Collaborative Discussion: Summary

During this discussion period, I learnt about a wide range of security weaknesses and mitigations. I researched the concepts of cross-site scripting, escaping, SQL injections, sensitive data exposure and techniques such as file upload vulnerabilities and salting.

Researching these various vulnerabilities and mitigations I realized that the problem was not any specific vulnerabilities being difficult to massively mitigate, but the sheer number of possible vulnerabilities. Even if most of the attack surface had security mitigations applied, one 'small' missed vulnerability can still have massive privacy consequences. I see now why tools such as OWASP top ten are so valuable, this tool helps to alleviate the largest vulnerability - a lack of knowledge (OWASP, 2018).

During this project, I realized that the OWASP top ten was similar to a tool I have previously used for Android development called Drozer. Drozer is a development tool that will try to exploit the attack surface of an Android application (Drozer, 2021). I think that a combination of the understanding provided by the OWASP Top Ten and the use of automation tools such as Drozer is required. A tool like Drozer will not be full-proof as each APK will have specific unique vulnerabilities that the tool may miss. Therefore, developers will need to apply their own knowledge (that can be acquired from the Top Ten) to have confidence.

Because it's impossible to ever be sure that the attack surface is 100% secure, we may wish to assume that breaches will be made and use preventative measures accordingly. My colleagues Anrich's discussion of sensitive data exposure brought this up while discussing how 'salting' can be used to securely encrypt data that should never be exposed - passwords. This feeds into the idea that we should try to mitigate the damage of a particular source being breached. For example, if we try to compartmentalize our data/services so that separate permissions would be needed for access to different portions of the system, we may be able to limit the scope of a breach.

[333 Words]

References

Drozer (2021) OWASP Top 10 Proactive Controls 2018. Available at: https://labs.f-secure.com/tools/drozer/

OWASP (2018) OWASP Top 10 Proactive Controls 2018. Available at: https://owasp.org/www-project-proactive-controls/.