“Zápočtovka”

Úlohou je oboznámiť sa s jednotlivými bezpečnostnými útokmi, s ktorými sa je možné stretnúť pri webových aplikáciách a dva z nich ilustrovať pomocou vlastného naprogramovaného príkladu, ktorý bude vysvetlený pomocou videoprezentácie.

Pri výbere útokov si je potrebné vybrať po jednom útoku z nasledujúcich dvoch skupín:

skupina 1	skupina 2
Script injection SQL injection Cross-site scripting	Cross-site request forgery Podvrhnutie preddefinovaných premenných Zafixovanie session Cookies útoky Aplikácia volajúca externý program

Ak by niekto chcel ilustrovať nejaký útok, ktorý nie je uvedený v žiadnej skupine, tak je to možné a môže týmto útokom nahradiť útok zo skupiny 2.

Videoprezentácia musí obsahovať aj vysvetlenie ako pri danom príklade môže prísť k útoku a ako sa je možné voči tomu chrániť. T.j. je potrebné nahrávať nielen obraz, ale aj zvuk, resp. aspoň použiť titulky.

Na nahrávanie je možné použiť napr. OBS studio, ku ktorému máme aj stručný návod: https://elearning.mechatronika.cool/blog/obs-studio-videonavod-nahravanie-obrazovky/

Do MS Teams sa odovzdáva:

- 2x videoprezentácia s ilustráciou bezpečnostného útoku,
- 2x skripty, na ktorých demonštrujete bezpečnostný útok.

Každý z ilustrovaných dvoch útokov sa hodnotí tromi bodmi.