Web application security checklist

for every full-stack app

- [ ] Use **HttpOnly** and **Secure** cookies
- [ ] Sign the cookies with strong secret
- [ ] Transport all data over HTTPS
- [ ] Use **Content Security Policy** ver. 2
- [ ] Do not allow inline scripts (*unsafe-inline*)
- [ ] Use ***integrity*** property for external scripts
- [ ] Validate and sanitize all the inputs
- [ ] Throttle failed login attempts
- [ ] Check permission / role on every endpoint
- [ ] Log application events and HTTP requests
- [ ] Consider Two-factor authentication w/ OTP
- [ ] Use **Referrer-Policy** HTTP header

CONTINUE READING

Web application security checklist

for every full-stack app

- [ ] Sign JWT with a strong secret
- [ ] Ensure JWT lib does not accept ***alg: none***
- [ ] Avoid bypassing framework sanitization
- [ ] Avoid **Access-Control-Allow-Origin: ***
- [ ] Use CSRF protection with anti-CSRF tokens
- [ ] Use ***state*** parameter in OAuth flows
- [ ] Use ***nonce*** parameter in OIDC flows
- [ ] Use *Proof Key for Code Exchange* in OAuth

Wait for my *WEEKLY* Web security tips & tricks at your mailbox every Tuesday!

Bartosz Pietrucha

@bartosz_io

websecurity-academy.com