JWT + cookies + HTTPS + CSRF

Asked 6 years, 11 months ago Modified 6 years, 11 months ago Viewed 6k times

16

I already worked with JWT on mobile app but I will implement it on a website for the first time for the authentication and I have a little thing I still didn't understood :

- if I use JWT token with localStorage, XSS attacks are possible
- if I use JWT token with cookies, CRSF attacks are possible

..., but if I use JWT token over HTTPS with httpOnly+secure cookies and a token lifetime of 1 month, are CSRF attacks still possible in this case ?

I see all over the web for custom token with cookie or custom token with localStorage or JWT but I didn't explicitly get the answer of httpOnly+secure cookie + JWT + HTTPS + the need of CSRF.

cookies https token csrf jwt

Share Improve this question Follow

asked Feb 10, 2016 at 11:02

Alex
527 5 16

1 Answer

Sorted by:

Highest score (default)

25

If you are using JWT as an authentication token, it should be stored as a cookie marked `httpOnly` and `secure`, as apposed to using Local/Session Storage. As you mention, this protects against XSS attacks, where we are concerned about malicious JavaScript being injected into our page and stealing our session token.

- A cookie marked `httpOnly` cannot be read by JavaScript, so it cannot be stolen in an XSS attack.
- Local/Session Storage, however, can be read by JavaScript, so putting the session token there would make it vulnerable to an XSS attack.

However, making the session token cookie `httpOnly` and `secure` still leaves you vulnerable to CSRF attacks. To see why, remember that cookies are marked with the domain from which they originated, and the browser only sends cookies that match the domain to which the request is being *sent* (independent of the domain of the page the request was sent from). For example, suppose I'm signed into `stackoverflow.com` in one tab, and in another tab go to

stackoverflow authentication token cookie will be sent to the stackoverflow server. Unless that endpoint is protecting against CSRF, my account will be deleted.

There are techniques for preventing CSRF attacks. I would recommend reading this OWASP page on CSRF attacks and preventions.

Share Improve this answer Follow

answered Feb 11, 2016 at 2:20

kuporific
9,933 3 42 46

1 Hi, many thanks for your answer. I will then implement a CSRF prevention after reading the article you shared. – Alex Feb 11, 2016 at 12:57

Hello! Please have a look at this question: stackoverflow.com/questions/49597702/... I am currently implementing a RESTful API + SPA, and have been wondering about the same. Came up with this approach. Maybe share your views? – Anindit Karmakar Apr 1, 2018 at 11:59