

HttpOnly cookie flag

- ✓ The cookie is not readable/writable from the frontend
- ➡ Prevents the authentication cookie from being leaked when an XSS attack (cross-site scripting) occurs

A01 Broken Access Control

Cross-Site Request Forgery