6 Security (mgk25)

(a) What is the purpose of the `HttpOnly` flag in the HTTP protocol? Briefly describe an attack that this flag was intended to prevent. 

(b) Users of web sites often commit transactions by filling out an HTML form and pressing a “Submit” button to update some state stored on a server (e.g., password change, purchase).

(i) HTML forms can submit such requests using either the `GET` or `POST` method of HTTP. Which is more appropriate here? Give three reasons.

(ii) Some web servers place an additional token value into an invisible field of HTML forms that are used to commit security-critical transactions. What security risk can such a token mitigate?

(iii) Explain three additional checks that a web server may implement to reduce this risk.