduce Bug

1- Intercept login

2- Set cookie value to 12345

3- In browser, open developer tools=> session storage and you can see cookie is set to 12345.

POC Link

https://drive.google.com/file/d/11gQEjCw5BDZKtQrTnYqEZElneHeoQUmS/view?usp=sharing

Fix Implemented

https://github.com/cubecart/v6/commit/aac7b3a13a43e302d91f94a120417b2fda737d0f

Impact

A successful session fixation attack gives the attacker access to the victim's account. This could mean access to higher level privileges or the ability to look at sensitive data.