**Week 10 - Supplementary Materials**

[Markdown](https://github.com/lawfareblog/hacking-cybersecurity/blob/main/week10/Week_10_Homework.md) | [PDF](https://raw.githubusercontent.com/lawfareblog/hacking-cybersecurity/main/week10/Week_10_Homework.pdf) | [MS Word DOCX](https://raw.githubusercontent.com/lawfareblog/hacking-cybersecurity/main/week10/Week_10_Homework.docx) | [Libre ODT](https://raw.githubusercontent.com/lawfareblog/hacking-cybersecurity/main/week10/Week_10_Homework.odt) | [HTML](https://raw.githubusercontent.com/lawfareblog/hacking-cybersecurity/main/week10/Week_10_Homework.html)

**Introduction**

Our attacks this week focus on Web applications and can be tried in any Web browser.

**SQL Injection**

[SQL injection](https://en.wikipedia.org/wiki/SQL_injection) takes advantage of poorly-sanitized inputs to inject code into Web applications and gather information from a database. This kind of attack is exemplified in this [xkcd](https://xkcd.com/327/) comic.